A Novel Authentication Protocol Based on Biometric and Identity-Based Cryptography

A thesis submitted in partial fulfilment of the requirements of Nottingham Trent University for the degree of Doctor of Philosophy

By

Dania Aljeaid

Nottingham Trent University

March 2015

Dedication

To my beloved parents
Faiza and Mesfer
For their love and sacrifice

To my dear sisters
Rania, Deema & Razan

To my dear brothers
Musharí & Nawaf

To my husband Yaser and
My precious daughter Joanne

Abstract

Recently, considerable attention has been devoted to distributed systems. It has become obvious that a high security level should be a fundamental prerequisite for organisations' processes, both in the commercial and public sectors. A crucial foundation for securing a network is the ability to reliably authenticate communication parties. However, these systems face some critical security risks and challenges when they attempt to stabilise between security, efficiency and functionality.

Developing a secure authentication protocol can be challenging; this thesis proposes an authentication scheme that employs two authentication factors involving something you know (password) and something you are (biometric) based on Identity-Based Cryptography and Elliptic Curve Cryptography. Two protocols have been chosen that provide mutual authentication and secure key exchange, which are the equivalent to the Diffie-Hellman key exchange. Due to a potential flaw in the protocols, guarding against attacks can be challenging. In order to alleviate some of the issues encountered with the new protocol, this thesis uses the encrypt-then-authenticate method.

Formal verification methods are used to evaluate the new protocol. First, finite-state machines are used to examine and predict the behaviour of the protocol. Modelling with this method shows that the new protocol can function correctly and behave correctly within the protocol description, even with invalid input or time delay. Second, Petri nets are used to model, simulate and analyse the new protocol. This thesis formulates several attack models via Petri nets in which the security of the proposed protocols is discussed precisely.

Ultimately, this novel work ensures that the new protocol provides a coherent security concept and can be implemented over insecure channels while offering secure mutual authentication.

Acknowledgments

Firstly, I would like to especially thank Dr. Xiaoqi Ma who was instrumental in helping me conceptualise, research, plan and structure this thesis.

My endless gratitude goes out to Dr. Caroline Langensiepen for her contributions to the research and her detailed advice and compilation of the thesis.

Yaser – you make every day of my life that bit easier. I could not have done my research without your selfless support.

I would like to thank my parents; Mesfer and Faiza who inspired me to work hard and never give up.

My sincere gratitude to my colleagues at Nottingham Trent University, who made my research time unique, memorable and joyful.

I would also like to thank all the people who have supported and inspired me during my life who I have neglected to mention.

List of Publications

Journals papers:

- Aljeaid, D., Ma, X. and Langensiepen, C., 2014. "*Modelling and Simulation of a Biometric Identity-Based Cryptography*". International Journal of Advanced Research in Artificial Intelligence (IJARAI), 3(10).
- Aljeaid, D., Ma, X. and Langensiepen, C., 2015. "*Analysis of Security Protocols Using Finite-State Machine*". International Journal of Advanced Research in Artificial Intelligence (IJARAI), 4(4).

Conferences papers:

- Aljeaid, D., Ma, X. and Langensiepen, C., 2014. "*Biometric identity-based cryptography for e-Government environment"*, Science and Information Conference (SAI), 2014, IEEE, pp. 581-588.
- Aljeaid, D., Ma, X. and Langensiepen, C., 2015. "*A new biometric ID-based cryptography protocol and security analysis using petri nets*", 6th Annual International Conference on ICT: Big Data, Cloud and Security (ICT-BDCS 2015). Global Science and Technology Forum, Global Science and Technology Forum.

Poster:

- Poster tilted "*e-Government Security Approach: Biometric Identity-Based Cryptography for e-Government Environment*" for the 7th Saudi Students Conference (SSC2014), Edinburgh, UK.

Contents

List of Notations

"Even the natives have difficulty mastering this peculiar vocabulary"

—*The Golden Bough*, Sir James George Frazer

Symbol	Expression	Meaning
C_i		User/Client /Computer
S_i		Server
R_i		Registration Centre
ID_{S_i}		Identity of Server
ID_{C_i}		Identity of user C
PW_{C_i}		User's password
Bio_{C_i}		Biometric template of C
Pub_K		Public Key
Pr_K		Private Key
||	x || y	x concatenated with y
p, n		Two large prime numbers
F_p		A finite field
Z_n		A set of positive integers less than *n*
Z^*_p		A cyclic group consists of all natural numbers less than p-1
E		An elliptic curve over a finite field F
G		The group of elliptic curve points on E
P		A point on elliptic curve E with order n
xP		Denotes point multiplication on elliptic curve
y		A secret information maintained by the server
(x, Pub_K_s)		The server S's Private/Public key pair, where $Pub\_K_s = xP$
r_{C_i}, r_{S_i}		A random number chosen by the C_i and S_i respectively
$H_1(.)$		A secure one-way hash function, where $H_1: \{0, 1\}^* \rightarrow Z^*_n$
$H_2(.)$		A secure one-way hash function, where $H_2: \{0, 1\}^* \rightarrow Z^*_p$
$H_3(.)$		A secure one-way hash function, where

		H_3: $\{0, 1\}^* \rightarrow Z^*_p$
$H_4(.)$		A secure one-way hash function, where H_4: $\{0, 1\}^* \rightarrow Z^*_p$
$MAC_{,k}$	$MAC_k(m)$	The secure message authentication code of m using secret key k
$\oplus$	$x \oplus y$	XOR of x and y for single-bit variables Bitwise XOR of x and y for multiple-bit variables

List of Abbreviations

ACK	**Ack**nowledgement Message
CA	**C**ertificate **A**uthority
CCA1	**C**hosen **C**iphertext **A**ttack
CCA2	**A**dopted **C**hosen **C**iphertext **A**ttack
CDHA	**C**omputational **D**iffie–**H**ellman **A**ssumption
CL-PKC	**C**ertificateless **P**ublic-**K**ey **C**ryptosystem
COA	**C**iphertext-**O**nly **A**ttack
CPA	**C**hosen-**P**laintext **A**ttack
DoS	**Denial of Service**
DDoS	**D**istributed **D**enial **o**f **S**ervice
ECC	**E**lliptic **C**urve **C**ryptography
FRR	**F**alse **R**ejection **R**ate
FSM	**F**inite-**S**tate **M**achines
HIBE	**H**ierarchical **I**dentity-**B**ased **E**ncryption
IBC	**I**dentity **B**ased **C**ryptography
IBE	**I**dentity **B**ased **E**ncryption
k-CAA1	**C**ollision **A**ttack **A**ssumption
KGC	**K**ey **G**eneration **C**entre
KPA	**K**nown-**P**laintext **A**ttack
MITM	**M**an-**I**n-**T**he-**M**iddle
PKG	**P**rivate **K**ey **G**enerator
PN	**P**etri **N**ets
SSL	**S**ecure **S**ocket **L**ayer
SYN	**S**ynchronise Message
UML	**U**nified **M**odelling **L**anguage

List of Figures

List of Tables

List of Protocols

List of Attacks

"Analysis and observation, theory and experience must never disdain or exclude each other; on the contrary, they support each other"

-On War, Carl Von Clausewitz

1

Introduction

While the pervasive use of distributed systems facilitates end-to-end communication for organisations through effective use of information technology, it also poses serious risks and security threats. The main challenge organisations face is to develop a framework that promotes exchanging data for organisational entities. When most distributed systems were being designed, Public Key Infrastructure (PKI) seemed to be the best solution for the scheme as far as security is concerned. PKI is presently deployed in most organisation implementations as it is perceived as a mature technology, which is widely supported and can be easily integrated with different systems. Examples of current initiatives that apply PKI on a large scale are the US eGov initiative (www.usa.gov), which is supported by Federal PKI (Caloyannides *et al.*, 2003), and the Saudi Arabian e-Government Program

(yesser.gov.sa) (Sahraoui, *et al*., 2006).

One of the main issues concerning the security perspective in distributed systems is granting access to authorised users as well as the need to verify that the user is really who they claim to be. The most common solution to this problem is to deploy PKI (Evans and Yen, 2005) and digital signatures in large-scale systems. Even though PKI supports strong authentication and digital signatures, it has a few disadvantages. For example, users must be pre-enrolled, certificate directories can leak critical information, key recovery is difficult and costly, and boundary services (anti-spam, anti-virus, archiving) integration is very difficult (Voltage Security, 2006; Zhao *et al*., 2012).

Thus, to take full advantages of the capabilities of distributed systems, end users need robust security solutions to achieve assurance when dealing with them. A variant of public key cryptography that derives public keys directly from unique identity information (such as an e-mail address) known by the user is called Identity-Based Cryptography (IBC). This approach has recently received considerable attention from researchers (Lim and Paterson 2011; Yussoff et al. 2012; Mishra and Mukhopadyay, 2013; Nicanfar et al., 2014; Joonsang et al., 2015) as the development of ID-Based Cryptography offers great flexibility and obviates the requirement for user certificates since the identity of the user can be transformed into encryption keys and used for authentication.

1.1 Problem Statement

Without a secure and trusted infrastructure, organisations, such as governments, would leave data electronically unsecured and vulnerable to attacks. Therefore,

organisations constantly look for ways to deliver secure and reliable services. ID-Based Cryptography introduces lightweight key management and offers encryption for data confidentiality and robust authentication, which are prerequisites for securing high-value transactions. The question this research addressing is, can biometric and ID-based security be successfully integrated into distributed systems and hence increase the usability and security of the authentication mechanism whilst reducing administrative overheads?

1.2 MOTIVATIONS

The PKI approach uses asymmetric algorithms, where a pair of keys is used to encrypt and decrypt data. Usually, a public key is used for encryption and it is usually known to everybody and freely distributed while a private key is kept secret from one part and is used for decryption.

In traditional PKI application, a user's public key is certified with a certificate issued by a Certification Authority (CA) as shown in Figure 1.1. For example, Alice (the sender) must obtain Bob's (the recipient) certificate in order to send him an encrypted message. However, both participants must first verify the corresponding certificates to check the validity of the public keys with a trusted authority.

When many CAs are involved between two users, trust relationships among those CAs also have to be verified. PKI is an important infrastructure for managing the trust relationship among entities in a hierarchical manner. In certificate-based schemes key revocation is also an issue which requires a large amount of storage and computing. As a result, certificate-based public key cryptosystems require a large

amount of storage and computing time to store, verify and revoke certificates (Zhao *et al*., 2012; Li *et al*., 2015).

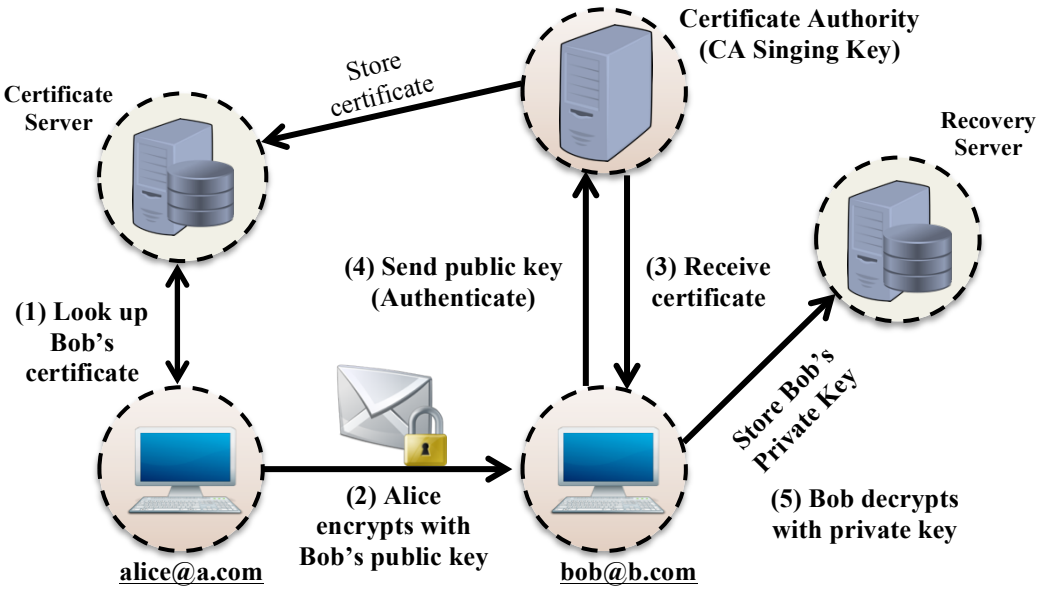


Figure 1.1: Public Key Infrastructure

In contrast to PKI, ID-based cryptography provides public keys for encryption, which are a combination of identity information known by users such as an e-mail address. For decryption, the corresponding private key is generated by a trusted third party called a Private Key Generator (PKG), which has been calculated from the user identity and the master secret as shown in Figure 1.2 and then given to the user through a secure channel (Shamir, 1985). The idea behind this scheme is to eliminate the public key distribution problem by making each user's public key derivable from some aspect of his identity (Joye *et al*, 2011; Abraham *et al*, 2011l; Krishna *et al*, 2012).

Since communications among organisations users are frequent, it is important to find a robust encryption and signature scheme to achieve a secure authentication. Identity-based cryptography is based on two popular approaches for the key management design: Elliptic Curve Cryptography and Bilinear Pairing Computation (Boneh and Franklin, 2001).

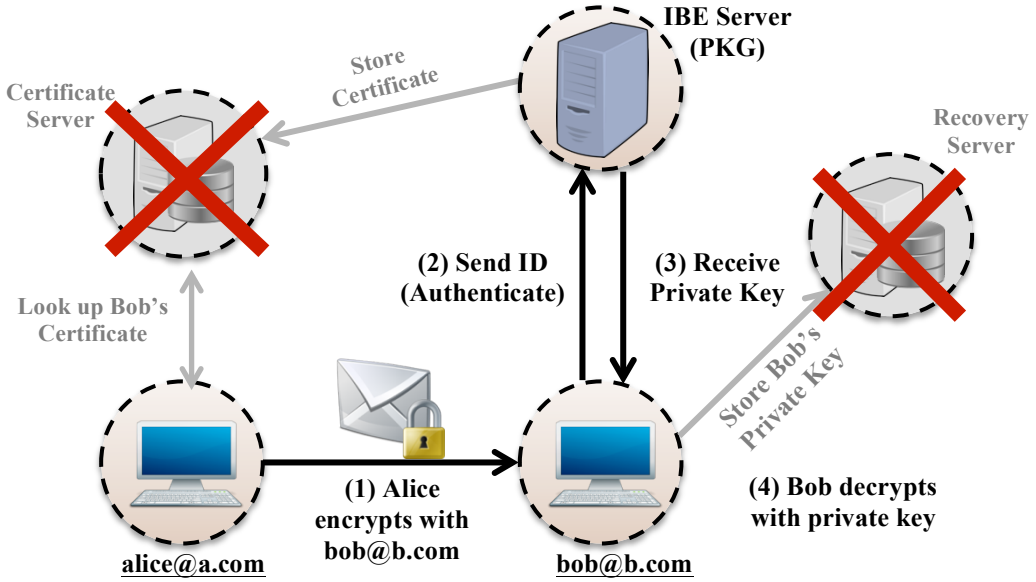


Figure 1.2: Identity Based Encryption

Also, what differentiates Identity-Based Encryption (IBE) from other infrastructures is the need for only a single connection and being able to operate offline, which is particularly useful in large distributed computing environments (Martin, 2008).

1.3 Research Methodology

Research methodology is the process of delivering an accurate explanation of the defined problem through a set of phases and steps. This step-by-step methodology provides a backbone to design and validate security protocols. It ensures that no

weakness or vulnerability is overlooked and that all essential information is gathered before designing the protocol. Zelkowitz and Wallace (1998) categorised computer science approaches into four groups: scientific method, engineering method, empirical method, and analytical method.

Freitas (2009) divided the computer science scientific research method into four classification: theoretical, experimental, and simulation. Whereas Elio *et al*. (2011) defined scientific research into five methodologies: formal, experimental, build, process and model. Given the nature of this research, it was challenging to find a suitable research methodology. As a result, a combination of the Freitas (2009) model approach and the Di *et al*. (2014) design security methodology were adopted to guide this research work. Di *et al*. (2014) methodology was chosen because it is based on a set of design principles to develop a step-by-step security protocol using a systemic approach.

This thesis examines the application of ID-based cryptography infrastructure and how to integrate a biometric verification method into systems as an alternative solution to current PKI. The research methodology is developing an authentication protocol that enforces security properties. This thesis explicitly models and simulates the behaviour of the proposed protocol by using finite state machines and Petri nets.

The research objectives and motivation stipulated that the best approach for the research is to be divided into two main parts (Figure 1.3). Each part consists of various phases to help develop and maintain a secure protocol. The first part of the research methodology consists of three cascading phases inspired by waterfall model: the first phase starts from gathering information and literature that are related to the research topic; the second phase defines protocol objectives and the security goals that the protocol must achieve in the end; the third phase highlights selection

and classification of the design principles. The second part of the methodology is regarded as an iterative process, which is very similar to spiral model (Boehm, 1988). Typically, it tends to optimise the current design of the proposed protocol without changing its functionality and maintaining low-cost cryptographic techniques. The strong point of this methodology is that it can be used to benchmark research progress and assess the state and maturity of the proposed protocol.

Phase 1 – Literature review

This phase of the methodology was the initial phase of the research work. It started with a reviewing of current and related literature for the defined problem, then study and synthesise of information and literature relevant to the research area. The chief goal was to gain knowledge about the security issues related to the research area and to identify feasible solutions. Some of the research topics under investigations are: current trends and security issues in distributed systems, weaknesses in PKI, ID-based encryption, biometric verification systems, and formal verification methods for evaluations. The information gathered mostly consisted of scientific papers, journals, conference proceedings, ISO standards and textbooks.

Phase 2- Define protocol objectives and security goals

After gathering and studying the literature, the objectives were formulated and linked to the fundamental aspects of security: confidentiality, integrity, and availability. Each protocol objective was achieved by reflecting the security aspects and protocol goals while underlining any potential threats. This was an important step because every aspect of the protocol is subject to an attack by a malicious entity and consistently reviewing the security goal keeps the protocol up-to-date.

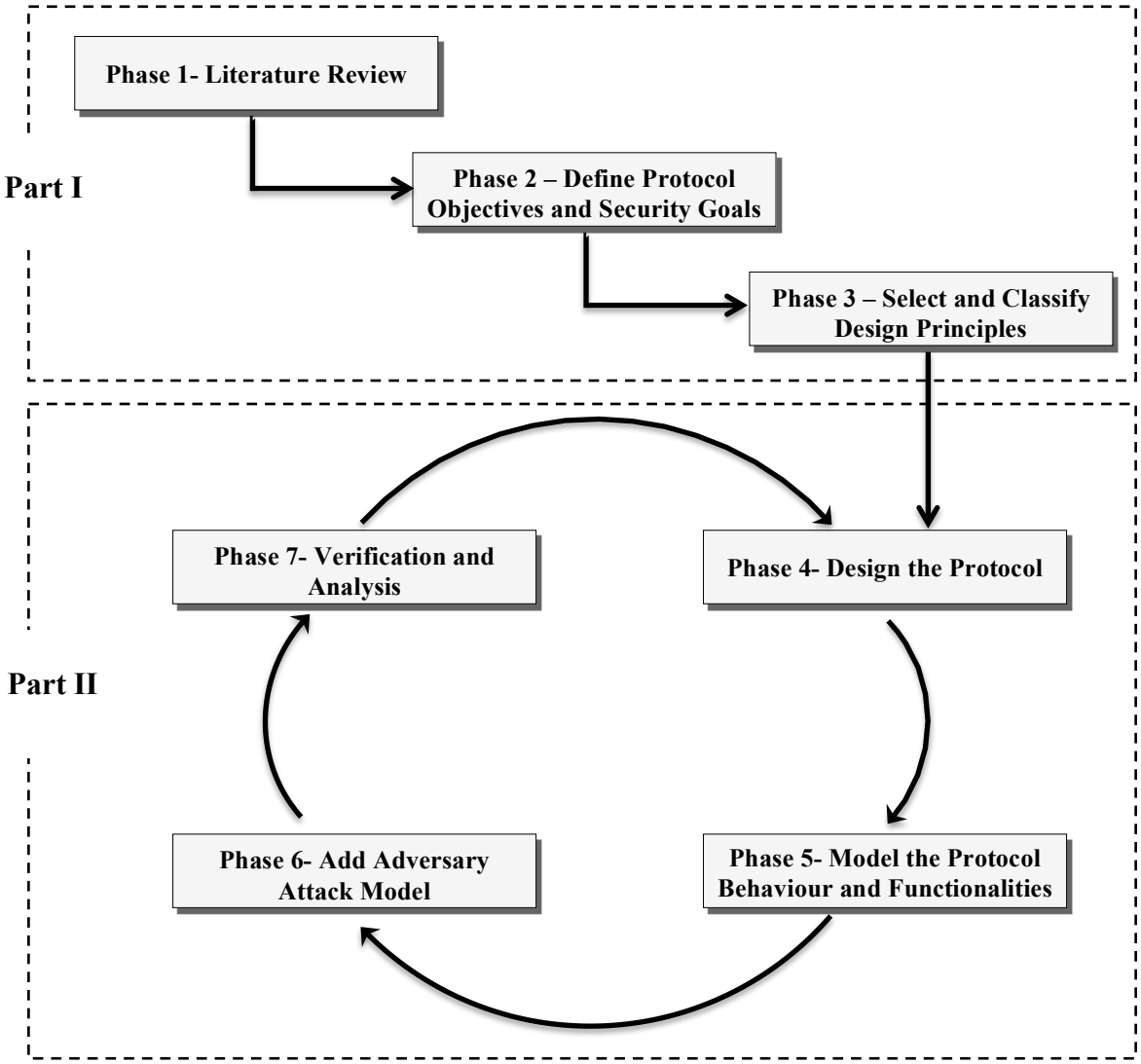


Figure 1.3: Research Methodology

Phase 3 - Select and classify design principles

This phase concerned cryptographic primitives and authentication algorithms. The security of the protocol depends on using *two-factor authentication*: the biometric verification system, elliptic curve cryptography and ID-based Cryptography. It was necessary to select a method that allows key agreement protocol to be established without being exposed during the handshake procedure.

Phase 4 - Design the protocol

In general, designing any protocol from scratch tends to be difficult. Therefore, the research focused on finding the most suitable lightweight protocol and improving its security characteristics. This was achieved by critically addressing each step of the protocol contexts and increasing the complexity of its security.

Phase 5 - Model the protocol behaviour and functionalities (simulation)

Behaviour modelling and simulation are usually easier and less expensive to run than in real environments. Simulation is a simple and safe practice to evaluate, and it tends to identify weaknesses and improve performance. Also, it defines the protocol steps and of what it is capable. Modelling and simulation include description of state machines and Petri nets of the communication between the server and the client. Two tools have been chosen for the research. The first software is Visual Automata Simulator (1.2.1) designed by Jean Boret. This software was developed to draw and simulate different theoretical machines, including finite state automate and turning machines. The second software is TAPAAL 3.1.3 and it was developed by Department of Computer Science at AALborg University in Denmark. This tool is a graphical editor for modelling, simulation and verification of Timed-Acr Petri net model. Both tools are compatible for Linux, Windows and Mac OS X platforms.

Phase 6- Add adversary attack model

This phase of the methodology is vital. Adding an attacker model to the protocol helps to assess how the protocol would run with an intruder and what information can be intercepted during transition and how much information are exposed during transmission. This phase simulates attacks in order to assessing authentication

controls and whether the adversary can probe the system and obtain valuable information.

Phase 7- Verification and analysis

This phase helps to validate the protocol with various attacks and identify flaws to amend them. This phase formally ensures the new protocol satisfies its specification and functions soundly via simulation tools chosen for this research. Furthermore, it provides a deeper understanding of the protocol's behaviour and simulate the progress of the protocol.

1.4 ORIGINAL CONTRIBUTIONS

The novel contribution of this research focuses on secure distributed systems and improving their authentication and communication. To guarantee the security of these systems, biometrics verification and ID-based cryptography are used. The new authentication protocol is based on a three-way handshake mechanism, which is the kernel of the protocol. This mechanism is applied to negotiate the secure components of a session between the client and the server, such as verifying the identity of the client using biometric data and password, agreeing on cryptographic algorithms, mutually authenticating each other, and using biometric and ID-based encryption techniques to generate session keys.

The proposed protocol allows a client and a server to exchange encrypted messages with each other. Symmetric cryptography is used to ensure that the subsequent messages are protected during transition. Each enciphered message is appended with a MAC value to alert the recipient in case of message tampering. The aim of the new protocol is to establish a shared session key between the server and the client with

mutual authentication using the encrypt-then-authenticate method. The protocol achieves cryptographic goals using bit-wise exclusive-OR (XOR) operations and collision-free one-way hash functions as the main cryptographic operation. Additionally, applying symmetric cryptography adds another layer of protection.

The new protocol is evaluated via two formal verification methods: finite-state machine (FSM) and Petri nets (PN). The security analysis via PN showed that the protocol is secure against most known active and passive attacks. Furthermore, the new protocol generation does not require heavy computation, such as modular exponentiations and digital signatures and it can be implemented efficiently in devices with poor computing power such as smartcards, ATMs and smartphones.

1.5 THESIS ORGANISATION

The rest of this thesis is organised as follows, mostly in accordance with the research methodology.

Chapter 2: Literature Review

This chapter introduces background material on computer security and security metrics, which includes availability, confidentiality, integrity, non-repudiation and authenticity. Furthermore it discusses the controls and the cryptographic considerations that are effective for each metric. Finally, the chapter provides a brief discussion on Public Key Infrastructure (PKI) and the most recent application on Identity-based cryptography.

Chapter 3: Design Analysis

This chapter introduces and explains some of the concepts that underpin the work in this thesis. It reviews the original steps of identity-based cryptography, briefly discusses biometric verification systems. Then, it analyses several attacks that authentication protocols may encounter. Finally, it examines two simulation tools.

Chapter 4: The new Protocol Architecture

This chapter draws a general idea of protocol architecture and the cryptographic techniques used to establish a secure key exchange. Additionally, it illustrates basic security properties to develop secure methodology.

Chapter 5: Protocol Design

This chapter describes the new protocol phases and the objectives the protocol should achieve. The proposed scheme consists of four phases: system initialisation phase, registration phase, login phase, and authentication phase. It identifies explicitly the process of each phase and discusses the defence mechanism used.

Chapter 6: Performance and Behaviour Modelling

This chapter elaborates the details of the finite-state verification of the new protocol and identifies the functionalities of each phase. Also, it studies the behaviour of each machine created for each phase and how they interrelate, even with invalid input or time delay. Modelling with a finite-state machine helps to understand the behaviour of cryptographic protocol. Additionally, it offers accurate results and provides a clear perception of the system's characteristics. The analysis presented in this chapter covers the process of the three-way handshake used to negotiate the session key, and examines the behaviours of the protocol and enumerates all possible states it can reach.

Chapter 7: Security Evaluation

This chapter presents a PN approach to modelling, simulating and analysing the new protocol. A formal approach like PNs allows one to formally represent communication protocols. For the sake of simplicity, a complex PN model will not be discussed until all attacks are demonstrated and the model has proved to be secure. This chapter shows how Petri nets are used to model and analyse the cryptographic protocol into two steps. First, the new protocol is modelled without an adversary, and then a generic adversary model is added to examine all possible adversary behaviours. The chapter presents an innovative idea to simulate different attacks such as man-in-the-middle attacks, parallel session attacks, and reflection attacks.

Chapter 8: The Modified Protocol

To give more perspective on the new protocol, this chapter is full of rich detail to finalise the new protocol. It discusses the enhancements to improve the new protocol and it presents a modified version of it. This includes another run of validation and evaluation via FSM and PN. Also, it briefly discusses various attacks against the modified proposed protocol. This chapter proves the benefit gained from Chapter 5 and 6 by using formal methods of analysis. This suggests how the methodology is capable of detecting flaws.

Chapter 9: Conclusions, Limitations, and Future Works

This chapter presents a summary of the proposed protocol and the security criteria provided for organisations. It briefly discusses some of the limitations that occurred during the research and the approach. In addition, it discusses further work that needs to be undertaken in this field.

2

Literature Review

This chapter describes all aspects of computer security. By examining them, one will be aware of a computer's major problem areas. This chapter introduces some background knowledge of computer security, further discusses the controls that are effective against them and how current research is addressing the open problems. Finally, the chapter provides a brief discussion on Public Key Infrastructure (PKI) and the most recent application on Identity-based cryptography.

2.1 WHAT IS SECURITY?

"Uncertainty is the only certainty there is, and knowing how to live with insecurity is the only security"

John Allen Paulos

Information security is the art of protecting information and information systems and understanding how to identify risks and weakness, as well as how to defeat or eliminate them. For this reason, it is essential to assess the true security profile, and this can be accomplished by understanding the source of risk and weaknesses that exist in the system. The most common risk is embodied by the external attacker accessing an organisation information system via the Internet. Usually these attackers break into a system for various reasons, for example, to steal information, or disrupt business and create chaos, or simply just for personal gratification.. Nowadays organisations view the computers on the Internet as valuable potential sources of information. Therefore, organisations always seek to secure their system and create a balance between security and functionality. To protect themselves, organisations must understand the impact of attacks and what the attackers are capable of in order to stop and limit the damage.

In essence, security must be assessed from multiple perspectives for the best result. These perspectives range from physical security of the machines to the configuration of the firewalls to the trustworthiness of employees. The security assessment of a system can be assessed by the CIA triad, sometimes called the security triad, comprising: confidentiality, integrity, and availability. The CIA triad plays a significant role in information security. It forms a foundation aspect that comes to

protect information by recognising security into three major areas. The goal of CIA is to ensure that protective measures are properly implemented to prevent attacks and intrusion and to limit the damages, for example, eliminating unauthorised access. The security metrics of the CIA triad are:

- ***Confidentiality***: ensures that an asset/data is viewed only by authorised parties
- ***Integrity:*** ensures that the data/asset is modified only by authorised parties
- ***Availability:*** ensures that the systems can be used by any authorised parties

These metrics are the basis of computer security. They help to define the objects of security threats and examine techniques to prevent security breaches or at least mitigate their effect. However, Sloan and Warner (2013) argue the CIA triad covers all information and it does not fully describe identity. Attacks can occur in the process of authentication by defeating online authentication. Any attacker who successfully impersonates a legitimate user would compromise both confidentiality and integrity by stealing protected information and altering data (Sloan and Warner, 2013).

In addition to the CIA, ISO 7498-2 added two more properties that are desirable, especially in communication networks (Pfleeger et al., 2015):

- ***Authentication:*** verifies entity access to system resources, including data and applications. Authentication controls include authorisations and accountability (Stapleton, 2014; Pfleeger et al., 2015).
- ***Non-repudiation or accountability:*** a combination of integrity and authentication (Pfleeger et al., 2015)

These two extra properties extend security notions with regard to identity and cover all the security aspects that were missing in the integrity and authenticity. There are many measures and controls available to provide security. To understand their impact it is necessary to review the types of attacks that can affect the security metrics. The Figure 1.2 is an enhanced version, which is adopted from Sloan and Warner (2013). It shows the different attacks that can be launched against the security metric if the vulnerability inherited with it were not covered. Be recognising the type of attacks against each metric, preventive and detection measures can be implemented to strengthen the security.

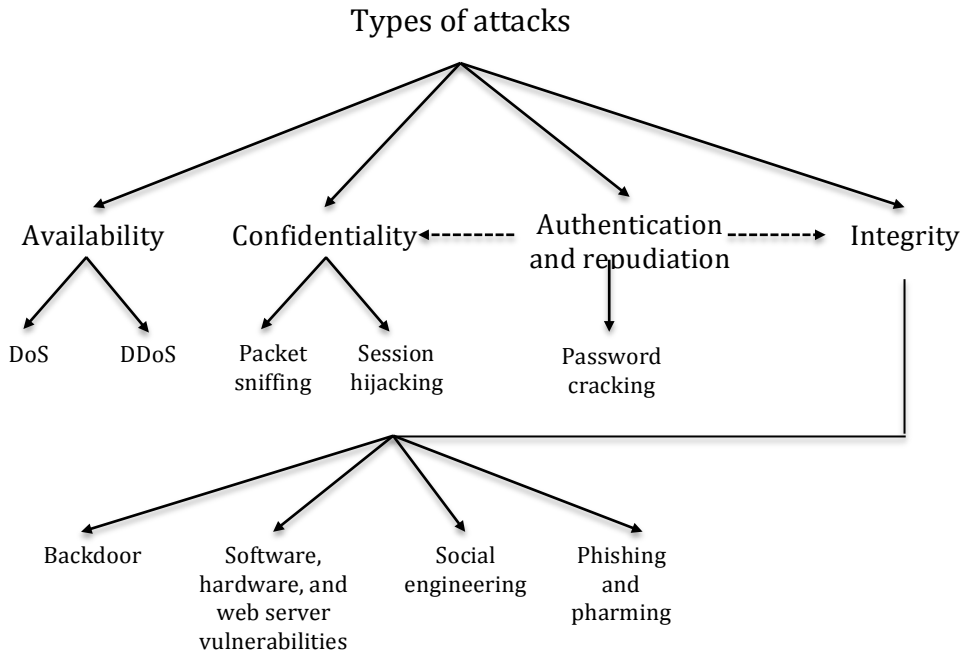


Figure 2.1 Complete an overview of types of attacks and examples

It is often hard to separate attacks on authentication alone from attacks on confidentiality and integrity, as the goal of many attacks is to steal personal information (by attacking confidentiality) and successfully impersonate someone

legitimate (by attacking authentication) in order to alter or delete information (by attacking integrity). These attacks are related to each other because they may affect all the security elements. The result of these attacks can potentially compromise the organisation's resources.

2.2 AVAILABILITY

Availability can be applied to data and services provided. It must ensure that the information must be accessible to authorised users at all times. Failure to provide services to users is one of the issues effecting availability. For example, experience overload, slow computer response, or access to information is denied due to denial of service attacks. Availability can be defined as a combination of the following criteria: capacity, performance, fault tolerance, and usability.

A typical example of attacking availability is the denial-of-service (DoS) attack, where the target is swamped with extremely large volumes of network traffic and becomes completely overwhelmed with requests. Another example is distributed denial-of service (DDoS) attack, where the requests appear to come from multiple sources. The target would have difficulty in distinguishing the attack traffic from legitimate ones. These attacks cause considerable disruption and force the organisation’s website to shut down (Sloan and Warner, 2013).

Therefore, while availability is an important security metric, this research will not discuss availability in detail and how this metric affect the new protocol. It is beyond the scope of the thesis to engage in a detailed discussion.

2.1.2 CONFIDENTIALITY

The aspect of confidentiality is straightforward. It refers to the secrecy to access protected data by authorised entities only. In other words, confidentiality identifies the security control requirements to protect the disclosure of information from unauthorised individuals or systems during the data life cycle (Stapleton, 2014). Data resides in many places, for example data stored in the database or data that is moving across the network. Ensuring confidentiality can be difficult because data classifications require different levels of control. For example, determining what level of control needed in protecting cryptographic keys is different to protecting passwords, and protecting passwords is different to protecting account numbers (Stapleton, 2014). It is important to emphasise the security controls and protect data from unauthorised access during transmission, or in storage. The adoption of data encryption provides mitigation against data breaches. Packet sniffing is one example that threatens confidentiality. To prevent sniffing of critical information encryption provides a good defence. Protecting confidentiality of data can be achieved through the combination of encryption and integrity protection techniques. The next section discusses the cryptographic consideration to guarantee confidentiality.

2.3.1 CRYPTOGRAPHIC CONSIDERATIONS

Throughout the ages, cryptography was used as a method to protect information. Encryptions such as Caesar's cipher and One-Time Pads were invented to protect sensitive data (Gregg, 2014). Cryptography is one way to protect computer security. It is considered one of the most powerful tools in delivering security by making it

harder or meaningless for the attacker to interpret the encoded data without knowing how the encryption was done.

Cryptography can be found in almost every information security control and it can be used to improve confidentiality, integrity, authenticity, and non-repudiation. For example, symmetric encryption provides confidentiality, hashing provides integrity, and digital signatures provides authenticity, integrity, and non-repudiation (Gregg, 2014).

Cryptographic algorithms can be categorised into three groups: symmetric, asymmetric and hashing. Each algorithm possesses a unique role in the world of cryptography and can be applied to protect data while in transit or at rest. The next section will explain the difference between symmetric and asymmetric algorithms. Hashing will be discussed in section (2.4.1). Confidentiality can be achieved through the use of encryption, offering an easy solution to protect informational assets in case the equipment contained within them is stolen, accessed by unauthorised users, or lost. The next section will discuss the difference between symmetric and asymmetric algorithms.

2.3.1.1 Symmetric Cryptography

Symmetric algorithm utilises a shared key and both the sender and recipient share the same secret key for the encryption and decryption process. Furthermore, it is well known to operate at extreme speeds -being one hundred times faster than asymmetric cryptography - and can encrypt and decrypt quickly (Murphy, 2015; Gregg, 2014; Gibson, 2012). Additionally, it is considered strong and hard to break if a large key is used (Gregg, 2014).

Symmetric cryptography can be used to encrypt data at rest and data in transit (Murphy, 2015). Symmetric encryption comprises two types of ciphers known as a block cipher and a steam cipher. The block cipher processes the message by dividing the input data into blocks while the stream cipher processes the message by dividing the input data into bits. Symmetric algorithms include (Gregg, 2014):

- *Data Encryption Standard (DES)*: This is the most common symmetric algorithm used. DES functions as a block cipher and processes 64 bits of plain text at a time to output 64-bit blocks of cipher text using a 56-bit key. DES has four modes: electronic codebook mode (ECB), cipher block chaining mode (CBC), cipher feedback mode (CFB), and output feedback mode (OFB). To extend the usefulness of DES, 3DES was developed as a multiple encryption, which can use two or three keys to encrypt data.
- *Advanced Encryption Standard (AES)*: also known as Rijndael, this is an iterated block cipher that supports variable key and block lengths of 128, 192, or 256 bits. In 2002, the U.S. government adopted AES to protect classified information because DES was vulnerable to brute-force attacks and meet-in-the-middle attacks. AES is considered a fast, simple, and robust encryption mechanism. Each step is performed involving four stages during each round, as follows: SubByte, Shift Row, Mix Column, and Add Round Key.
- *Rivest Cipher (RC)*: This includes RC2, RC4, RC5, and RC6. The ciphers of this family all designed by Ron Rivest. RC4 is a stream-based cipher and is faster than block mode ciphers and most commonly found in 128-bit key versions. RC5 is a block-based cipher and the number of rounds performed ranges from 0 to 255 and the key ranges from 0 bits to 2040 bits in size. Finally, RC6 features variable key sizes and rounds and includes two new

features - integer multiplication and four 4-bit working registers.

Even though symmetric algorithm has a fast encryption and decryption process, it also has three disadvantages. The first problem is key distribution (Gregg, 2014). For example, a secure method must be applied during key transfer in order for this algorithm to be effective. The second challenge with symmetric encryption is privately sharing the key (Gibson, 2012). The shared key must only be known by the entities encrypting and decrypting the data. The dual use of keys causes weakness in the algorithm and the confidentially would be violated if the key was discovered by other entities who were able to decrypt the data.

2.3.1.2 Asymmetric Cryptography

Asymmetric encryption is based on an asymmetric algorithm that utilises two keys for encryption and decryption. It differs from symmetric encryption because it uses a difficult mathematical problem, which is called a trapdoor function (Gregg, 2014). Trapdoor functions perform on the difficulty in factoring large prime numbers. These functions are useful because it can perform in both directions. For example, forward direction is used for encryption and signature verification, and the inverse direction is used for decryption and signature generation (Gregg, 2014). This algorithm, by design, is relatively slow when compared to symmetric algorithms (Murphy, 2015). Also, it requires a longer key length in order to achieve the same level of security that is achieved through symmetric cryptography (Chapple *et al*., 2013; Ballad *et al*., 2011). The most widely used asymmetric cryptography solutions are as follows:

Diffie-Hellman Key Exchange

Whitfield Diffie and Martin Hellman introduced the first asymmetric cryptography algorithm in 1976. It was originally used to distribute the symmetric keys and is based on the mathematics of discreet logarithms in a finite field and the use of one-way functions (Gregg, 2014; Chapple *et al*., 2013; Ballad *et al*., 2011). The Diffe-Hellman is used as a component in Secure Socket Layer (SSL) and IPesc (Gregg, 2014) and it allows two entities to receive the symmetric key without any prior communication. The key exchange mechanism for Diffie-Hellman is constructed as follows (Konstantinou *et al*., 2013; Chapple *et al*., 2013; Ballad *et al*., 2011):

Suppose two communicating parties, ***A*** and ***B***, want to agree on a shared secret key, they may execute the following steps.

1. ***A*** and ***B*** first agree on a finite cyclic group G as well as one of its generators g (it is not necessary to keep g secret).
2. ***A*** initiates the protocol by generating a secret random positive integer a.
3. ***B*** also generates a secret random positive integer b.
4. Then ***A***'s public value is computed as g^a mod p while ***B***'s public value is g^b mod p.
5. Next, ***A*** and ***B*** exchange their public values, ***A*** computes $g^{ab}= (g^b)^a$ mod p, and ***B*** computes $g^{ba} = (g^a)^b$ mod p. It is easy to check that $g^{ab}= g^{ba} = k$.
6. ***A*** and ***B*** can now communicate using their secret shared key which they can, subsequently, use to communicate by means of a shared key block cipher.

The Diffie-Hellman algorithm is susceptible to man-in-the-middle attacks because no authentication occurs when the public keys are sent (Kahate, 2013; Chapple *et al*.,

2013; Ballad *et al*., 2011). To overcome this problem, the use of digital signature or the Password Authentication Key Exchange (PAKE) form of Diffie-Hellman can be effective (Gregg, 2014).

Rivest, Shamir, and Aldeman (RSA)

RSA is the popular asymmetric algorithm and it can be used for digital signature, key exchange, encryption, and decryption (Gregg, 2014; Chapple *et al*., 2013; Ballad *et al*., 2011). Although RSA is not as fast as a symmetric encryption, it is strong because it uses two large prime numbers. This algorithm derives both the public and private keys by multiplying two large prime numbers. While it is easy to multiply two numbers, it is extremely complex to factor the product of these two large prime numbers (Gregg, 2014; Gibson, 2012). The RSA algorithm was developed to resolve man-in-the-middle attacks (Chapple *et al*., 2013). For example, When the RSA is used in a PKI system, the cryptosystem generates a symmetric key using a symmetric algorithm such as AES. The cryptosystem encrypts the symmetric key with the receiver's public key. Only the receiver will be able to decrypt the message via the use of his/her private key and be able to retrieve the symmetric key. RSA key sizes can increase up to 4096 bits in length and cracking a key of this size requires an extraordinary amount of computer processing power and time (Gregg, 2014). The RSA cryptosystem can be found in many products, such as Microsoft Internet Explorer and Mozilla Firefox (Gregg, 2014).

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) has recently received a great deal of consideration due to the fact that not only does ECC require smaller key size and lesser bandwidth, but that also the computational cost and storage space is effectively

low (Hankerson *et al*., 2004). ECC is more efficient than typical asymmetric encryption methods such RSA because it takes less processing power, which is useful in hardware devices like cell phones and tablets (Gregg, 2014; Gibson, 2012)

Let p be a prime number, and let F_p denote the field of integers modulo p. An elliptic curve E over F_p is defined by an equation of the form

$$E: y^2 = x^3 + ax + b$$

Where a and b are elements of a finite field with p^n elements, where p is a prime larger than 3. A pair (x,y), where $x, y \in F_p$, is a *point* on the curve if (x, y) satisfies the equation above. The *point at infinity*, denoted by ∞, is also said to be on the curve. The set of all the points on E is denoted by $E(F_p)$.

The key exchange mechanism for ECC is constructed as the following (Hankerson *et al*., 2004):

A and ***B*** agree on an Elliptic Curve E (specified by the field F and parameters a, b) and a base point g on E.

(1) A secretly selects an integer x, then computes $X = xg$ and sends it to ***B***.

(2) B secretly selects an integer y, then computes $Y = yg$ and sends it to ***A***.

(3) A computes: $xY = x(yg) = xyg$.

(4) ***B*** computes: $yX = y(xg) = yxg = xyg$.

Now, ***A*** and ***B*** both share the point xyg which they can use to create a secret key. ECC maintains the same security level of the RSA cryptosystem, but with small key sizes, bandwidth savings and faster computation These features are desirable in most security applications where computational power and circuit space is limited, such as

smart cards and wireless devices (Yokoyama, 2000; Koblitz *et al.*, 2000; Ballad *et al*., 2011; Chapple *et al*., 2013). The French National Institute in Computer Science and Control tested the strength of ECC in early 2000. They used a distributed network of more than 9,500 computers and were able to brute force ECC and recover the 109-bit key that was used to encrypt a message. This only proves that it is hard to break ECC on a single machine and it would take almost 500 years to achieve (Gregg, 2014). However, if larger keys were used, it would take longer to crack it. Therefore, brute-force attacks are difficult to mount and they are extremely time-consuming and computationally intensive.

2.4 INTEGRITY

Integrity is another important pillar in information security, and can be recognised in different aspects. It can be thought as a way to detect errors and modifications and reflects the logical correctness (Andress, 2014; Gregg, 2014). For example, integrity ensures that information remains correct from the point it was created until it reaches the desired location. Integrity is significant for many organisations, especially during the exchange of sensitive or secret information that allows users to have confidence in its correctness. Therefore, integrity of information must be protected in storage and transit. Protecting integrity of information in storage can be accomplished by using access and audit controls as well as cryptography through hashing algorithms applications (Gregg, 2014). As for integrity in transit, information can be protected by applying security controls to the protocols, such as hashing and cryptography (Andress, 2014; Gregg, 2014).

2.4.1 CRYPTOGRAPHIC CONSIDERATIONS

To maintain integrity, using simple cryptographic techniques such as checksums help preventing unauthorised modification, forging or replaying messages. Integrity can be enforced by employing one or two of the integrity check methods. Session hijacking is one example of attack on the integrity.

2.4.1.1 Hash and Message Digest

What makes hash algorithms plausible is the noticeable improvement of performance and efficiency. For example, the hash value used in such algorithms is smaller than the original message. The same hash value is used to verify the integrity of the message.

The two most popular hashing algorithms are the Message-Digest algorithm family and Secure Hash Algorithm family. An example of each algorithm family is explained below:

- **MD5**: This produces a fixed 128-bit output and divides the data into blocks of 512 bits. MD5 digests are widely used for software verification and forensics to ensure that a downloaded file has been unchanged.
- **SHA-1**: This generates a 160-bit hash value and can be used as input to the digital signature algorithm for both generation and verification of message (Pachghar, 2015). However, SHA algorithms are considered less prone to collision due to the large message digest. Other examples of SHA are SHA-2 and the soon-to-arrive SHA-3

However, MD5 is considered faster when compared with SHA-1, but has been attacked and found to be less secure. MD5 is prone to collisions and it can be easy to generate. Being collision resistance is one of the main properties of hash function. The main properties of cryptographic hash functions defined as the following (Dong and Chen, 2012; Menezes *et al*., 2010):

1. *Pre-image resistance* — for essentially all pre-specified outputs, it is computationally infeasible to find any input which hashes to that output, i.e. to find any preimage *x'* such that *h(x') = y* when given any *y* for which a corresponding input is not known.
2. *2nd-pre-image resistance* — it is computationally infeasible to find any second input which has the same output as any specified input, i.e. given *x*, to find a 2nd pre-image *x' = x* such that *h(x) = h(x')*.
3. *Collision resistance* — it is computationally infeasible to find any two distinct inputs *x*, *x'* which hash to the same output, i.e. such that *h(x) = h(x')*. (Note that here there is free choice of both inputs.)

2.4.1.2 Message Authentication Code (MAC)

A message authentication code is a sophisticated type of keyed hash function that provides message authenticity by a symmetric technique. Menezes *et al*. (2010) and Stallings (2011) defined a message authentication code as an algorithm that takes two functionally distinct parameters - a message and a secret key - and produces a fixed-size output. The MAC helps to detect unauthorised changes in data transfer and provides integrity as well as verification of the message source. The MAC can be recognised as a cryptographic checksum that basically works as a hash function and

condenses a variable length message with a secret key to a fixed-sized authenticator or code. The MAC computation is performed as follows (Smart, 2008; Stallings, 2011):

$$code = MAC_k(m)$$

Where

- MAC is the check function,
- k is the secret key,
- m is the message.

2.4.1.3 Hashed Message Authentication Code (HMAC)

Hashed message authentication code is a strong integrity method that employs a symmetric encryption with a hash algorithm. It detects any changes in the cleartext but it cannot stop attackers changing the contents of the original data. The HMAC computation is performed as follows (Ramkumar, 2014):

$$code = MAC_K(m) = H((K \oplus Po) \,||\, H((K \oplus Pi) \,||\, M))$$

Where:

H is a cryptographic hash function,

K is the shared key by the sender and receiver

Po *is the standard outer pad and* $Po = 0x5c5c\ldots5c5c$

Pi *is the standard inner pad and* $Pi = 0x3636\ldots3636$

M is the message to be authenticated,

|| denotes concatenation,

⊕ denotes exclusive or (XOR),

The two parties involved in the process must pre-share a secret key. First, the sender performs XOR twice to combine the secret key once with the outer pad and another inner pad, and then combines the result with plaintext and hashes the output using

algorithms like MD5 or SHA-1. Finally, the hash code is combined with the secret key again to create an HMAC. Once the receiver receives the HMAC, he performs the same process locally and compares the result of computed HMAC with the sender's HAMC. If the two values match, the sender is authenticated and the message's integrity is assured (Ramkumar, 2014; Conrad, 2012). An example protocol that employs HMAC for data integrity is the SSL protocol (Stapleton, 2014).

2.4.1.4 Digital Signature

Digital signature is an application of asymmetric encryption that provides authentication. It validates the integrity of the data and the sender. The following steps illustrate the mechanism of digital signature (Gregg, 2014; Stapleton, 2014):

1. ***A*** produces a message digest by passing a message through a hash algorithm.
2. The message digest is then encrypted using ***A***'s private key.
3. The message is forwarded, along with the encrypted message digest to the recipient ***B***.
4. ***B*** creates a message digest from the message with the same hashing algorithm that ***A*** used. ***B*** then decrypts ***A***'s signature digest by using ***A***'s public key.
5. Finally, ***B*** compares the two message digests - the one originally created by ***A*** and the other that was created by it. If the two values match, ***B*** has proof that the message is unaltered and did come from ***A***.

2.5 NON-REPUDIATION AND AUTHENTICITY

These two properties are used to ensure that a sender of data is provided with proof of delivery and the recipient is assured of the sender's identity. Today, the Internet makes it difficult to trust others without knowing whom we are dealing with. That is why non-repudiation became very critical. Non-repudiation is a set of controls necessary to prevent repudiation. It is a method to ensure that individuals cannot later deny their own actions and it can be thought of as a combination of integrity and authentication controls that have to be verified by a third party. Non-repudiation is achieved through digital signatures, digital certificates, and message authentication codes (Gregg, 2014; Stapleton, 2014). Authentication is a method that enables one to verify the identity of individuals. Authentication includes proactive controls including methods for single, mutual, and multifactor authentication. It involves knowledge, possession, biometrics and cryptographic factors. Passwords, tokens, PINs and biometrics are common examples for person authentication. Authentication is related to integrity and the same cryptographic considerations of integrity applied to authentication. Authenticity can be achieved through MAC, HMAC, digital signature and trusted time stamps. For example, MAC can be used for authenticity since the sender and the receiver share the same key. Authenticity is also necessary in asymmetric public keys to prevent adversarial modification.

2.6 AUTHENTICATION PROTOCOLS

Authentication protocols often use cryptographic protocols and they are essential in real world applications. Various protocols have been proposed to provide mutual authentication and key establishment security (Dong and Chen, 2012). Moreover,

authentication protocols are prone to errors and flaws which make it difficult to detect sometimes. Many protocols have been proved to be flawed even after a period of time of their publication. Chapter 3 discusses various examples of flawed protocols. However, therein lies the problem and question of whether the security of an authentication protocol is adequate and has been extensively studied to meet all the fundamental security measures. This thesis will introduce a new security protocol, which was theoretically proved secure against attacks. Furthermore, it will uncover some flaws found in the new protocol and suggest how to amend them and achieve security.

An authentication protocol is a protocol to provide one entity some degree of assurance about the identity of the entity with whom it is communicating. Both entities must follow a set of rules to achieve authentication. There are a number of different authentication mechanisms, but all serve this same purpose.

2.6.1 PUBLIC KEY INFRASTRUCTURE (PKI)

PKI is a framework that consists of a set of security services that enable the user to manage, create, store, and distribute keys and digital certificates (Stapleton, 2014; Stalling, 2011; Graves, 2010). In reality, PKI is highly reliable with a relatively sophisticated user infrastructure. It was developed to overcome the problem of exchanging keys among big groups. The component of the PKI framework include the following (Gregg, 2014; Stapleton, 2014):

- **Certificate authority (CA):** a function managed by a third party to issue certificates to authorised users. Basically, CA creates, signs and verifies the authenticity of certificates.

- **Certificate revocation list (CRL):** this list is maintained by CA to verify the accuracy and integrity of the digital certificates.
- **Registration authority (RA):** the RA cannot generate a certificate but it can accept requests, verify identities and passes these information to the CA for certificate generation. The purpose of RA is to reduce the load on the CA.
- **Certificate server:** this server keeps the database of stored certificates.
- **X.509 standard:** the accepted standard for digital certificates.

The technology behind PKI provides a true robust example of non-repudiation through digital certificates. It also invokes the sender to use their private key to encrypt messages to achieve confidentiality. However, one major issue affecting PKI is a compromised CA. If the attackers could convince a CA that they are legitimate users, the CA would issue them a certificate. Certificate management can be challenging. Sometimes vulnerabilities can be found in the protocol that is using PKI for example, the BEAST (2011), CRIME (2012), and Lucky13 (2013) attacks on SSL/TLS. Another weakness found in PKI based on OpenSSL is the Heartbleed vulnerability (2014). The Heartbleed is a recent vulnerability that can expose the original private key. This means both keys and certificate are likely to be compromised undetectably. Unfortunately, this small bug does not require any attack on cryptographic algorithms. In fact, it is the result of a simple bound check in the code that handles TLS (Meyer and Schwenk, 2014; Ristic, 2014; Zhang *et al*., 2014).

2.6.2 IDENTITY-BASED CRYPTOGRAPHY

The idea of identity-based cryptography was originally proposed by Shamir in 1984 but practical identity-based encryption schemes were not found until 2001 by Boneh

and Franklin. The idea behind identity-based cryptography is to eliminate the requirement of checking the validity of certificates in PKI. For example, using identities instead of digital certificates can save significant amounts of resources for computation and communications, and resolve scalability problems (Joonsang *et al*., 2015). The attractive benefits gained from applying identity-based cryptography draws researchers' attentions to test and implement this public key approach to different environments, such as in wireless sensors networks, grid computing, and digital rights management systems.

Mishra and Mukhopadyay (2013) proposed a certificateless authenticated key agreement protocol for Digital Rights Management (DRM) systems by utilising identity-based encryption. The main motivation of their research is to protect authorised digital contents and prevent illegal distribution by utilising identity-based encryption. They show that their protocol ensures flawless mutual authentication and that it establishes a session key between the user and the server. Their protocol eliminates the use of trust certificate authority, uses PKG-generated partial private key share, and self-generates secret values to solve key escrow problems (Mishra and Mukhopadyay, 2013).

Yussoff *et al*. (2012) proposed IBE-Trust protocols to confirm the trustworthiness of nodes in wireless sensor networks (WSN). They aimed to design a trusted platform and an energy efficient authentication protocol. Their protocol proves that it can establish trust in WSN with less computation and communication, and most importantly, eliminates the need for neighbouring evaluation for trust management systems (TMS) (Lopez *et al*., 2010), or relying on external security chips.

Recent research on gird computing has focused on implementing identity-based cryptography into gird security architectures since the majority of current grid

systems use PKI to securely authenticate grid users. Lim and Paterson (2011) proposed a customised identity-based key agreement protocol that is compatible with the Grid Security Infrastructure (GSI). Their new protocol provides a more lightweight secure job submission environment for grid users. The analysis shows that the computational costs in Lim and Paterson's proposal are approximately less costly when compared with PKI. In terms of communication costs, their scheme appears to be significantly more lightweight and less bandwidth-consuming than PKI because of its certificate-free nature and small key sizes (Lim and Paterson, 2011).

Nicanfar *et al*. (2014) propose an efficient scheme that provides mutual authentication based on identity-based cryptography for secure smart grid communication. Their protocol is capable of preventing various attacks such as an unknown key-share attack and insider attacks, while reducing the management overhead. Their scheme shows an improvement in key management by periodically refreshing public and private key pairs as well as utilising smaller key sizes and reducing resource consumption in the system (Nicanfar *et al*., 2014).

Joonsang *et al.* (2015) proposed a secure cloud computing-based framework for big data information management called "Smart-Frame". The main idea behind this framework is to develop a hierarchical structure of cloud computing centres at three levels to provide different types of computing services for information management and big data analysis. Furthermore, the security of this framework is based on identity-based encryption, signature and proxy re-encryption. The scheme achieved scalability, flexibility and data confidentiality (Joonsang *et al.,* 2015).

In light of that, previous research showed that replacing PKI with identity-based infrastructure could offer an alternative security infrastructure with lightweight computation.

2.7 SUMMARY

Computer security revolves around the protection, prevention and detection of any unauthorised use of all data as well as computer systems. Information security is achieved through a process that is a combination of three aspects. It seeks to prevent unauthorised access (confidentiality) or modification (integrity) of data while maintaining access to resources (availability). Moreover, this chapter presents an overview of the controls available to protect information and examining some of the controls in detail. Table (2.1) maps the security method to achieve certain security aspects.

Table 2.1 Cryptography services summary

Confidentiality	Integrity	Authentication	Non-repudiation
Encryption	MAC HMAC Digital signature	MAC HMAC Digital signature	Digital Signature

Table 2.2 provides a comparison summary of symmetric algorithms and asymmetric algorithms attributes. Even though encryption is an important tool in computer security, encryption does not solve all computer problems. Protection of data can be achieved through the combination of encryption and integrity protection techniques. Thus, it is important to implement a combination of the controls to secure valuable information and resources. Furthermore, this chapter presents the most recent application of identity-based cryptography and research suggests it can be a good authentication infrastructure in term on fast communication and low cost.

Table 2.2 Symmetric versus Asymmetric attributes

Attribute	Symmetric Algorithms	Asymmetric Algorithms
Keys	One key is shared between two or more entities	Public key is available to all. Private key is kept secret to the owner and never shared
Example algorithms	Des, 3DES, AES	RSA, ECC, Diffie-Hellman
Key exchange	Requires sharing keys in advance through another secure mechanism	Easy to deliver public key
Encryption speeds	Fast	Slower
Security services provided	Confidentiality, integrity and authentication	Confidentiality, integrity, authentication and no-repudiation

3

Design Analysis

One cannot appreciate the technical details underlying security protocol without understanding the services it provides. This chapter reviews the original concept of identity-based cryptography, discusses biometric verification systems briefly, and highlights various attacks that communication protocols may encounter. Finally, it examines the available simulation tools.

3.1 IDENTITY-BASED ENCRYPTION

In order to introduce ID-Based Encryption to distributed systems, an initial review of the current literature is required to provide an overview of the related topics. The idea of identity-based cryptography was originally proposed by Shamir in 1984 but practical identity-based encryption schemes were not found until recently. Several proposals have been made to tackle these problems and to improve the IBE scheme.

In 2001, Boneh & Franklin developed a fully functional ID-based encryption scheme, which can be constructed efficiently by using Weil pairing on elliptic curves. The PKG in this scheme can be distributed so that the master key is never available in a single location. This scheme based its security under the bilinear Diffie-Hellman assumption:

"Let G_1; G_2 be two groups of prime order q. Let $\hat{e}$: $G_1 X G_1 \rightarrow G_2$ be an admissible bilinear map and let P be a generator of G_1. The BDH problem in $<G_1, G_2, \hat{e}>$ is as follows:

Given $<P, aP, bP, cP>$ for some $a, b, c \in Z^*_q$ compute $W = \hat{e}(P; P)^{abc} \in G_2$."

According to Boneh & Franklin (2001), there are four algorithms: Setup, Extract, Encrypt, and Decrypt called "BasicIdent". These algorithms are defined as the following:

- **Setup**

Given a security parameter $k \in Z^+$ and letting g be some parameter generator, the algorithm works as follows:

(1) Run g on input k to generate two groups G_1, G_2 of some prime order q and an admissible bilinear map $\hat{e}$: $G_1 X G_1 \rightarrow G_2$

(2) Select a random $s \in Z^+$ and set $P_{pub} = sP$, where s is the master key picked at random and its public key computed.

(3) Choose a cryptography hash function:

$H_1: \{0, 1\}^* \rightarrow G_1$ (extract point from ID)

$H_2: G_2 \rightarrow \{0, 1\}^n$ for some n, (where n is the length of a plaintext message)

The message space is $\mathcal{M} = \{0, 1\}^n$ and the ciphertext space is $C = G_1 X \{0, 1\}^n$. The system parameters are prams= $<q, G_1, G_2, \hat{e}, n, P, P_{pub}, H_1, H_2>$.

❖ **Extract**

For a given string $ID \in \{0, 1\}^*$, the algorithm does:

(1) Computes $Q_{ID} = H_1(ID) \in G_1$

(2) Sets the private key $d_{ID} = sQ_{ID}$, where s is the master-key

❖ **Encryption**

To encrypt $M \in \mathcal{M}$ under the public key *ID*:

(1) Compute $Q_{ID} = H_1(ID) \in G_1$

(2) Choose a random $r \in Z_q$

(3) Set the ciphertext to be

$$C = < rP, M \oplus H_2(g_{ID})^r >, \text{where } g_{ID} = \hat{e}\,(Q_{ID}, P_{pub}) \in G_2$$

❖ **Decryption**

Let $C = < U, V > \in C$ be a ciphertext encrypted using the public key *ID*. To decrypt C using the private key $d_{ID} \in G_1$, compute:

$$V \oplus H_2(\hat{e}(d_{Id}, U)) = M$$

In ID-Based cryptosystems, there is a trusted third party called the Private Key Generator (PKG), which is responsible for generating the secret keys for all users. As a result, a PKG holds the users' private keys. If a PKG is malicious, it can impersonate any user and therefore decrypt any cipher text or forge a signature on any message. This fact can lead to a problem known as the key escrow (Liao *et al.*, 2005; Yuen *et al.*, 2010).

The concept of Hierarchical Identity-Based Encryption (HIBE) was first introduced by Horwitz and Lynn (2002) and a fully practical HIBE system was proposed by Gentry and Silverberg (2002). The latter scheme was an extension of the Boneh-Franklin IBE scheme and its security is based on the Bilinear Diffie-Hellman assumption in the random oracle model (Boneh and Franklin, 2001). Gentry and Silverberg demonstrated how a root PKG in HIBE could distribute the workload by delegating private key generation and identity authentication to lower-level PKGs, which, in turn, are responsible for generating the private keys for users in their domains on the next level. In an HIBE scheme, the identities are organised in a hierarchy tree as shown in Figure 3.1. Later, Boneh and Boyen (2004) constructed an efficient HIBE with a weaker notion of security without the random oracle model. Boyen and Waters (2006) presented an anonymous HIBE without random oracles. The system, which works with small ciphertext, is efficient and practical and it is proved to be secure by using a standard model based on the linear assumption in bilinear groups.

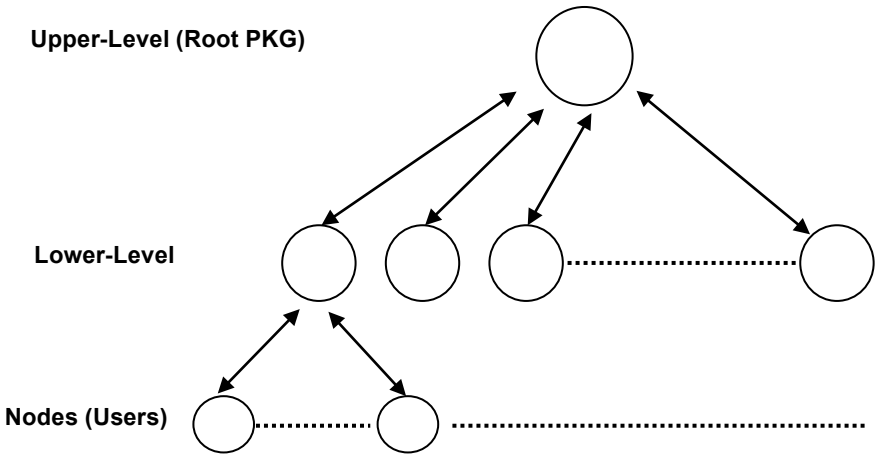


Figure 3.1: Hierarchical architecture for ID-Based Encryption

Another approach to address the key escrow problem is a Certificateless Public-Key Cryptosystem (CL-PKC). This paradigm is a strong security model and was established by Al-Riyami and Paterson in 2003. The concept of the CL-PKC scheme is that the user's private key is not only generated by the Key Generation Centre (KGC), it is also a combination of some contribution of KGC (called partial-private-key) and some user-chosen secret. Zhang *et al.* (2006) proposed a security model for certificateless public-key signatures based on *n*-bilinear pairings and showed that the scheme is equivalent to the computational Diffie-Hellman problem in the random oracle model (Boneh and Franklin, 2001).

3.1.1 Review of He et al.'s Scheme

He *et al*. (2012) proposed an ID-based remote mutual authentication with a key agreement scheme on ECC. This proposal attempts to cope with many of the well-known security problems such as know session key security and perfect forward secrecy.

The security of He *et al*.'s scheme is based on the intractability of two mathematical problems on elliptic curves: the computational Diffie–Hellman assumption (CDHA) and collision attack assumption 1 (k-CAA1). The protocol is divided into three phases: system initialisation phase, client registration phase and mutual authentication with key agreement phase.

System Initialisation Phase

S generates parameter of the system. First, *S* selects an elliptic curve equation *E, a* base point *P* with the order n over E, the master key *x* and computes public key $Ps = xP$. Next, the server chooses three secure one-way hash functions $H_1(\cdot), H_2(\cdot), H_3(\cdot)$ and a message authentication code $MAC_k(m)$. Finally, the server publishes $(F_p, E, n, P, Ps, H_1, H_2, H_3, MAC_k(m))$ but keeps x private.

Client Registration Phase

First, C_i submits his/her identity ID_{C_i} to *S*. Next, ***S*** computes $h_{Ci}=H_1(ID_{C_i})$ and the client's private key/public key $D_{C_i} = (x+ h_{Ci}))^{-1}.P$ and $P_{Ci} = (h_{C_i}+x).P = h_{C_i}P+PS$ and returns the private key along ID_{C_i} to C_i via secure channel. Finally, C_i validates the private/public key pair (D_{C_i}, P_{C_i}) by checking whether the equation $P_{C_i} = (h_{C_i}+x).P = h_{C_i}P+PS$ holds.

Mutual Authentication with Key Agreement Phase:

(1) The client C_i chooses a random number $r_{C_i} \in Z_n^*$, and computes $M = r_{C_i} \cdot P$, $M' = r_{C_i} \cdot D_{C_i}$. Then C_i computes $k = H_2(ID_{C_i}, T_{C_i}, M, M')$, where T_{C_i} is a timestamp.

Finally, C_i sends a service request message $M_1=\{ID_{Ci}, T_{C_i}, M, MAC_k(ID_{C_i}, T_{C_i}, M)\}$ to the server.

(2) After receiving M_1, S checks the validity of ID_{C_i} and the freshness of T_{C_i} and computes $h_{C_i}=H_1(ID_{C_i})$, $M'=(x+h_{C_i})^{-1}.M$ and $k=H_2(ID_{C_i}, T_{C_i}, M, M')$. Then, S checks the integrity of $MAC_k(ID_{C_i}, T_{C_i}, M)$ with the key k. S chooses a random number $r_S \in Z_n^*$, and computes $W = r_S \cdot P$, $KS = r_S \cdot M$ and the session key $sk= H_3(ID_{C_i}, T_{C_i}, T_S, M, W, K_S)$. Then S sends $M_2=\{ID_{Ci}, T_S, W, MAC_k(ID_{C_i}, T_S, W)\}$ to C_i, where T_S is a timestamp.

(3) C_i checks the integrity of $MAC_k(ID_{C_i}, T_S, W)$ with the key k and computes $K_{C_i}=r_{Ci}\cdot W$ and the session key $sk=H_3(ID_{C_i}, T_{C_i}, T_S, M, W, K_{C_i})$.

Protocol 3.1 summaries the authentication and key agreement steps of He *et al.*'s protocol.

Client		***Server***
$r_{C_i} \in Z_n^*$ $M = r_{C_i} \cdot P$ $M' = r_{C_i} \cdot D_{C_i}$ $k=H_2(ID_{C_i}, T_{C_i}, M, M')$	$M_1=\{ID_{Ci}, T_{C_i}, M,$ $MAC_k(ID_{C_i}, T_{C_i}, M)\}$ →	$h_{C_i}=H_1(ID_{C_i})$, $M'=(x+h_{C_i})^{-1}.M$ $k=H_2(ID_{C_i}, T_{C_i}, M, M')$ S checks the integrity of $MAC_k(ID_{C_i}, T_{C_i}, M)$ $r_S \in Z_n^*$ $W = r_S \cdot P$, $KS = r_S \cdot M$ $sk= H_3(ID_{C_i}, T_{C_i}, T_S, M, W, K_S)$
C_i checks the integrity of $MAC_k(ID_{C_i}, T_S, W)$ $K_{C_i}=r_{Ci}\cdot W$ $sk=H_3(ID_{C_i}, T_{C_i}, T_S, M, W, K_{C_i})$	← $M_2=\{ID_{Ci}, T_S, W,$ $MAC_k(ID_{C_i}, T_S, W)\}$	

Protocol 3.1: The He *et al.*'s authentication protocol

Cryptanalysis of He et al.'s Scheme

He *et al*. claimed that their scheme provides resilience against many cryptographic attacks. However, researchers Wang *et al.* (2013) and Islam *et al*. (2012) proved that their scheme fails to protect a user's anonymity, known session-specific temporary attacks, privileged-insider attacks, and many logged-in users' attacks and has no provision for leaked key revocation phase.

This protocol attempts to cope with many of the well-known security and efficiency problems. However, the scheme has a potential flaw that may lead to man-in-the-middle attacks and impersonation attacks (Wang *et al.*, 2013; Islam *et al.*, 2012). It can be seen that if an attacker E eavesdrops and listens to the communication between $\boldsymbol{S}$ and $\boldsymbol{C_i}$, then, E can intercept a valid login request $M_1=\{ID_C, T_C, M, MAC_k(ID_C, T_C, M)\}$ or $h(ID \,||\, Xs)$ and masquerade as a legal user.

3.2 BIOMETRIC VERIFICATION SYSTEMS

Biometric technology and verification systems offer a number of benefits to distributed systems and their users (Jain *et al.*, 2015). Biometrics are automated methods and are used to recognise a person based on a physiological or behavioural characteristic. Biometric technologies are becoming a fundamental element to ensure highly secure identification and personal verification solutions (Jain *et al.*, 2015). Biometric keys can be extracted from keystroke patterns (Monrose *et al.*, 1999), fingerprints (Seto, 2002; Clancy *et al.*, 2003), handwritten signatures (Hao *et al.*, 2002), the human voice (Monrose *et al.*, 2001), and facial characteristics (Goh and Ngo, 2003); each method being unique to a greater or lesser extent.

An accurate and reliable authentication is needed in distributed systems as the level of security breaches increases. Biometric technologies are able to provide a highly secure identification and verification system through something that you possess individually, such as fingerprints. That is why it is considered to be a unique feature of individuals. The probability of two people sharing the same biometric data is virtually nil. As a result, they cannot be shared or cannot be lost unless in the case of a serious accident. Moreover, adopting and utilising biometrics for personal authentication is becoming more convenient for both public and private sectors, because it can help to combat credit card and transaction fraud, prevent identity theft, restore identity, enhanced security, data verification and authentication (Abidin *et al*., 2014; Jain *et al.*, 2015).

Combining ID based cryptography with biometric techniques can effectively improve the security in authentication systems, which provides a reliable identity with a high degree of assurance. The biometric technology is regarded as a powerful solution due to its unique link to identify individuals, which is somehow impossible to fake. Thus, a biometric identity is an inherent trait, which will always remain with the person all the time. In another words, using biometric techniques in IBE will mean that the person will always have their identification handy.

However, irrevocability is the most severe concerns in security engineering aspects. Biometric features are inherent in individuals, therefore, they cannot be changed easily once they are exposed or compromised Abidin *et al*., 2014; Jain *et al.*, 2015). A related problem is "*key diversity*", for example, an individual prefers to have separate keys for their bank account and for access to their workplace computer, so that they can revoke one without affecting the other (Hao *et al.*, 2005).

On the other hand, one of main obstacles to this powerful technique is that biometric measurements are proved to be noisy by nature while cryptography demands correctness in keys otherwise the protocols would fail. In light of that, deploying biometric measurements in the existing IBE systems directly can be difficult because most attempts have suffered from an excessive False Rejection Rate (FRR), usually over 20%, which is unacceptable for practical applications (Hao *et al*., 2005; Bissessar *et al*., 2016).

Moreover, biometric data suffers from a low level of secrecy or not being very secretive. For instance, people leave fingerprints everywhere and iris images can be captured by hidden camera. Overall, the more a biometric is used, the less secret it will be. It would be unwise to depend on a biometric alone, especially if that biometric becomes used on a global scale. Social acceptance is necessary to biometric technology and it tends to be a primary measure of success. The fear of potential misuse of biometric data may make the public hesitant to use systems that rely on it. Also, compromised biometric templates pose serious security and privacy issues (Abidin *et al*., 2014; Jain *et al.*, 2015; Bissessar *et al*., 2016).

3.2.1 Review of Li-Hwang's Scheme

Li and Hwang (2010) proposed an efficient biometrics-based remote user authentication scheme using smart cards. The security of their scheme is based on a one-way hash function, biometrics verification, smart card and nonce. The scheme is very efficient in computation of costs, which have been proved to be relatively low compared with other related schemes, such as Lin-Lai scheme (2002), Lee-Chiu scheme (2005), Chang *et al.'s* scheme (2006).

Li-Hwang's scheme is composed of four phases, namely the registration phase, the login phase, the authentication phase and the password change phase. In their scheme, there are three participants, the registration centre ($\boldsymbol{R}$), the server ($\boldsymbol{S_i}$) and the user ($\boldsymbol{C_i}$), where $\boldsymbol{R}$ is assumed to be a trusted party. $\boldsymbol{R}$ chooses the master secret key Xs and distributes it to $\boldsymbol{S_i}$ via a secure channel.

Registration Phase

First, the client $\boldsymbol{C_i}$ submits personal biometrics B_i and the password PW_i, identity ID_i to the registration centre R_i. Then, R_i computes $r_i = h\ (PW_i \,||\, h(B_i))$ and $e_i = h\ (ID_i \,||\, Xs) \oplus h(PW_i \,||\, f_i)$ where Xs is secret information generated by the server. After storing $\{ID_i, h\ (.), f_i, e_i\}$ on the user's smart card, $\boldsymbol{R_i}$ sends it to the user via a secure channel.

Login Phase

When the user $\boldsymbol{C_i}$ wants to logon to a remote server, he inserts his smart card into the card reader and submits the personal biometrics, B_i, if $h(B_i) = f_i$. The Smart card requires $\boldsymbol{C_i}$ to input the PW_i and computes $r`_i = h(PW_i \,||\, f_i)$, $M_1 = e_i \oplus r`_i = h(ID_i \,||\, Xs)$, $M_2 = M_1 \oplus Rc$, where Rc is a random number generated by the user. Finally $\boldsymbol{C_i}$ sends the message (ID_{C_i}, M_2) to the server $\boldsymbol{S_i}$.

Authentication Phase

After receiving the request login message, $\boldsymbol{S_i}$ checks the format of ID_{C_i}, and then sends $M_5 = h(ID_i \,||\, Xs) \oplus Rs$ and $M_6 = h(M_2 \,||\, (M_2 \oplus h(ID_i \,||\, Xs))$ back to $\boldsymbol{C_i}$, where Rs is a random number generated by S_i. C_i verifies the validity $M_6 ? = H_4(M_2 \,||\, Rc)$, and sends back $M_8 = h(M_5 \,||\, (M_5 \oplus M_1))$ to $\boldsymbol{S_i}$. If $M_8 = h(M_5 \,||\, Rs)$. $\boldsymbol{C_i}$ and $\boldsymbol{S_i}$ authenticate each other successfully.

Password Changing Phase

First, C_i inserts the smart card and inputs B_i. After passing the biometric verification (i.e., $h(B_i) = f_i$), C_i is required to enter the old password PW_i, and the new password, new PW^n_i. Next, the smart card will compute: $r'_i = h(PW_i \,||\, f_i)$, $e'_i = e_i \oplus r'_i = h(ID_i \,||\, Xs)$, $e''_i = e'_i \oplus h(PW^n_i \,||\, f_i)$. Finally, the e_i is replaced with e''_i on the smart card.

Protocol 3.2 summaries the authentication steps in Li-Hwang protocol.

Client		***Server***
$r`_i = h(PW_i \,||\, f_i)$ $M_1 = e_i \oplus r`_i$ $M_2 = M_1 \oplus Rc$	(ID_C, M_2) →	$M_5 = h(ID_i \,||\, Xs) \oplus Rs$ $M_6 = h(M_2 \,||\, (M_2 \oplus h(ID_i \,||\, Xs))$
$M_6 ? = h(M_2 \,||\, Rc)$, $M_8 = h(M_5 \,||\, (M_5 \oplus M_1))$	← (M_5, M_6) → (M_8)	$M_8 ? = h(M_5 \,||\, Rs)$.

Protocol 3.2: The Li-Hwang authentication protocol

Cryptanalysis of Li-Hwang's scheme

Researchers Li *et al.* (2011) and Jeon *et al.* (2011) showed that Li and Hwang's scheme is vulnerable to various attacks such as replay attacks and man-in-the-middle attacks. And it showed weakness to the password-changing scheme. Also, it fails to provide proper authentication. One of the key characteristics of the cryptographic hash function is that the outputs are very sensitive to small perturbations in their inputs. Hash functions cannot be applied directly when the input data is with noise

such as biometrics (Vacca, 2007; Bissessar *et al*., 2016). Therefore, a secure one-way hash function cannot be used for biometric verification.

In the login phase of Li-Hwang's scheme, the user computes $h(B_i)$ based on the personal biometric template B_i. Then, the biometric authentication process relies on comparing the hash value $h(B_i)$ with f_i. However, the scheme does not seem to be able to handle natural variations in the biometrics. For example, when the user logs in, his fresh biometric sample has to match exactly the template recorded during the registration phase, which never happens in practice. Thus, the protocol is fundamentally flawed and does not fulfil the basic objectives of a biometric authentication protocol. As a result, this may prevent a legal user to pass biometric verification at the login phase. So, Li-Hwang's scheme is vulnerable to denial-of-service attacks.

In addition, Li-Hwang's scheme is prone to man-in-the-middle attacks. In the login phase, when the user $\boldsymbol{C_i}$ sends the login request (ID_i, M_2) to the server $\boldsymbol{S_i}$, an attacker $\boldsymbol{A}$ may eavesdrop the login message and then start another session with S_i and send both messages (ID_i, M_{A2}), (ID_i, M_2) to $\boldsymbol{S_i}$. Upon receiving (ID_i, M_{A2}) and (ID_i, M_2), $\boldsymbol{S_i}$ generates two random numbers R_S and R_{AS} and computes the following (Jeon *et al*., 2011):

$M_3 = h\ (ID_i \,||\, Xs)$, $M_4 = M_2 \oplus M_3$, $M_5 = M_3 \oplus R_S$, $M_6 = h\ (M_2 \,||\, M_4)$ and $M_{A3} = h\ (ID_i \,||\, Xs)$, $M_{A4} = M_{A2} \oplus M_{A3}$, $M_{A5} = M_{A3} \oplus R_{AS}$, $M_{A6} = h\ (M_{A2} \,||\, M_{A4})$. Then, $\boldsymbol{S_i}$ sends the message (M_5, M_6) and (M_{A5}, M_{A6}) for the two sessions respectively. It is worth noting that $M_{A3} = M_3$, $M_{A4} = M_4$, $M_{A5} = M_3 \oplus R_{AS}$, $M_{A6} = h\ (M_2 \,||\, M_4) = h\ (M_{A2} \,||\, M_{A4})$. In the meantime, $\boldsymbol{A}$ captures (M_5, M_6) and (M_{A5}, M_{A6}) and sends the fabricated message $(M'_5, M'_6) = (M_{A5}, M_{A6})$ to $\boldsymbol{C_i}$. After receiving (M'_5, M'_6), $\boldsymbol{C_i}$

verifies $M'_6 = H_4(M_2 \,||\, Rc)$, which in this case is $M'_6 = M_{A6} = h\,(M_2 \,||\, M_4) = h\,(M_2 \,||\, R_C)$. So $\boldsymbol{S_i}$ is successfully authenticated by $\boldsymbol{C_i}$. Then $\boldsymbol{C_i}$ computes $M_7 = M'_5 \oplus M_1 = R_{AS}$, $M_8 = h\,(M'_5 \,||\, M_7) = h\,(M_{A2} \,||\, R_{AS})$ and sends M_8 to $\boldsymbol{S_i}$. *A* intercepts M_8 and sends the message $M_{A8} = M_8$ to $\boldsymbol{S_i}$. After receiving M_{A8}, $\boldsymbol{S_i}$ verifies the equation $h(M_{A5} \,||\, R_{AS}) = M_8$. Thus, $\boldsymbol{A}$ is successfully authenticated by $\boldsymbol{S_i}$ masquerading $\boldsymbol{C_i}$. From this description, Li-Hwang's scheme is vulnerable to man-in-middle-attacks and impersonation attacks. The attacker can cheat the server by impersonating the user or can impersonate the server to cheat the user without knowing any secret information (Li *et al.*, 2011).

3.3 SECURITY ATTACKS

Security attacks can be achieved in different ways but they all lead to the goal of obtaining disclosed private information or exhausting the resources to deny legitimate users to gain access and use them. Security attacks may be conveniently classified into three categories. These are *physical attacks*, *passive attacks*, and *active attacks* as illustrated in Figure 3.2.

In a physical attack, an attacker can gain physical entry to organisation premises by pretending to be an employee or valid user and, in this way, gets inside the facility. This mischievous act allows the attacker to steal equipment or gather information from trashcans, desktops, or computer systems, or steal confidential documents that are not stored in a secure location. Moreover, the attacker can plug in any hardware keylogger to a PC or plant viruses or Trojans directly on the target system. That is why organisations need to enforce security policies and restriction access (Graves, 2010).

In a passive attacks, the attacker sniffs or monitors transmitted traffic. The attacker's main purpose is to obtain valuable information about the entities involved in the process. This attack is difficult to detect because the attacker does not affect the normal execution of protocols (Jahankhani, 2010; Stallings, 2011) but breaches confidentiality. Examples of this attack include: preforming network analysis, eavesdropping, traffic analysis, port scanning, and monitoring of unprotected communications. Passive attacks can be formed in two types. The first type is monitoring and reading the release of message contents. An attacker can acquire sensitive or confidential information by listening to a telephone conversation, reading electronic mail messages, or observing transmitted confidential data.

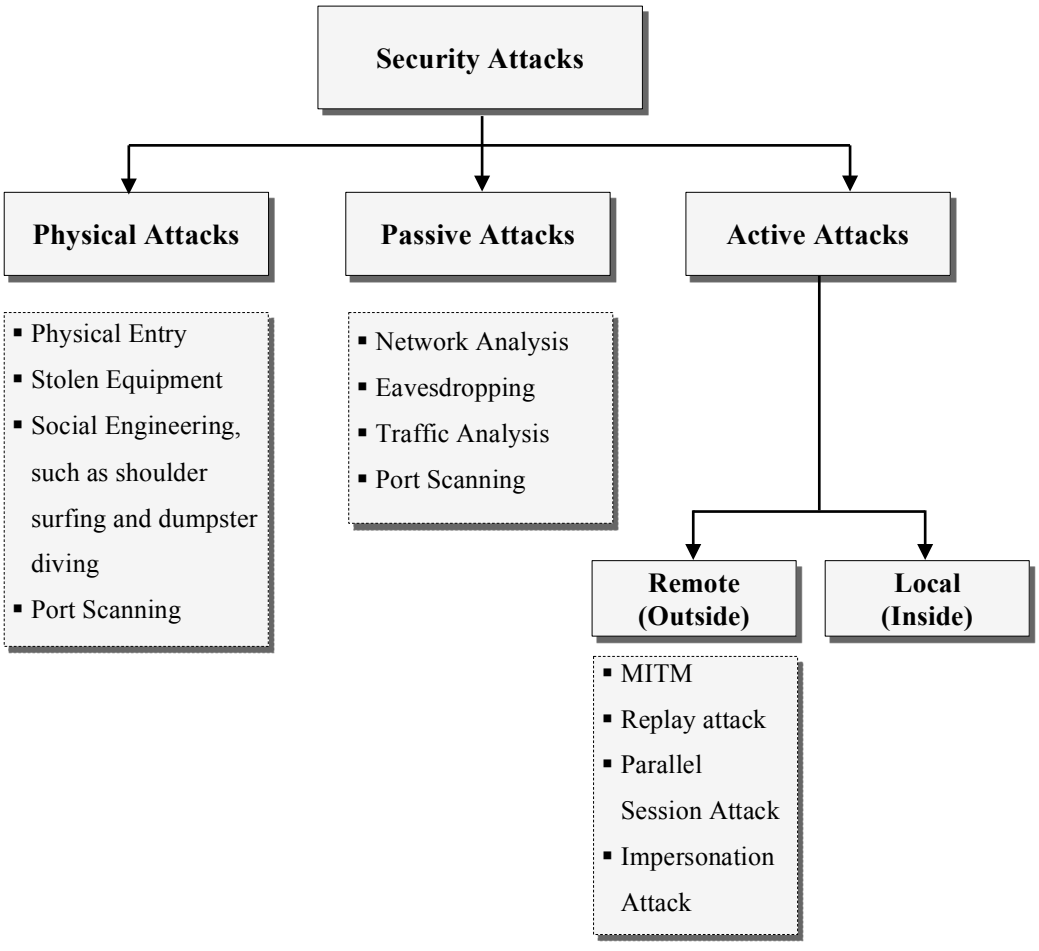
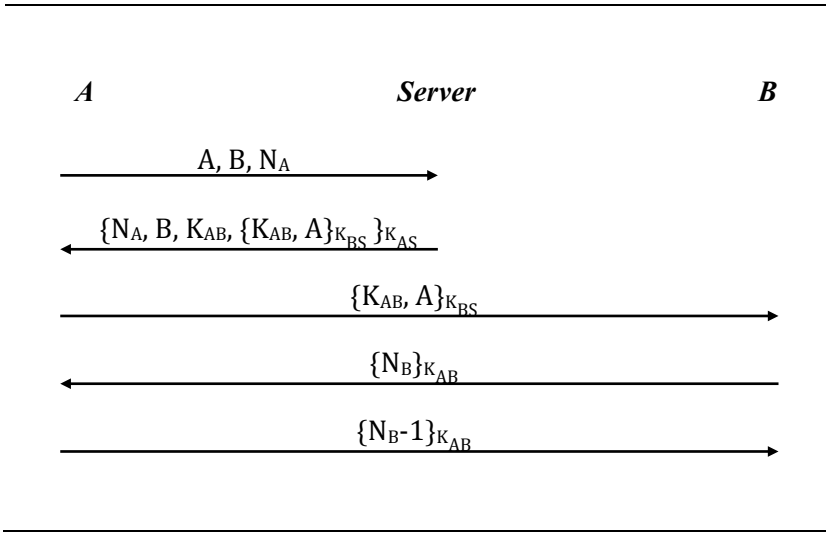


Figure 3.2: The classifications of security attacks

In active attacks, the attacker may modify the intercepted data, delay, delete or create a false message. This type of attack affects the availability, integrity, and authenticity of data (Graves, 2010), and takes many forms. For example, impersonation attacks, replay attacks, man-in-the-middle attacks, reflection attacks, parallel session attacks and denial-of-service attacks. To understand these possible attacks, this section includes, but is not limited to, the most relevant attacks on authentication protocols.

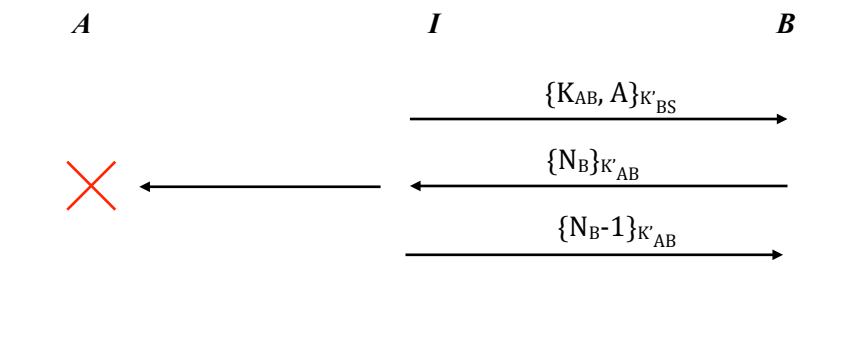
3.3.1 Replay Attacks

A replay attack occurs when the attacker intercepts a valid message and replays it again in a fraudulent way to sabotage a communication channel (Boyed and Mathurua, 2006; Gurtov, 2008). A very clear example of this attack can be found in the Needham-Schroeder secret key authentication protocol (Needham and Schroeder, 1978). The protocol achieves mutual authentication between two principals, $\boldsymbol{A}$ and $\boldsymbol{B}$, through a trusted third part server. First, $\boldsymbol{A}$ requests a session key from the server to communicate with $\boldsymbol{B}$. Then, the server generates the key and sends it to $\boldsymbol{A}$. Finally, $\boldsymbol{A}$ and $\boldsymbol{B}$ perform entity authentication and key confirmation (Clark and Jacob, 1997). The corresponding steps of this protocol are described in Protocol 3.3.



Protocol 3.3: The Needham-Schroeder secret key authentication protocol

Denning and Sacco (1981) identified that the protocol is vulnerable to a replay attack and demonstrated the attack as shown in Attack 3.1. An intruder ***I*** intercepts a successful run of the protocol that consists of the compromised session key *K*. Thus ***I*** knows *K* and $\{K_{AB}, A\}_{K_B}$. ***I*** masquerades as ***A*** to ***B*** and makes ***B*** accept this old and compromised session key ***K***. The flaw with this protocol is that there is no proof to guarantee the freshness of the message. According to Denning and Sacco (1981), the problem could be fixed by including the timestamps in the relevant messages.



Attack 3.1: Attack on The Needham-Schroeder secret key authentication protocol

3.3.2 MAN-IN-THE-MIDDLE ATTACKS

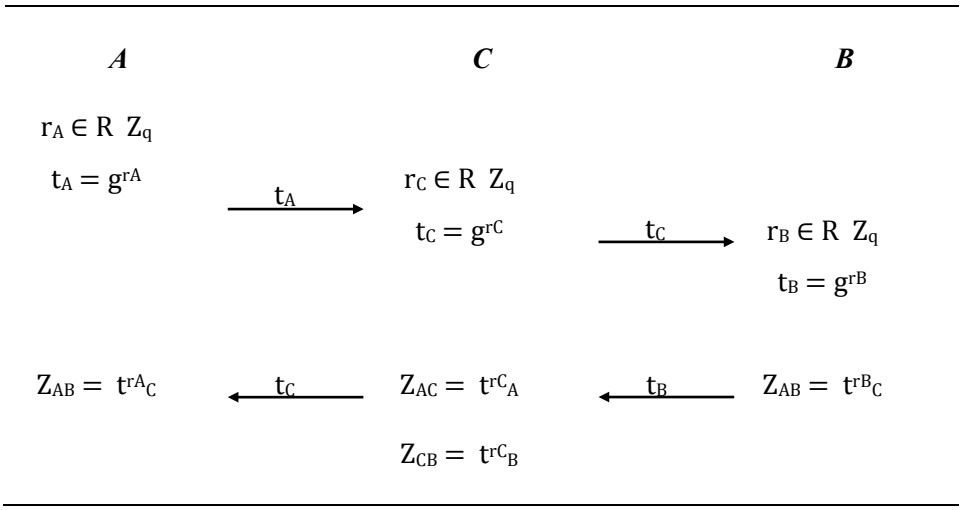
A man-in-the-middle (MITM) attack is a special form of impersonation attack (Gurtov, 2008). As implied by the name, the attacker imposes himself between two entities during the communication. MITM can be a passive attack if the attacker only forwards the packets between entities. However, if the attacker modifies, delays, or drops the packets it becomes an active attack. To illustrate this attack, consider the Diffie-Hellman protocol as shown in Protocol 3.4 (Boyed and Mathurua, 2006).

Shared information: Generator g of G

A		***B***
$r_A \in R\ Z_q$		
$t_A = G^{rA}$	$\xrightarrow{t_A}$	$r_B \in R\ Z_q$
		$t_B = G^{rB}$
$Z_{AB} = t^{rA}{}_B$	$\xleftarrow{t_B}$	$Z_{AB} = t^{rB}{}_A$

Protocol 3.4: The Diffie-Hellman key agreement

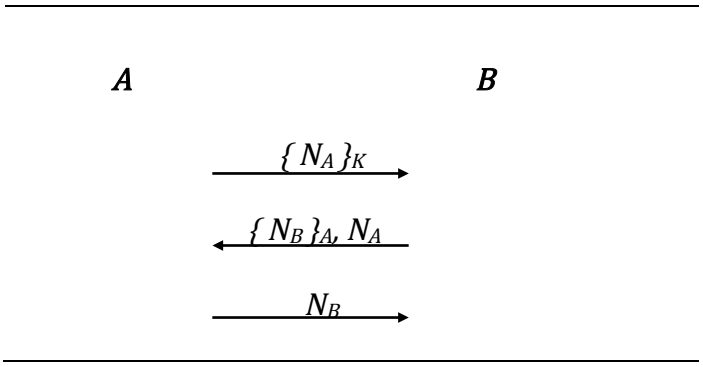
The absence of authentication of the message sent can lead to a MITM attack. Where the attacker $\boldsymbol{C}$ masquerades as $\boldsymbol{B}$ to $\boldsymbol{A}$ and masquerades as $\boldsymbol{A}$ to $\boldsymbol{B}$. Attack 3.1 shows how both $\boldsymbol{A}$ and $\boldsymbol{B}$ complete a normal run without knowing they both share keys with $\boldsymbol{C}$ (Boyed and Mathurua, 2006).



Attack 3.2: Attack on basic Diffie-Hellman key agreement

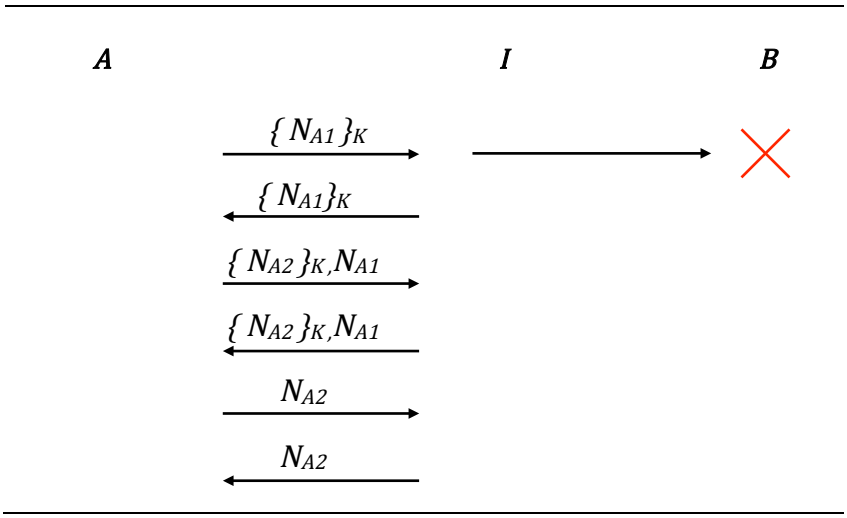
3.3.3 REFLECTION ATTACKS

This type of attack is a special case of replay attack, as the name implies. A malicious attacker reflects the message back at an honest agent. The idea of a reflection attack is to fool the challenge originator into providing the correct response to her\his message (Ryan and Schneider, 2001; Boyd and Mathuria, 2003). In order to demonstrate the execution of the attack, the basic protocol example first is described in Protocol 3.5, which is adopted from Boyd and Mathuria (2003). Suppose ***A*** and ***B*** are honest agents and share a secret *K*. N_A, N_B are nonces generated by ***A*** and ***B*** respectively for use in the protocol. This protocol is intended to achieve mutual authentication for both parties.



Protocol 3.5: A protocol vulnerable to reflection attack

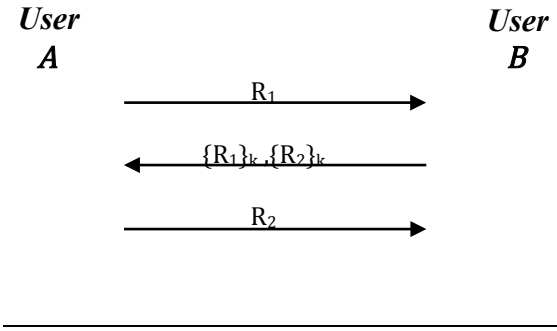
An adversary ***I*** can successfully complete two runs of the protocol as shown in Attack 3.3. ***I***(***B***) is an intruder who masquerades as ***B***. ***I*** intercepts the message $\{N_{A1}\}_K$ and reflects it back to ***A***. Then, ***A*** starts another run of the protocol with ***I*** and sends a response to ***I***. The reply allows ***I*** to deceive ***A*** by responding to the first message with ***A***'s reply and so on. As a result, the same challenge-response is used by ***A*** and ***I*** to authenticate each other (Boyd and Mathuria, 2003).



Attack 3.3: Reflection attack on Protocol 2.5

3.4.1 PARALLEL SESSION ATTACKS

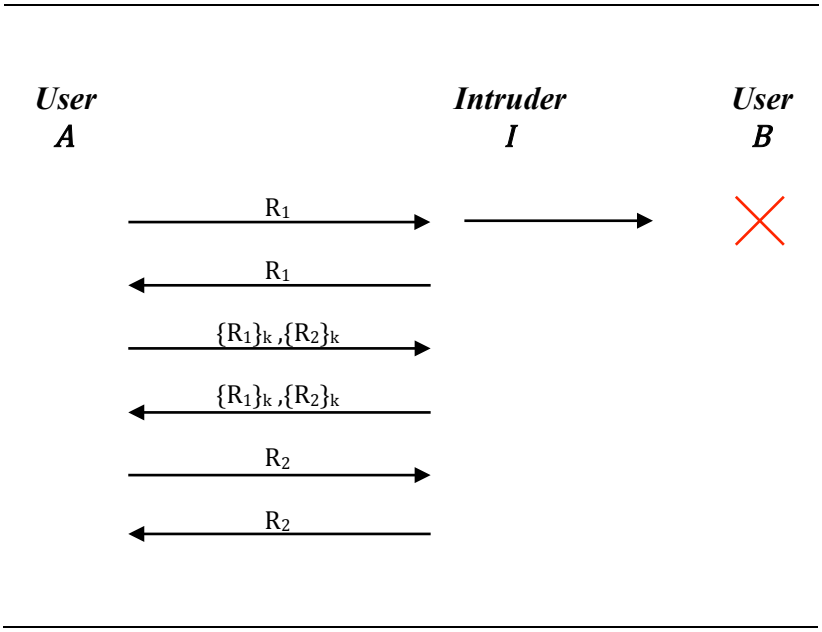
A parallel session attack is an example of interleaving attacks. It is conducted by subsequent interleaving replays among contemporaneous protocol sessions (Basagiannis *et al.*, 2007), where the attacker undertakes a passive role while manipulating protocol participants. In other words, the attack occurs when two or more protocol runs are executed concurrently and messages from one are used to form messages in another (Clark and Jacob, 1997). The ISO two-way authentication protocol is vulnerable to parallel session attack. Protocol 3.6 describes the ISO two-way authentication protocol without an attacker.



Protocol 3.6: The ISO two-authentication protocol

Attack 3.2 depicts how the parallel session attack performs on the ISO two-authentication protocol. Suppose that ***A*** and ***B*** are honest principles and ***A*** wishes to communicate with ***B***. ***A*** generates a random number R_1 and sends it to ***B***. An intruder ***I*** intercepts the challenge R_1, and starts a second session with ***A***, in which he impersonates ***B*** by sending the intercepted challenge to ***A*** as if he generated it himself. Meanwhile, ***A*** assumes that the random number is from ***B*** and encrypts it with the secret key *k,* which ***A*** shares it with ***B***. Then ***A*** generates a random number

R_2 encrypted with k, and sends both encrypted number to ***B***. ***I*** intercepts the encrypted random numbers: $\{R_1\}_k$ $\{R_2\}_k$ and replies to ***A*** as a part of the first session. In this case, ***A*** believes he is receiving the encrypted random numbers from ***B*** and decrypts them with k. The received random number R_1 is the same as the one ***A*** has generated for the first session, so ***A*** believes that he is actually communicating with ***B***. Consequently, ***I*** has now authenticated himself to ***A*** as ***B***. In order to complete the first session, ***A*** sends R_2 to ***B***. ***I*** intercepts the message and replies back to ***A*** as part of the parallel session. ***A*** receives R_2 and assumes he is communicating with ***B***. As a result; ***I*** has authenticated himself again to ***A*** as ***B*** (Bird *et al*., 1993; Obaidat and Boudriga, 2007).



Attack 3.4: A parallel session attack against the ISO two-authentication protocol

3.3.5 ATTACKS ON ENCRYPTION SCHEMES

The obvious main objective to mounting attacks on ciphertext is to systematically recover plaintext or to deduce the decryption key (Menezes *et al.*, 2010). This attack can take different forms, such as ciphertext-only attacks (COA), known-plaintext attacks (KPA), chosen-plaintext attacks (CPA), chosen-ciphertext attacks (CCA-1) and adaptive chosen-ciphertext attacks (CCA-2). This is a very threatening attack because the attacker may be able to recover the hidden secret key used for decryption. For example, in a chosen-ciphertext attack, the attack is conducted by choosing a ciphertext and obtaining its decryption under an unknown key. The attacker has a chance to enter one or more known ciphertexts into the system in an attempt to obtain the resulting plaintext. This attack model is used by cryptanalysts to gather information in order to perform cryptanalysis (Menezes *et al.*, 2010).

3.4 EVALUATION AND SIMULATION TOOLS

Security protocols are rising in prominence in communication systems, and verifying them has gained significant attention by researchers and developers. Formal verification methods of cryptographic protocols aim to formally guarantee these protocols to satisfy their specifications, and they can function soundly. These methods can be employed to identify errors and they provide a deeper understanding of the protocols' behaviour. Security evaluation is a fundamental step in the development of security protocols. The methods used to analyse security protocols can be categorised into two groups: methods based on analytical approach and methods based on simulation. The analytical approach offers accurate results and provides a clear perception of the system characteristics. This approach can be

classified into two groups based on the analysis methods according to Meadows (1995):

1) Methods based on logic, for example, BAN logic (Burrows et al., 1990).
2) Methods based on algebra such as CSP algebra (Ryan and Schneider, 2001).

However, the analytical approach becomes unreliable when dealing with a high complex system (Genter *et al*., 2007). Therefore, the latter approach, which is the simulation approach, has become more popular in system analysis. Simulation tools, such as finite-state machines and Petri nets, expose progress in two directions: one related to the development of faster methods during execution of mathematical algorithms (Chiola and Ferscha, 1993), and the other associated with the effectiveness of simulation presentations and results (Genter *et al*., 2007).

3.4.1 FINITE-STATE MACHINES

Verification is a crucial step in designing security protocols. Finite-state machines (FSM), also called finite-state automata, are a mathematical model of behaviour and they are considered a powerful tool to simulate software architecture and communication protocols. FSM can only model the control part of a system and consists of a finite number of states, a finite number of events, and a finite number of transitions. A formal definition of an EFSM is as follows (Hopcroft and Ullman, 1979):

An FSM may be regarded as a five-tuple (Q, ∑, Δ, σ, q0), where:

Q: finite set of symbols denoting states

∑: set of symbols denoting the possible inputs

Δ: set of symbols denoting the possible outputs

σ: transition function mapping to Qx∑ to QxΔ

q0 ϵ Q: initial state.

Basic Notation

An FSM is a graphical representation and it can be described as a state transition diagram (Gajski, 1997; Luba, 2001; Adamski and Barkalov, 2006). A state diagram is a direct graph that consists of the following components (De Micheli, 1994; Hopcroft and Ullman, 1979):

- States are represented by a finite set of vertices, drawn as circles labelled with a state name.
- Transitions are represented by direct edges, drawn as an arrow from a current state to the next state.
- Output symbols are represented by labels.
- The initial state is mostly represented by an arrow pointed at it.

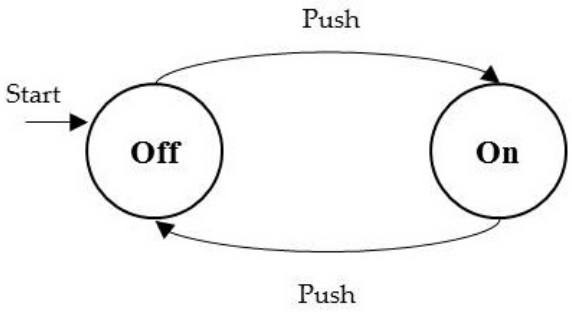


Figure 3.3: A finite-state machine modelling an off/on switch

A simple example of FSM is an *on/off* switch. This device remembers what state it is in. It allows the user to press a button and change to a different state depending on the previous one. For example, if the switch is in the *off* state, then pressing the button changes it to the *on* state. As shown in Figure 3.3, this finite-automaton model consists of two *states*: namely, the states *on* and *off*. The *arcs* between the states represent external influences on the system. In this example, both arcs are labelled by the input *Push*, which represents a user pushing the button. The state *off* is chosen to be the start state, the state in which the system is placed initially. The initial state is mostly indicated by an *arrow* and the word *Star*t. Also, it is often necessary to indicate one or more state as a "final" or "accepting" state (Hopcroft and Ullman, 1979).

3.4.2 PETRI NETS

Historically speaking, the concept of the Petri nets was introduced in 1962 by Carl Adam Petri. Petri nets are graphical diagrammatic tools based on strong mathematical foundation. They are used as a visual communication aid to model concurrency, synchronisation, limited resources, sequentially mutual exclusion and behaviour in distributed systems (Peterson, 1981; Murata, 1989; Bobbio, 1990).

Basic Notation

A Petri net is defined as a bipartite directed, weighted graph with two types of nodes called places and transitions, linked by directed arcs. In other words, a Petri net must consist of the following components (Peterson, 1981; Murata, 1989; Bobbio, 1990):

- A set of places (drawn as circles), representing conditions and possible states of the system.
- A set of transitions (drawn as rectangles or thick bars), representing a change of state, which is caused by events or actions.
- A set of arcs (drawn as arrows) connecting a place to transition and vice versa.
- Tokens (drawn as black dots), occupying places to represent the truth of the associated condition.

Murata (1989) defined a formal definition of a Petri net as follows:

A Petri net is 5-tuple, $PN=(P,T,F,W,M_0)$ where:

$P=\{p_1, p_2,\ldots,p_m\}$ is a finite set of places,
$T=\{t_1,t_2,\ldots,t_n\}$ is a finite set of transitions,
$F \subseteq (P \times T) \cup (T \times P)$ is a set of arcs (flow relations),
$W:F \rightarrow \{1, 2, 3,\ldots\}$ is a weight function,
$M_0:P \rightarrow \{0, 1, 2, 3,\ldots.\}$ is the initial marking,
$P \cap T= \emptyset$ and $P \cup T \neq \emptyset$.

A Petri net structure $N=(P, T, F, W)$ without any specific initial marking is denoted by N.

A Petri net with the given initial marking is denoted by (N,M_0).

Furthermore, he distinguishes the dynamic behaviour of many systems according to their states or changes. To simulate the behaviour, a state or marking in a Petri net is changed according to the following transition (firing) rules (Murata, 1989):

1) A transition t is said to be enabled if each input place P of t is marked with at least $w(p, t)$ tokens where $w(p, t)$ is the weight of the arc from p to t.

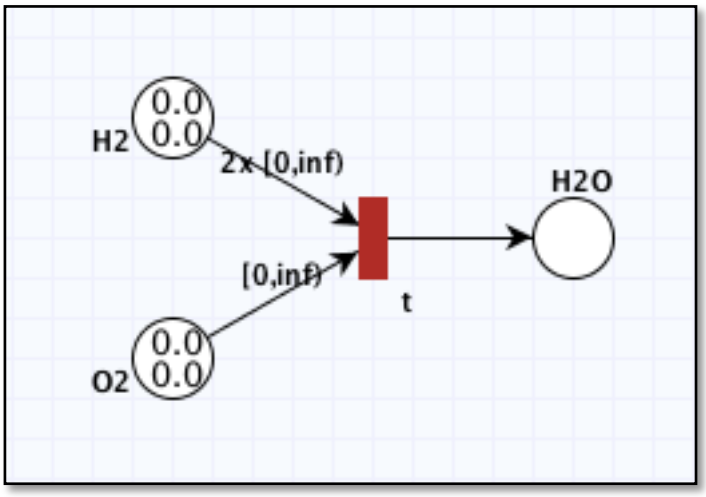
2) An enabled transition may or may not fire (depending on whether or not the event is actually takes place).
3) A firing of enabled transition t removes $w(p, t)$ tokens from each input place p of t, and adds $w(t, p)$ tokens to each output place p of t, where $w(t, p)$ is the weight of arc from t top.

Definition 1. *A transition without any input place is called a source transition, and one without any output place is called a sink transition. Note that a source transition is unconditionally enabled, and the firing of a sink transition consumes tokens, but does not produce any.*

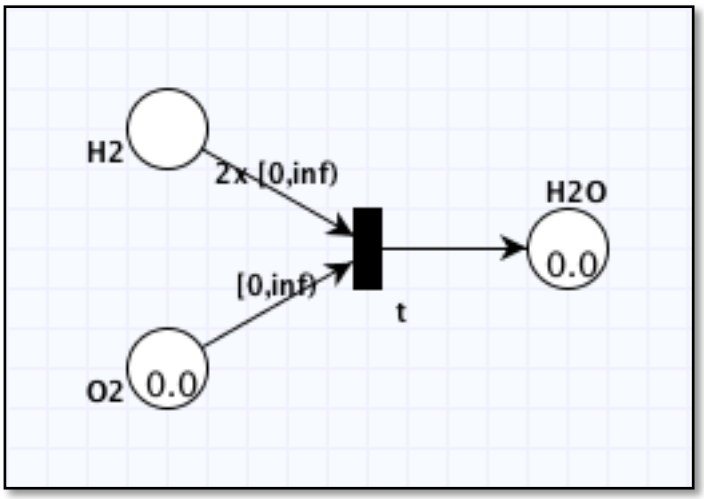
Definition 2. *A pair of a place p and transition t called self-loop if p is both an input and output place of t. A Petri net is said to be pure if it has no self- loops. A Petri net is said to be ordinary if all of its arc weights are 1's.*

Murata (1989) illustrated a transition (firing) rule using a simple example of the well-known chemical reaction: $\boldsymbol{2H_2 + O_2 \rightarrow 2H_2O}$.

Figure 3.4 (a) shows two tokens in each input place are available, and a transition *t* is enabled and can fire when at least two units of H_2 and one unit of O_2 contain the input places. After firing, a new even has occurred resulting in a change in the reaction state $2H_2O$. Also, the marking has changed to zero unit in H_2 and one unit in O_2 as shown in Figure 2.4 (b), in which the transition *t* is no longer enabled.



(a)



(b)

Figure 3.4: An illustration of transition (firing) rules:

(a) The marking before firing the enabled transition t.

(b) The marking after firing t, where t disabled.

Petri nets behaviour properties

A well-known major strength of Petri nets is the ability to analyse properties and complications associated with concurrent systems. The basic behavioural properties of Petri nets can be summarised in the following (Murata, 1989):

1. *Reachability* is a foundation for examining the dynamic properties of any system. The firing of an enabled transition will change the token distribution (marking) in a net, according to the transition rules.
2. *Boundedness* is achieved when the number of tokens in each place does not exceed a finite number k for any marking reachable from M_0. Thus, a Petri net is ***k-bounded***. A Petri net is said to be ***safe*** if it is ***1-bounded***.
3. *Liveness* is associated to the complete absence of deadlock in the system. A Petri net is said to be ***live***, if no matter what marking has been reached from M_0, it is possible to ultimately have some further firing sequence.

3.5 SUMMARY

This chapter examines the original concept of the identity based encryption and its basic algorithms for encryption and decryption. The He *et al*. scheme was examined thoroughly. Even though the protocol overcame many of the security problems, unfortunately it is vulnerable to reflection attack and parallel session attack. Next, a detailed description of Li-Hwang scheme was presented as a biometric authentication protocol, which also suffers from security issues such as man-in-the middle attack. Understanding the security flaws in previous cryptographic protocols is the leading key to fix the existing protocols and avoid to making the same flaws again. The chapter analyses the most common security flaws in authentication protocol and demonstrates each attack against them. Finally, the chapter discusses the most common simulation tools that are used in the research and reviews their structures and properties.

4

The New Protocol Architecture

This chapter investigates the basic security properties that must be kept in mind when designing protocols. Also, it introduces the new scheme and some of the cryptographic techniques used to establish a secure key-exchange. Then, UML modelling is discussed briefly to represent all sequences of messages in the login phase.

Today concerns about security breaches are constantly increasing in all areas and affecting organisations such as governments, military agencies, banks, the healthcare industry, and educational institutions. There are several issues contributing to security concerns and some of them are related to authentication mechanisms. One common example can be found in passwords being the weakest link in modern security. Unfortunately most users prefer to pick easy-to-remember passwords, which make them vulnerable to easy guessing, sniffing, and brute force attacks. As a result, they might allow malicious users to get easy access to computers or online accounts and further compromise the entire network. Most systems nowadays depend on inherently weak password mechanisms to authenticate and verify their users' identities. Other authentication methods that can increase security are smart card authentication and biometric authentication. Biometrics can be used in many scenarios but for the purpose of this thesis it is used (1) as an authentication method to confirm user's identity, (2) as a way to salt the password in order to defend against dictionary attacks and rainbow table attacks, i.e. the biometric and the password are concatenated and processed with a cryptographic hash function. Having two authentication factors to identify a person definitely enhances security. In addition, this combination can limit any potential for fraud as well as provide a degree of distinctiveness and secrecy.

4.1 Developing Secure Methodology

One of the main goals the organisation seeks is to promote secure authentication and data exchange electronically in distributed systems. Thus, developing an effective methodology is essential and it is the key factor for success. In terms of information security management and biometric security frameworks, both ISO/IEC 27001:2005

and ISO 19092:2008 have been carefully studied to produce the proposed conceptual method, as shown in Figure 4.1. There are various techniques used in the proposed methodology in order to achieve the objectives of the security requirements. The purpose of the conceptual methodology is to investigate the requirements and mechanisms associated with building a secure protocol. Moreover, it attempts to identify factors to achieve functionalities and security in complex systems.

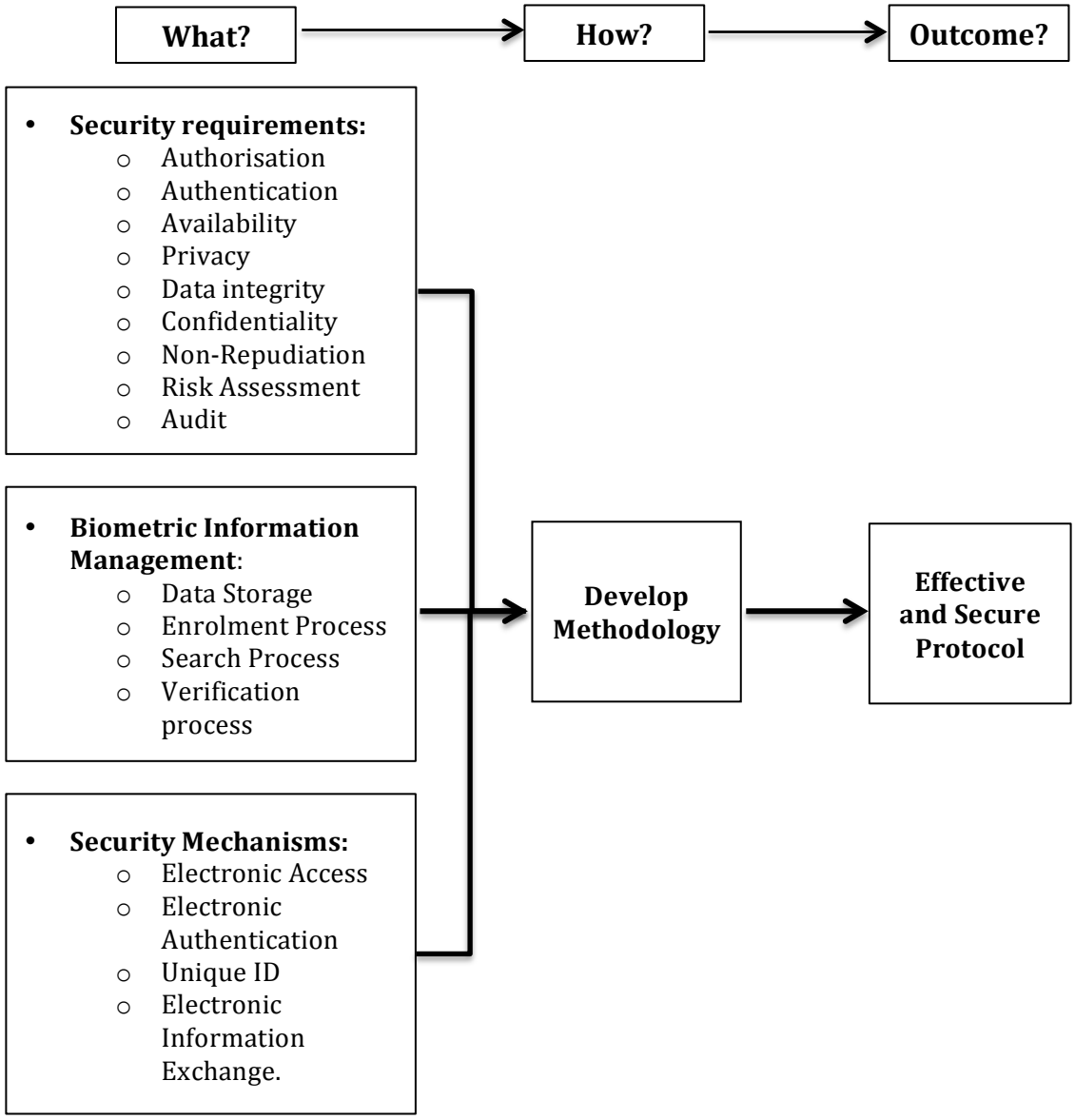


Figure 4.1: Conceptual of secure methodology

When designing security protocols, it is crucial to consider all the security properties and to carefully implement them in the right place. Those properties essentially become required security functions and are summarised as follows (Boyd and Mathuria, 2003; Stallings, 2011; Stapleton, 2014):

- *Authentication*: is the ability to determine the origin of the received message and ensure no malicious user should be able to send a forged message.
- *Authorisation*: restricts access to the resource for only authorised and legitimate users in the network.
- *Privacy*: guarantees that the identity of a user should not be exposed to unauthorised entities and should remain anonymous.
- *Data integrity*: assures that the recipient of a message should be able to verify that the contents of the message are authentic and have not been modified in transmission.
- *Confidentiality*: provides protection against eavesdropping and unauthorised access while data in transit or set. Also, ensure that only those are authorised can access the data.
- *Non-repudiation:* ensures that entities cannot later deny sending or receiving messages that they have committed to.
- *Risk assessment:* includes vulnerability assessment by identifying weakness and threats. Also, it helps to understand exposures and limit any potential threats.
- *Audit logs:* need to be collected and analysed to maintain proper controls in case of potential security breaches. They contain sufficient information to detect attacks and valuable information for forensic analysis.

The baseline of this methodology is treating the security requirements as a foundation of the authentication protocols. For example, in authorisation and authentication, a combination of biometric information and ID-Based Encryption ((IBE) are applied to ensure that only authorised persons are allowed to gain access to the network after their credentials have been verified. Also, encryption is implemented to guarantee data confidentiality and privacy.

4.2 The New Protocol Architecture

Authentication is considered a significant pillar of a standard security model. It is the process to validate and confirm the identification of a client who is attempting to gain accesses in remote systems and using resources. The new scheme supports secure authentication by implementing biometric verification with IBE. Using IBE as an infrastructure will certainly simplify the encryption-decryption process. For example, a sender can encrypt a message by using the recipient's identity (such as e-mail address) and public parameters that have been generated by the server. Then, the server generates a private key for the recipient in order to decrypt messages.

Before secure communication occurs, each individual user needs to be registered with the system first. This process is called enrolment. In this process, reference features for each user are stored in the system and associated with the identity of the subject (Figure 4.2). The process starts with the acquisition of physiological traits. The digital information representation after this step is denoted as enrolment samples. As shown in Figure 4.2 copies of enrolment samples may be stored in some evaluation environment in order to allow later reproduction of the original writing processes. From these original enrolments, features are then extracted after pre-

processing. These extracted features are stored as references in a storage location of the authentication systems (Jain *et al.*, 2015). As for authentication, the system performs a comparison of the data from the actually presented traits to stored references (Figure 4.3). The steps are identical to those in the enrolment mode until reaching the completion of the feature extraction process. Here, the features derived from the actual sample presented for authentication are compared to stored references from the references storage. Based on the result of the comparison, the system will then perform a classification (Jain *et al.*, 2015).

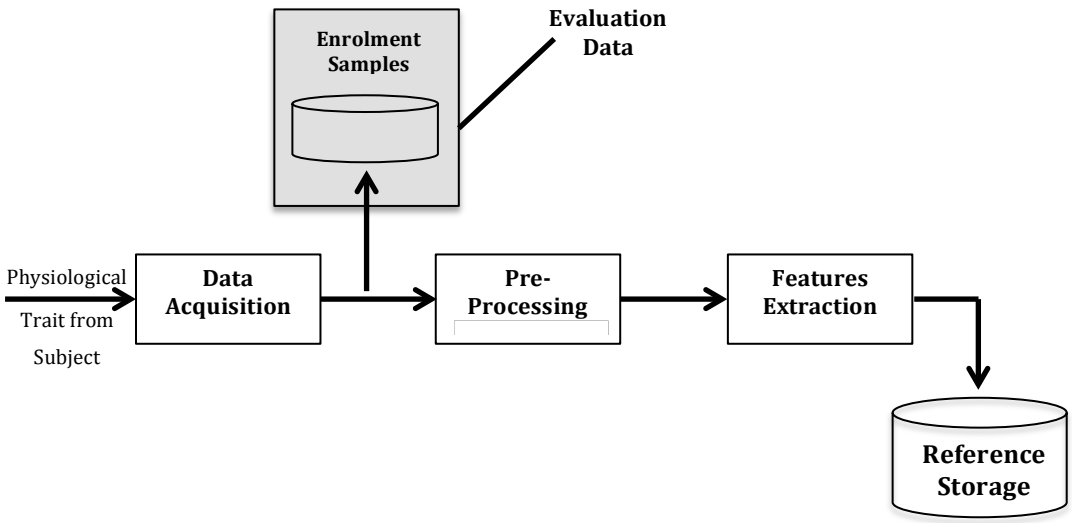


Figure 4.2: Enrolment mode of a biometric authentication system adopted from Vielhauer (2005)

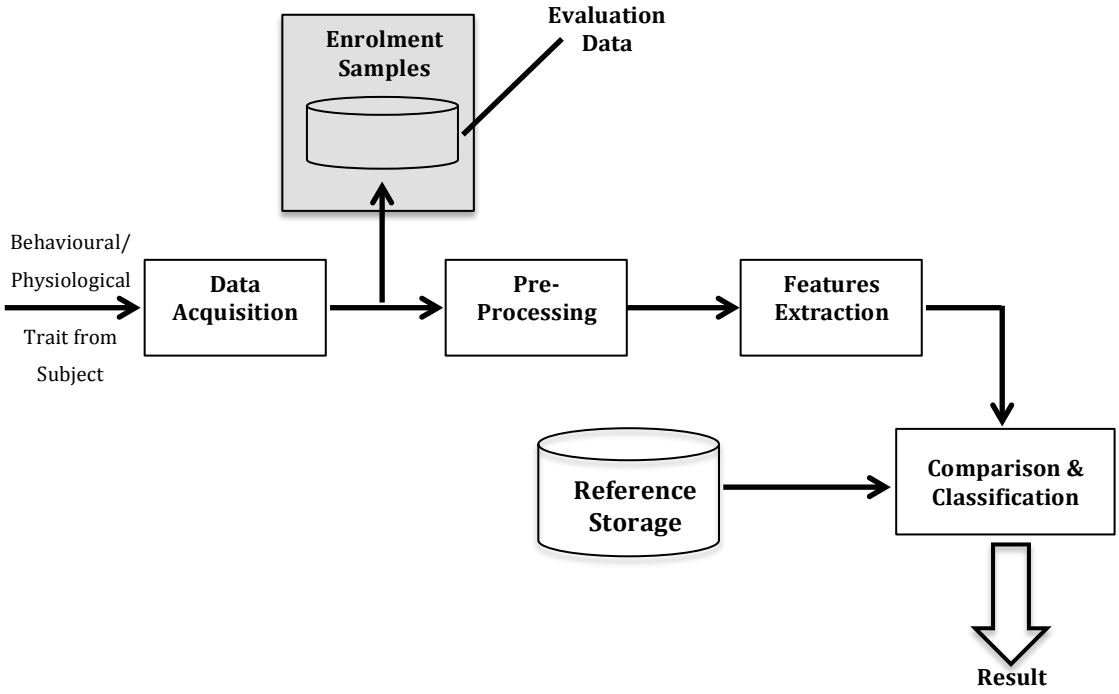


Figure 4.3: Authentication Mode of a Biometric Authentication System adopted from Vielhauer (2005)

The new scheme consists of three phases: registration phase, login phase, and authentication phase. It is based on a three-way handshake that promotes secure key establishment. Peers involved in the scheme must share the same security context. The protocol diagram shown in Figure 4.4 is a collaboration diagram that defines the necessity element to establish a secure interaction between the client and the server. This diagram formulates the ideas to help design the protocol. The aim of the proposed protocol is to establish a new secret session key between any trusted client and server, which they can use for subsequent secure communication. Additionally, both the client and the server should be able to calculate the session key at the end of the protocol process but it must be difficult for other parties to learn the true value of the session key. The session key should be generated within every new session to avoid replay attacks.

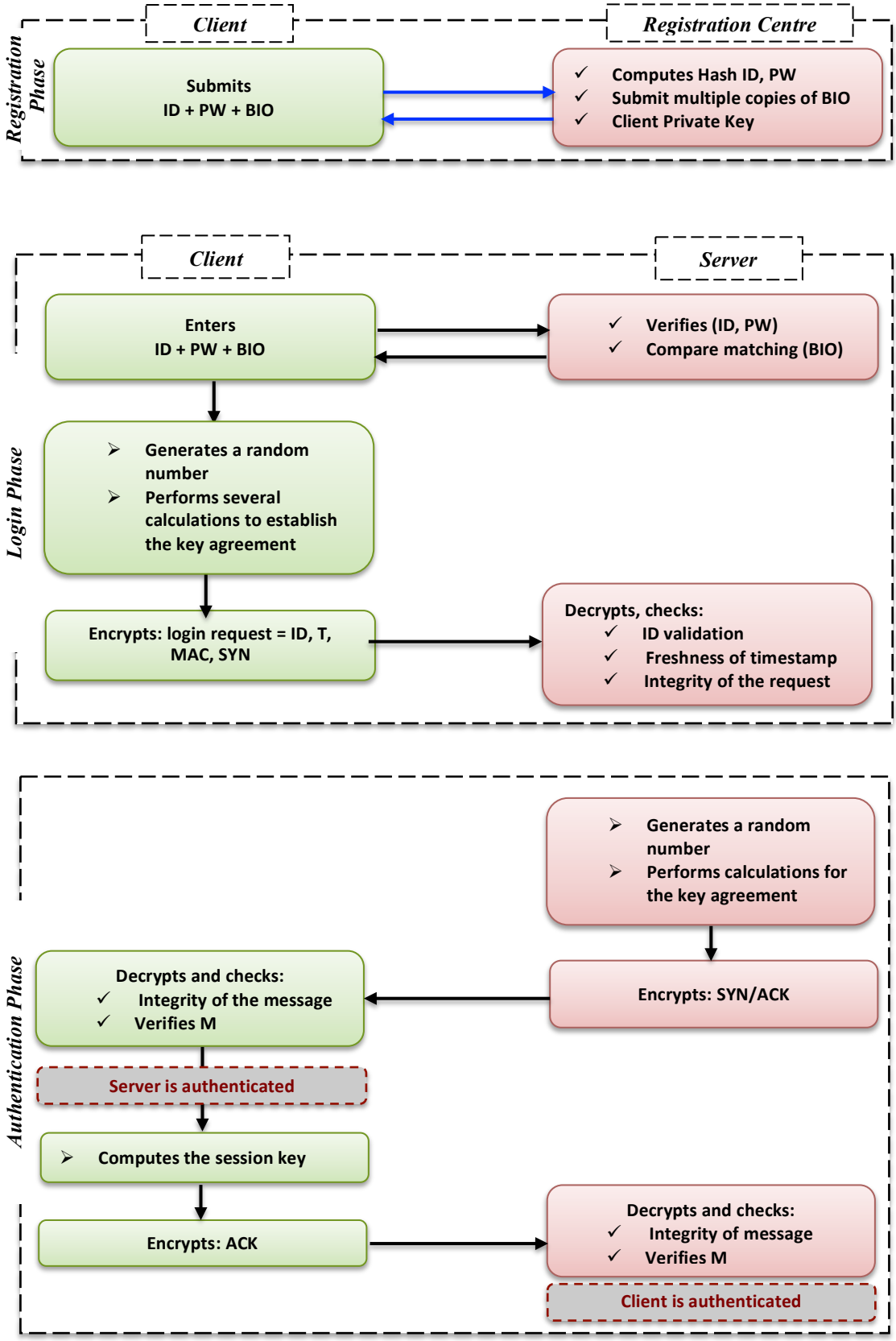


Figure 4.4: The new scheme architecture

In the registration phase, the client must submit his/her ID, password and biometric data for identification purposes. As for the login phase, the client needs to provide his/her credentials to confirm his/her identity. The negotiation of the session key begins once the client passes the identity check. Basically, the proposed authentication process implies that messages exchanged between entities must convey identities, freshness, and authenticity.

The mechanism in the diagram in Figure 4.4 corresponds to the TCP handshake where the client establishes a connection with the server using a three-way handshake or SYN - SYN/ACK - ACK. First, the client creates a login request based on the generated random number, timestamp, and other computational values to disguise the random number. This part of the procedure resembles the SYN part in the three-way handshake. When the server receives the SYN, it checks the authenticity and integrity of the request. This can be achieved by checking the freshness of the timestamp and the MAC value. Once the verification is valid, the server generates random a number and a timestamp to create the SYN/ACK. At this stage, the server should have all the data needed to calculate the session key for the client. The client then computes the shared session key and sends an ACK message to the server. The server then uses the shared knowledge to verify that the message returned from the client could have only been computed using the shared information.

4.3 THE NEW PROTOCOL PROCESS MODEL

Developing a secure model for organisations tends to be difficult due to finding the right balance between security and functionality. For this reason, the research will focus on secure distributed systems and improve their authentication and communication. To guarantee the security of these distributed systems, biometric techniques and ID-based cryptography are adopted. Since it is very hard to design such a model correctly and without errors, a Unified Modelling Language (UML) (Larman, 2002; Stevens, 2006) is used to represent the abstraction level between the client and the server. This process is the initial phase to understand the functionality of the proposed protocol. It consists of:

1. Using a case model to capture the functional requirements of the system
2. Using an activity and sequence diagram to capture the dynamic behaviour of the system and articulates a sequence of messages exchanged in the protocol.

System Requirements:

The main goal is to design a secure computer system that fully supports biometric verification and IBE in any distributed system. The organisation employees and users could connect to the systems (server-side) from any place (client-side) through the Internet.

The proposed system functions as the following:

- The system provides users with a reliable authentication mechanism.
- Data interchange in transaction should be secure.
- Data storage should be secure and reliable.

The following activity diagram in Figure 4.5 shows the actions that occur during the login process for registered users. The primary actors in this activity diagram are the users and the system administrator. The diagram illustrates the steps taken as an authorised employee logs on to the computer system. Access to the system is only granted if the user's ID/ password/ biometrics are all entered correctly within the first three attempts. Otherwise, the user ID will be locked out after the third attempt and the system administrator will need to issue a new password. Once access is granted the user can use the system according to their level of authorisation. The rational reason behind implementing limited entry attempts and lockout policy is to prevent brute force attack and unauthorised access.

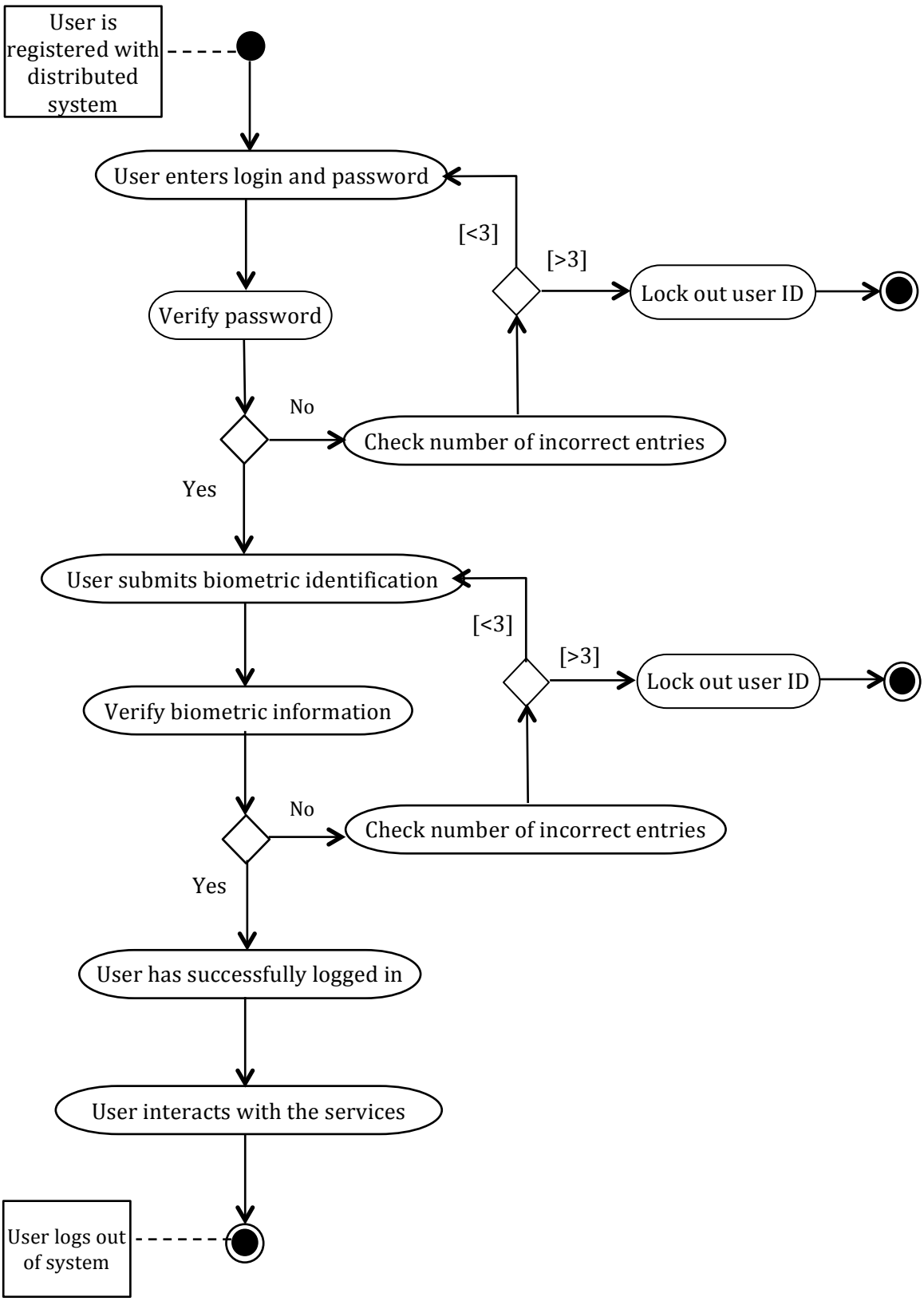


Figure 4.5: Activity diagram for logging on

The next diagram shown in Figure 4.6 below is the sequence diagram. It is used to show how the user interacts in a given situation in a timely manner.

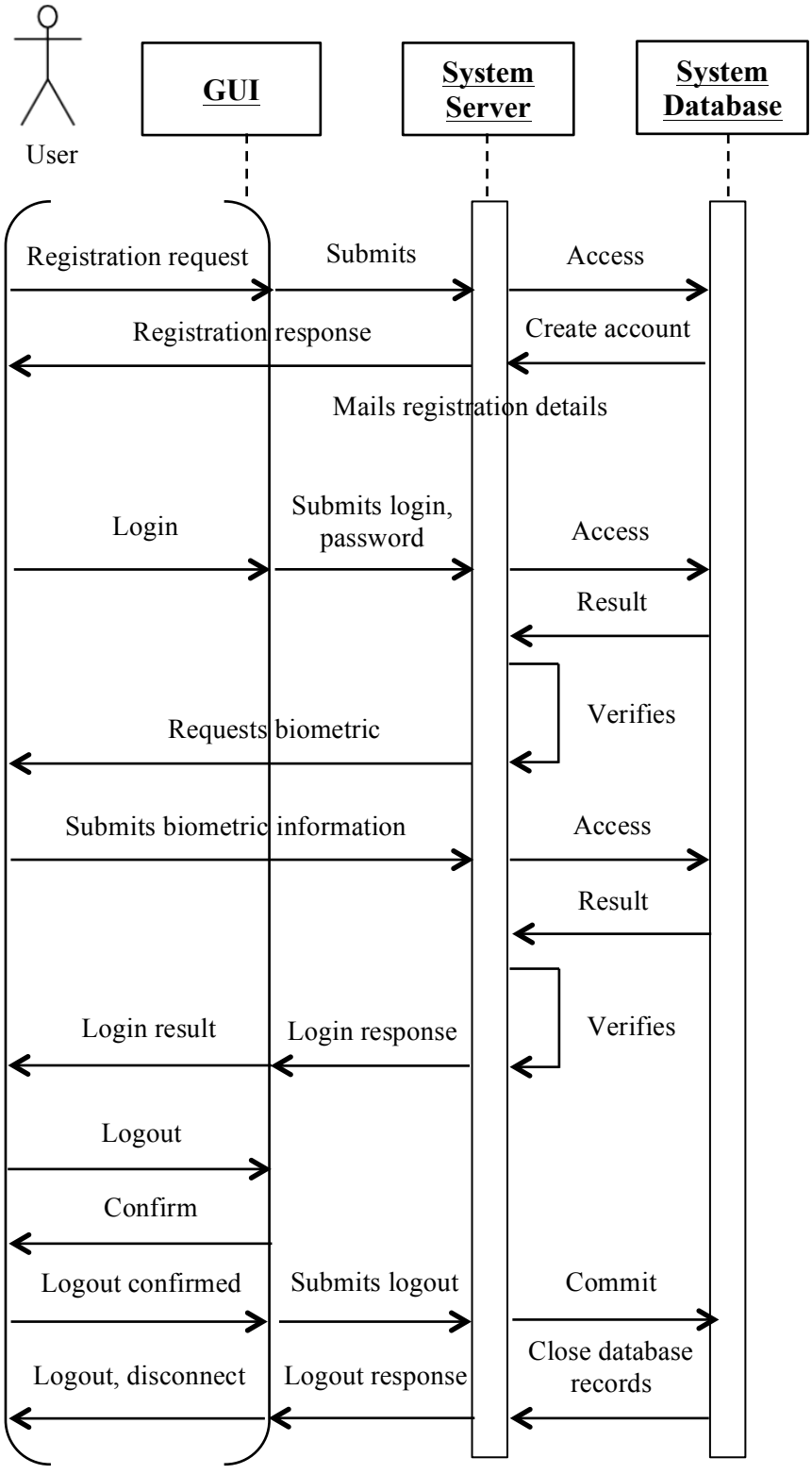


Figure 4.6: Detailed system behaviour for user activities

4.4 SUMMARY

Designing a new authentication protocol can be challenging because authentication protocols are schemes based on cryptographic algorithms, which provide secure communication for authenticating peers. This chapter aims to present a methodology to formulate the basic notation to build a new scheme and helps to set the protocol rules and security context for the next chapter. The new scheme comprises a sequence of interactions between a client and a server designed to achieve mutual authentication and establish session keys between entities. The exchange of messages between entities uses various cryptographic mechanisms such as symmetric encryption, hash function, message authentication code, random numbers, and timestamps. These mechanisms will be discussed explicitly in Chapter 5. Moreover, this chapter discussed the concept of the new scheme and its architecture and shows the importance to consider all security requirements. The internal behaviour of the login phase is modelled with UML modelling to understand and visualise the initial phase of the protocol design.

5

Protocol Design

This chapter concentrates on designing an authentication protocol. First, it describes the objectives of the new protocol and scheme preliminaries. Then, it elaborates the details of the proposed protocol and identifies explicitly the process of each phase. The proposed scheme consists of four phases: system initialisation phase, registration phase, login phase, and authentication phase.

Authentication protocols can be thought of as schemes to authenticate the identity of entities, which are based on cryptographic algorithms (Stallings, 2011). It is essential to design a robust authentication scheme with well-built security measures. The main method used for devising the proposed protocol was to reengineer the He *et al*. scheme (2012) and Li-Hwang scheme (2010) and combine them together to produce a new protocol with the best features of both and without their flaws. To achieve the confidentiality goal of the new protocol, symmetric encryption is applied between the client and server during the mutual authentication to prevent passive attacks such as eavesdropping or active attacks such as man-in-the-middle attacks. Additionally, to guarantee the integrity of the protocol, a message authentication code (MAC) is employed in every message transmitted to detect any modification or tampering.

5.1 Protocol Description and Objectives

The protocol objectives describe the environment within which the information transmission will be carried out between the client and server. It provides hybrid cryptography by utilising both ID-based encryption and biometric. The protocol objectives can be summarised as follows:

1. The protocol can operate in insecure channels, such as the Internet, except in the registration phase where SSL is used.
2. The protocol is an authentication protocol that provides mutual authentication through a three-way handshake between two participants: a server and a client.

3. To protect subsequent communication between the server and client within the organisation network, a short-term session key is established during the authentication process.

5.2 PROTOCOL PRELIMINARIES

The novel contribution of this submission is focused on secure distributed systems such as e-Government and improves their authentication and communication. To guarantee the security of these distributed systems, biometric verification and ID-based cryptography are used. The proposed protocol is based on the following assumptions:

- The shared secrets in the registration phase will never be disclosed.
- The cryptographic algorithms are secure. For example, it is impossible to cryptanalyse a ciphertext without prior knowledge of the secret key.
- Both the client and server are able to generate a random number securely.

The security of the proposed scheme is based on the intractability of the following two mathematical problems on elliptic curves (Boneh and Franklin, 2001; He *et al*., 2012)

(i) **C**omputational **D**iffie–**H**ellman **A**ssumption (CDHA): Given $P, xP, yP \in G$, it is hard to compute $xyP \in G$.

(ii) **C**ollision **A**ttack **A**ssumption 1 (k-CAA1): For an integer k, and $x \in Z_n^*$, $P \in G$, given $(P, xP, h_0, (h_1, (h_1+x)^{-1}P), \ldots, (h_k, (h_k+x)^{-1}P))$, where $h_i \in Z_n^*$, and distinct for $0 \leq i \leq k$, it is hard to compute $(h_0+x)^{-1}P$.

The proposed scheme consists of four phases: system initialisation phase, registration phase, login phase and authentication and key agreement phase. The notations used throughout this chapter are summarised in the list of notation section.

5.3 System Initialisation Phase

System initialisation is executed by the server to setup the security domain for protocol message exchange. This process is obtained by generating security parameters and publishing public parameters. The initialising steps in this phase are very similar to He *et al*.'s scheme where the server S_i generates parameters of the system.

Step 1: S_i chooses an elliptic curve equation $E_P(a, b)$.

Step 2: S_i selects a base point P with the order n over $E_P(a, b)$.

Step 3: S_i randomly selects its master key x and secret information y and computes public key $Pub\_K_s = xP$.

Step 4: The server chooses four secure one-way hash function $H_1(.)$, $H_2(.)$, $H_3(.)$, $H_4(.)$, where $H(.)$ is a known hash function that takes a string and assigns it to a point on the elliptic curve, i.e. $H(A) = QA$ on E, where:

- $H_1(.)$: a secure one-way hash function, where $H_1: \{0, 1\}^* \rightarrow Z^*_n$
- $H_2(.)$: a secure one-way hash function, where $H_2: \{0, 1\}^* \rightarrow Z^*_p$
- $H_3(.)$: a secure one-way hash function, where $H_3: \{0, 1\}^* \rightarrow Z^*_p$
- $H_4(.)$:a secure one-way hash function, where $H_4: \{0, 1\}^* \rightarrow Z^*_p$

Where: $\{0, 1\}^*$ denotes the set of all finite binary strings,

Z^*_n is the multiplicative group of positive integers less than n,

Z^*_p is the multiplicative group $Z^*_p = \{1,2,...,p-1\}$ of order p, where p is a prime.

Also, the server keeps x private and publishes $\{F_p, E, n, P, Pub\_K_s, H_1, H_2, H_3, H_4, MAC_k(m)\}$.

5.4 Registration Phase

A client C_i with identifier ID_{C_i} should be registered first with R_i before using the services provided. Clients may use a unique *ID*, for example, the employee number as an identity, when contacting R_i for authorisation and authenticity. In this phase, C_i needs to perform the following steps:

Step 1: User C_i inputs their ID_{C_i} and personal biometrics Bio_{C_i} on a specific biometric device, and provides the password PW_{C_i} to R_i via a secure channel (or to the registration centre in person).

Step 2: R_i computes the following:

$$f_i = H_4 (Bio_{C_i})$$

$$z_i = H_4 (PW_{C_i} || f_i)$$

$$e_i = H_4 (ID_{C_i} || y) \oplus z_i$$

Step 3: R_i computes C_i's private key using the system private key x and C_i's public key.

$$Pr\_K_{C_i} = (x + H_4 (ID_{C_i}))^{-1} P \in G$$

$$Pub\_K_{C_i} = H_4 ((ID_{C_i}) + x) P = H_4 ((ID_{C_i})P + Pub\_K_s)$$

Step 4: R_i stores $\{ID_{C_i}, H_4 (.), Enc\{\}_a/Dec\{\}_a, f_i, e_i, \tau, Pr\_K_{C_i}\}$ on a secure database and sends it to the user via a secure channel, where $Enc\{\}_a/Dec\{\}_a$

is a symmetric encryption with secret key a and τ is a predetermined threshold for biometric verification (Inuma *et al.*, 2009).

5.5 LOGIN PHASE

The user C_i sends a login request to the server S_i and performs the following steps:

Step 1: C_i enters the ID_{C_i} and PW_{C_i}, then S_i verifies the authenticity of client's identity and password.

Step 2: C_i submits the Bio_{C_i} on a specific biometric device, then S_i verifies the following:

$$\begin{cases} \text{Accept if } d(Bio_{C_i}, Bio^*_{C_i}) < \tau \\ \text{Reject if } d(Bio_{C_i}, Bio^*_{C_i}) \geq \tau \end{cases}$$

Step 3: if the above does not hold, it means the biometric information does not match the template stored in the system. Thus C_i does not pass the biometric verification process and the authentication scheme is terminated. Otherwise, C_i passes the biometric verification and computes the following:

$$f_i = H_4\,(Bio_{C_i})$$

$$z`_i = H_4\,(PW_{C_i} \,||\, f_i)$$

$$M_1 = e_i \oplus z`_i = H_4\,(ID_{C_i} || y)$$

$$W_1 = r_{C_i}.\,P$$

$$M_2 = r_{C_i}.\,Pr\_K_{C_i}$$

$$M_3 = M_1 \oplus r_{C_i}$$

Where $r_{C_i} \in Z^*_n$ is a random number generated by the client. For this step, the random value r_{C_i} is introduced to mask the hash of the secret value $H_4(ID_{C_i}||y)$.

Step 4: C_i computes the secret key for $MAC, k = H_2\ (ID_{C_i}, T_{C_i}, W_1, M_2)$, where T_{C_i} is a timestamp denoting the current time and calculates the MAC value for $(ID_{C_i}, T_{C_i}, W_1, M_3)$.

Step 5: Finally, C_i encrypts the message $\{ID_{C_i}, T_{C_i}, W_1, M_3, MAC_k\ (ID_{C_i}, T_{C_i}, W_1, M_3)\}_a$ and sends it to the server S_i. This login request contains the initial components of the negotiated session key: ID_{C_i}, T_{C_i}, W_1 as contribution of the session key.

The encrypted message includes C_i's timestamps to provide freshness guarantees; the value of W_1 is a multiplication of the C_i's random number with P point on elliptic curve E with order n.

5.6 Authentication and Key Agreement Phase

After receiving the request login message, S_i and C_i will perform the following steps for mutual authentication:

Step 1: S_i decrypts the message $\{ID_{C_i}, T_{C_i}, W_1, M_3, MAC_k(ID_{C_i}, T_{C_i}, W_1, M_3)\}_a$, then checks the validity of ID_{C_i} and the freshness of T_{C_i}. The freshness of T_{C_i} is checked by performing $T^* - T_{C_i} \leq \Delta T$, where T^* is the time when S_i receives the above message and ΔT is a valid time interval. In the case where ID_{C_i} is not valid or T_{C_i} is not fresh, then S_i aborts the current session. This means the

system stops processing the request due to invalid parameters and the client has to login again.

Step 2: If Step 1 holds, S_i computes the following to create the secret key for MAC:

$$M_2 = (x + H_1(ID_{C_i})^{-1}. W_1$$

$$= Pr\_K_{C_i} . r_{C_i}$$

$$k = H_2 (ID_{C_i}, T_{C_i}, W_1, M_2)$$

S_i checks the integrity of $MAC_k (ID_{C_i}, T_{C_i}, W_1, M_3)$ with the key k. S_i will quit the current session if the check produces a negative result.

Step 3: If Step 2 holds, S_i chooses a random number $R_{S_i} \in Z^*_n$ and computes the following:

$$M_4 = H_4 (ID_{C_i} || y)$$

$$W_2 = r_{S_i} . P$$

$$K_{S_i} = r_{S_i} . W_1$$

Now S_i is able to complete the protocol and compute the absolute value of the session key $sk = H_3 (ID_{C_i}, T_{C_i}, T_{S_i}, W_1, W_2, K_{S_i})$, where T_{S_i} is a timestamp denoting the current time.

$$M_5 = M_3 \oplus M_4 = r_{C_i}$$

$$M_6 = M_4 \oplus r_{S_i}$$

$$M_7 = H_4(M_3 || M_5)$$

Where M_5 is the random value r_{C_i} of the user C_i and only S_i can unmask the value because it can compute $H_4\ (ID_{C_i}\ ||\ y)$.

Step 4: S_i computes the MAC value for $(ID_{C_i}, T_{S_i}, W_2, M_6, M_7)$, then encrypts the message $\{ID_{C_i}, T_{S_i}, W_2, M_6, M_7, MAC_k(ID_{C_i}, T_{S_i}, W_2, M_6, M_7)\}_a$ and sends it to C_i.

Step 5: Upon receiving the S_i's message, C_i first decrypts $\{ID_{C_i}, T_{S_i}, W_2, M_6, M_7, MAC_k(ID_{C_i}, T_{S_i}, W_2, M_6, M_7)\}_a$, and checks the freshness of T_{S_i} by performing $T' - T_{S_i} \leq \Delta T$, where T' is the time when C_i receives the above message and ΔT is the expected time interval for the transmission delay.

Step 6: C_i verifies whether the received message M_7 matches the computation of $H_4\ (M_3\ ||\ r_{C_i})$ and checks the integrity of $MAC_k\ (ID_{C_i}, T_{S_i}, W_2, M_6, M_7)$ with the key k. C_i will quit the current session if the check produces a negative result.

Step 7: If it holds, C_i believes that S_i is authenticated and then computes the following:

$$K_{C_i} = r_{C_i} . W_2$$

The session key $sk = H_3\ (ID_{C_i}, T_{C_i}, T_{S_i}, W_1, W_2, K_{C_i})$

$$M_8 = M_6 \oplus M_1 = r_{S_i}$$

$$M_9 = H_4(M_6\ ||\ M_8)$$

Where M_9 is the random value r_{S_i} of the server S_i and only the client C_i, which know $M_1 = H_4\ (ID_{C_i} || y)$, can send back the correct hashed value of $M_9 = H_4\ (H_4\ (ID_{C_i} || y) \oplus r_{S_i}) || r_{S_i})$.

Step 8: C_i compute the MAC value for M_9, then sends the encrypted message $\{M_9, MAC_k(M_9)\}_a$ to S_i.

Step 9: After receiving C_i's message, S_i decrypts $Enc\{M_9\}_a$ and checks the integrity of $MAC_k(M_9)$. Then, S_i verifies whether $M_9 = H_4\ (M_6 || r_{S_i})$ or not.

Step 10: If the above-mentioned holds, S_i accepts C_i's login request or otherwise rejects it.

5.7 Protocol Defence Mechanisms

Securing authentication protocols plays a crucial role in the area of protocol design. The security of algorithms and techniques are equally important as efficiency and functionality. Carefully choosing adequate cryptographic algorithms can remove real threats that most protocols face. For example, encrypt the traffic to ensure confidentiality and apply message authentication code for integrity check. It is fundamental to consider if every component in the protocol represents complementary building blocks. Sometimes it is necessary to combine several mechanisms to achieve certain benefits on security features. This strategy often helps to focus on the small details of the protocol design and treat vulnerabilities and flaws as a visible opponent.

5.7.1 One-way cryptographic hash functions (OWCHF)

Hash functions in general were introduced in modern cryptography to provide data integrity and message authentication, and digital signatures (Menezes *et al*., 2010). Hash functions have many practical applications in computer science and information security. For example, cryptographic hash functions are used as a way to detect data corruption. In case the data is corrupted, a re-computation of the hash value will certainly change and eventually it will not match the stored value (Ryan and Schneider, 2001). However, the key purpose of using hash functions is to maintain integrity, protect sensitive data and computation values from security breach and determine if the data is authentic. However, there is a crucial difference between a standard hash function and a cryptographic hash function. A cryptographic hash function must at least have the property of being one-way. To clarify, given any string y from the range of h, it should be computationally infeasible to find any value x in the domain of h such that (Smart, 2008):

$$h(x) = y.$$

One-way cryptographic hash functions are mathematical computations that take in a relatively arbitrary amount of data as input and produce a fixed size output. They are easy to compute once the input is known but it should be difficult to calculate the hashed value without a prior knowledge of the original input (Stallings, 2011). The one-way hash function can be defined as a transformation mechanism that takes an arbitrarily large data field as its argument and maps it to a fixed output with the additional properties of preimage resistance and 2nd pre-image resistance. It is mostly used for authentication schemes (Menezes *et al*., 2010).

The one-way cryptographic hash function in the proposed protocol satisfied the following properties: pre-image resistance, 2^{nd}-pre-image resistance, collision resistance. A formal detailed security proof in the random oracle model has been conducted by He *et al*. (2012) based on the intractability of the following two mathematical problems assumptions: Computational Diffie-Hellman Assumption (CDHA) and Collision Attack Assumption 1 (k-CAA1). Note that, the reason for emphasis on that $H_2, H_3, H_4:\{0, 1\}^* \rightarrow Z^*_p$ is because it is known that half of the elements in Z^*_p are quadratic non-residues modulo p. The hash value of any binary message is thus some element of the group Z^*_p, which is easily computable and difficult to invert (Menezes *et al*., 2010).

In principle, storing the hash value of an applied one-way function can relatively prevent possible attacks for the following reasons. First, It should be computationally difficult for an attacker to find different inputs that produce the same hash value. Second, it should be computationally difficult for an attacker to find from one message a modified image of this message that both have the same hash values. Hence, if a hash function is resistant to a second pre-image attack it means that the one-way function will continue being one-way and it will always produce the same specific hash value for a specific message. Based on that, the password is concatenated with *f*, which is the biometric hashed value of the client. Thus, legitimate clients must provide something they know (password) and something they are (biometric) in order to be authenticated. This combined hashed value creates a tricky situation for an attacker to mount a brute force attack. It is crucial that the password is concatenated with the biometric template *f t*o prevent the rainbow table attack. The technique prevents knowing the common inputs and produces long hash value, which makes it hard for the attacker to generate a rainbow table.

5.7.2 Message Authentication code (MAC)

In the new protocol, a MAC-based method is applied instead of using a signature-based method. This method provides a guarantee that messages arriving at a destination are indeed in their original form as sent by the sender and they are coming from an authentic source. Moreover, the MAC detects if the content or timing of the message is modified. Also, it ensures non-repudiation by verifying the source that originated the message. The recipient can do the checksum with the shared key and compare the received checksum. This way the recipient only has to verify the integrity of messages using the same MAC algorithm.

Some attacks simply seek to corrupt particular fields in a packet's internal data by replacing some bytes of the transmitted data with random inputs to change the original plaintext for sabotage purposes. The proposed protocol relies on using MACs to authenticate the messages exchange between the client and server. The main goal that the proposed protocol seeks to achieve with the MAC is the ability to detect any attempt to corrupt or modify the transmitted data by attackers. The proposed protocol is designed to limit the attacker's ability to produce feasible messages the client will deem authentic. That is, the attacker will not be able to create a feasible message: $\{ID_{C_i}, T_{C_i}, W_1, M_3\}$ without recovering the secret key to compute the MAC code. This type of forgery might be useless to mount against the new protocol because a message should have a certain format to pass the validation check, which is matching the MAC codes and comparing them. Therefore, it is necessary to consider a message authentication code to design a good protocol as well as providing data origin authentication.

5.7.3 Symmetric Key Cryptography

Cryptography is the art of disguising information during data transmission and it adequately addresses information security in a way that prevents malicious activities. Encryption algorithms are divided into two groups based on the key type: symmetric or secret key, and asymmetric or public key encryption. In symmetric key encryption both the sender and recipient use the same secret key to encrypt and decrypt, whereas in asymmetric key encryption, the sender and the receiver each have distinct private and public keys. Symmetric encryption should be thought of as a method that can handle the problem of privacy and secrecy. Encryption alone does not protect data from alteration by another party, but the advantages of symmetric encryption should be obvious in that it conceals the contents of the messages exchanged such as password, hash values and other sensitive data.

In contrast to asymmetric encryption, which is considered very computationally intensive, symmetric encryption is computationally light. The sender and receiver use a shared key to encode and decode the messages, thus privacy can be enforced even if a third party listens to the conversation. In summary, symmetric encryption provides secrecy and confidentiality. The purpose of using symmetric encryption over other algorithms is because it is designed to be computationally fast and simple. Also, it can accommodate high rates of data throughput (Menezes *et al*., 2010). The main goal of using symmetric key cryptography is to maintain an efficient way of achieving confidentiality and prevent any act of eavesdropping, thus attaining a secure channel between the client and server during negotiation and mutual authentication.

5.8 DISCUSSION

Enhancing the result of merging the two protocols is significantly essential. Without the adjustments, both protocols do not apply any encryption mechanisms and this increases the likelihood of exploit. Insecure protocols can be threatening because an eavesdropper gets to observe any sensitive data exchanged between a client and a server.

The merits of both protocols after merging still exist in the new protocol. The security of the new protocol is equivalent to the security of Diffie-Hellman key exchange, which provide perfect forward secrecy. The client and the server agree on the key session during the handshake based on prior information without allowing an eavesdropper to obtain a copy of the session key. The handshake in the new protocol is based on ECC, both the client and the server's random numbers are disclosed and it is hard for an attacker to reverse engineer random numbers. In the system initialisation phase, the server selects an elliptic curve equation $E_P(a, b)$ and a base point P with the order n over $E_P(a, b)$ and shares these values with the client. The key exchange mechanism in the new protocol follows the same step on ECC key exchange:

(1) The client generates a random number r_C, then computes $W_1 = r_C \, . \, P$ and sends it to the server.

(2) The server generates a random number r_S, then computes $W_2 = r_S \, . P$ and sends it to the client.

(3) The client computes $r_C \, . \, W_2$, which equals to $r_C . \, r_S \, . \, P$.

(4) The server computes $r_S \, . \, W_1$, which equals to $r_S \, . \, r_C \, . P$.

At this stage, the client and the server now share the point $r_S \, . \, r_C \, . P$ to create the

session key.

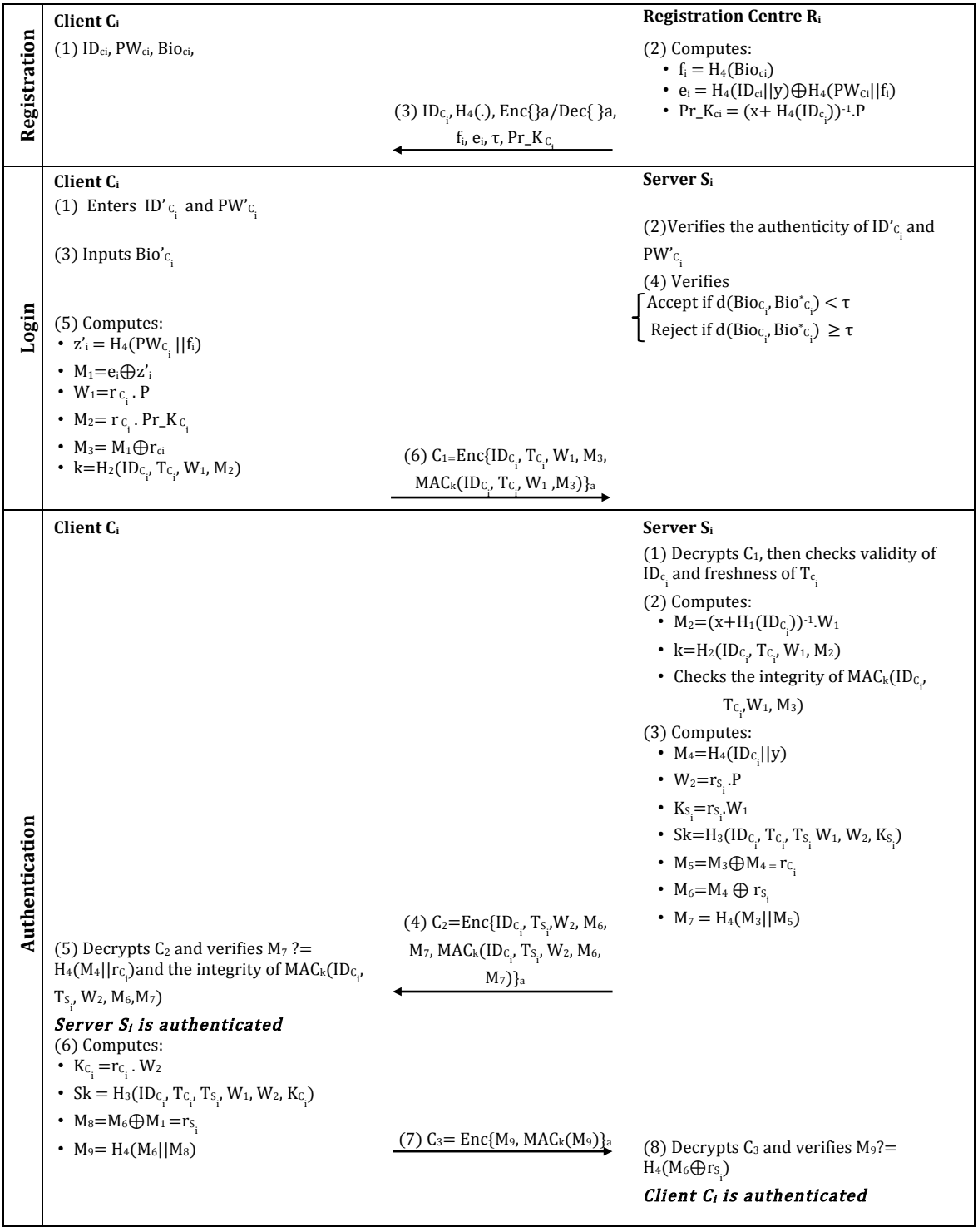
However, the security of key exchange does not prevent other attacks like man-in-the-middle attack, parallel session attack and reflection attack as demonstrated in Chapter 7. To protect the messages from passive attacks such as eavesdropping, it is necessary to send the messages in encrypted form. For this reason, the new protocol uses a secret key cipher to encode the messages using the mutually agreed secret key *a*.

In the new protocol, the contents of the message exchange are not exposed to spoofing attacks. The method of authenticate-then-encrypt is used where every message is concatenated with MAC code for an integrity check and then encrypted via symmetric encryption. However, this method may raise other security concerns and make the new protocol vulnerable to a chosen cipher-text attack. This flaw will be discussed explicitly in Chapter 7.

5.9 SUMMARY

The proposed authentication protocol is based on a three-way handshake mechanism, which is the kernel of the protocol. This mechanism is applied to negotiate the secure components of a session between the client and server, such as verifying the identity of the client using biometric and password information, agreeing on cryptographic algorithms, mutually authenticating each other and using biometric and ID-based encryption over ECC to generate session keys. The proposed protocol allows the client and the server to exchange encrypted messages between each other. The symmetric cryptography is used to ensure that the subsequent messages are protected during transmission. Since encryption does not automatically protect data against

modification, each message contains a MAC to alert the receiver in case the message has been tampered with. Figure 5.1 summarises the phases of the new protocol.



Protocol 5.1. The new protocol

6

Performance and Behaviour Modelling

This chapter starts by giving a brief definition of extended finite state machines (EFSM). Then it elaborates the details of the finite-state verification of the proposed protocol and identifies the functionality of each phase. Also, it studies the behaviour of each machine created for each phase and how they interrelate together.

6.1 Protocol Model and State Machine

Protocol modelling is a crucial step in designing security protocols. It contributes to diminishing ambiguity and misinterpretation of protocol specifications. For example, modelling a protocol using a finite-state machine (FSM) can help to understand how it will interact with changes and how it will behave with invalid inputs. A finite-state machine is a powerful tool to simulate software architecture and communication protocols. FSM can only model the control part of a system and consists of a finite number of states, a finite number of events and a finite number of transitions.

In order to model the complex behaviour of the proposed protocol, an extended model of FSM is considered. According to Alagar and Periyasamy (2011), EFSM helps to comprehend the *state space* complexity of a system when the number of states and transitions increases. They also emphasise the importance of introducing *state variables* into FSM models. State variables play a key role in modelling because they can *define a range of arithmetic and logical operators to manipulate state variables and trigger transitions based on logical primitives* (Alagar *et al*., 2011). Moreover, EFSM with variables can transfer variable values from one model to another. Consequently, the produced output value from one machine can be consumed by other machines. With the introduction of variables, EFSM allows one to model a system with conditions. Transitions may have guards and predicates, which consist of operations or Boolean-valued expressions that can depend on input variables (Alagar and Periyasamy, 2011). A formal definition of an EFSM is as follows (Androutsopoulos *et al*., 2009; Alagar and Periyasamy, 2011):

An Extended Finite State Machine (EFSM) is defined by the tuple $M = (S, T, E, V)$, where:

S is a set of states,

T is a set of transitions,

E is a set of events, and

V is a store represented by a set of variables.

Transitions have a source state $source(t) \in S$, a target state $target(t) \in S$ and a label $lbl(t)$. Transition labels are of the form $e1[c]/a$ where $e1 \in E$, c is a condition and a is a sequence of actions.

The EFSM is used to model the communication channel of the new protocol between the Client C_i and the Server S_i. Since the exchange of packets follows a pattern defined by a finite set of rules, each principal in the protocol has a corresponding state machine: $EFSM_{server}$, $EFSM_{register}$ and $EFSM_{client}$.

6.2 SERVER EFSM

The EFSM at the server side represents the various on-going communications with the client at any point in time. It is modelled using 10 states and 22 transitions as detailed below in Table 6.1. Figure 6.1 illustrates the server machine modelled by EFSM.

Table 6.1: THE TRANSITIONS SPECIFICATION OF THE SERVER-SIDE EFSM

Transition	Transition Direction	Guards/Condition
Waiting for clients	S0 → S0	-
Request to enrol	S0 → R0	ClientEnrol == True
Client is registered	S0 → S1 R0→S0	ClientReg == True
Enter ID	S0 → S1	ID Valid
Enter Password	S1 → S2	Password Valid
Submit Biometric	S2 → S3	Biometric Valid
Request client login (SYN received)	S3 → S5	
Re-enter ID/Password/Biometric	S2→S2 S3→S3 S4→S4	ID_attempt < 3, ID_attempt = ID_attempt +1 PW_attempt < 3, PW_attempt = PW_attempt +1 Bio_Attempt == < 3, Bio_attempt = Bio_attempt +1
Invalid ID/Password/Biometric	S2→S4 S3→S4 S4→S4	ID_attempt == 3 PW_attempt == 3 Bio_Attempt == 3
Send SYN/ACK and C2	S5→S6	$T` - T_{C_i} \leq \Delta T$ $Server\_MAC_k$ == Client_MAC
Client ACK and C3 received	S6→S7	
Terminate	S5→S8 S6→S8	
Timeout	S1→ S0 S2→S0 S3→S0	

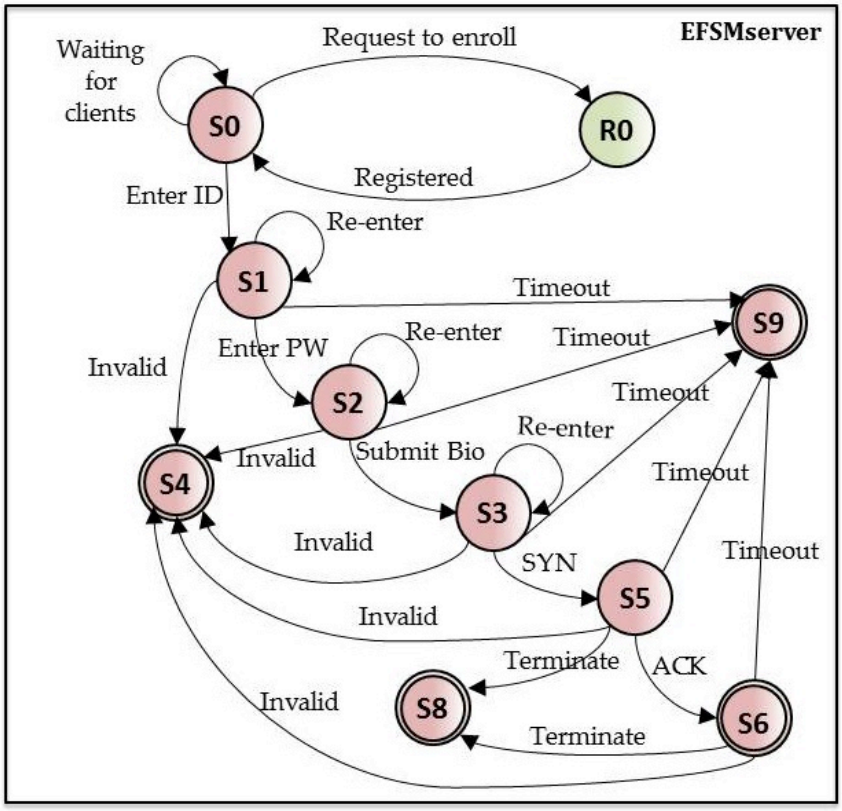


Figure 6.1: The server machine modelled by EFSM

1) The $EFSM_{server}$ will loop itself as the server is waiting for clients. The machine advances to the next state once it is triggered by a login/enrol transition accordingly.
2) When the $EFSM_{server}$ is in the state S1, it checks the validity of the received ID. If ID is proved to be incorrect, S_i will request C_i to enter the valid ID for three times and $EFSM_{server}$ will loop until C_i enters the valid ID or if the attempts exceed three times. In the latter case, the C_i's account will be blocked and $EFSM_{server}$ will change to state S4 from state S1. Generally, three attempts are made through our protocol steps to allow common errors.

3) When the $EFSM_{server}$ is in the state S2, it is triggered by valid ID and it is now waiting for a valid PW. Once S_i receives PW, it verifies the validity of PW. If PW is proved to be wrong, S_i will request C_i to enter the valid PW for three times and $EFSM_{server}$ will loop until C_i enters the valid PW or if the attempts exceed three times. In the latter case, the C_i's account will be blocked and $EFSM_{server}$ changes state to S4 from state S2.

4) When the $EFSM_{server}$ is in the state S3, it is triggered by valid PW and it is now waiting for a valid Bio. Once S_i receives Bio, it verifies the validity of Bio by comparing the imprinted Bio with the template stored. If Bio does not match the stored template, S_i will request C_i to enter the valid Bio up to three times and the $EFSM_{server}$ will loop until C_i enters the valid PW or if the attempts exceed three times. In the latter case, the C_i's account will be blocked and the $EFSM_{server}$ changes state to S4 from state S3.

5) In state S5, the $EFSM_{server}$ waits until it receives the login request $SYN = \{ID_{C_i}, T_{C_i}, W1, M3, MAC_k(ID_{C_i}, T_{C_i}, W_1, M_3)\}_a$ from the FSM_{client} to establish a connection by performing the three-way handshake.

6) While in state S5, the $EFSM_{server}$ checks the validity of ID, freshness of T and the integrity of MAC_k. Then S_i generates a random number and timestamp in order to calculate the session key $sk = H_3(ID_{C_i}, T_{C_i}, T_{S_i}, W_1, W_2, K_{S_i})$. After that, S_i replies with the $SYN/ACK = \{ID_{C_i}, T_{S_i}, W_2, M_6, M_7, MAC_k(ID_{C_i}, T_{S_i}, W_2, M_6, M_7)\}_a$ to the $EFSM_{client}$.

7) In state S6, $EFSM_{server}$ waits until it receives the ACK from the $EFSM_{client}$. Once the $EFSM_{client}$ sends $ACK = \{M_9\}_a$, EFSMserver verifies

$M_9 \stackrel{?}{=} H_4\ (M_6\ //\ r_{S_i})$. In this instance, $\boldsymbol{S_i}$ authenticates $\boldsymbol{C_i}$ as a legitimate user.

8) At state S5 and state S6, $EFSM_{server}$ terminates the current session if any of the following situations occurs:
    - The client ID is invalid
    - The freshness of $T' - T_{C_i} \geq \Delta T$
    - Negative result when checking the integrity of $MAC_k(ID_{C_i}, T_{C_i}, W_1, M_3)$
    - $M_9 != H_4\ (M_6\ //\ r_{S_i})$

At any stage of $EFSM_{server}$, $EFSM_{server}$ aborts the current session and changes to state S9 if the timeout exceeds the defined TIME_WAIT while waiting for packets. This feature helps to prevent an infinite from waiting when the $EFSM_{client}$ fails to respond.

6.3 CLIENT EFSM

The EFSM at the client side represents the various on-going transmissions with the server at any point in time. It is modelled using 9 states and 21 transitions as detailed in Table 6.2 below. Figure 6.2 shows the transitions diagram for the $EFSM_{client}$.

1) First, the $EFSM_{client}$ is in the initial state C0. That is when the request for register/login is initiated by itself. While in state C0, the $EFSM_{server}$ checks whether $\boldsymbol{C_i}$ is enrolled or not. The next state will be decided according to the condition $ClientReg == True$.

TABLE 6.2: THE TRANSITIONS SPECIFICATION OF THE CLIENT-SIDE EFSM

Transition	Transition Direction	Guards/Condition
Request to enrol	C0 → R0	ClientEnrol == True
Client is registered / Enter ID	C0 → C1	ClientReg == True
Enter Password	C1 → C2	ID valid
Submit Biometric	C2 → C3	Password valid
Send login request SYN (C_1)	C3 → C5	Biometric valid
Re-enter ID/Password/Biometric	C1→C1 C2→C2 C3→C3	ID_attempt < 3, ID_attempt = ID_attempt +1 PW_attempt < 3, PW_attempt = PW_attempt +1 Bio_Attempt < 3, Bio_attempt = Bio_attempt +1
Invalid ID/Password/Biometric	C1→C4 C2→C4 C3→C4	ID_attempt == 3 PW_attempt == 3 Bio_Attempt == 3
Client receives SYN/ACK (C2)	C5→C6	
Client sends ACK (C3)	C6→C7	$M_8 == H_4(M_4 \mid\mid r_{C_i})$ $Client\_MAC_k == Server\_MAC$
Authenticated by server	C7→C8	
Terminate	C5→C8 C6→C8	
Timeout	C1→C0 C2→C0 C3→C0	

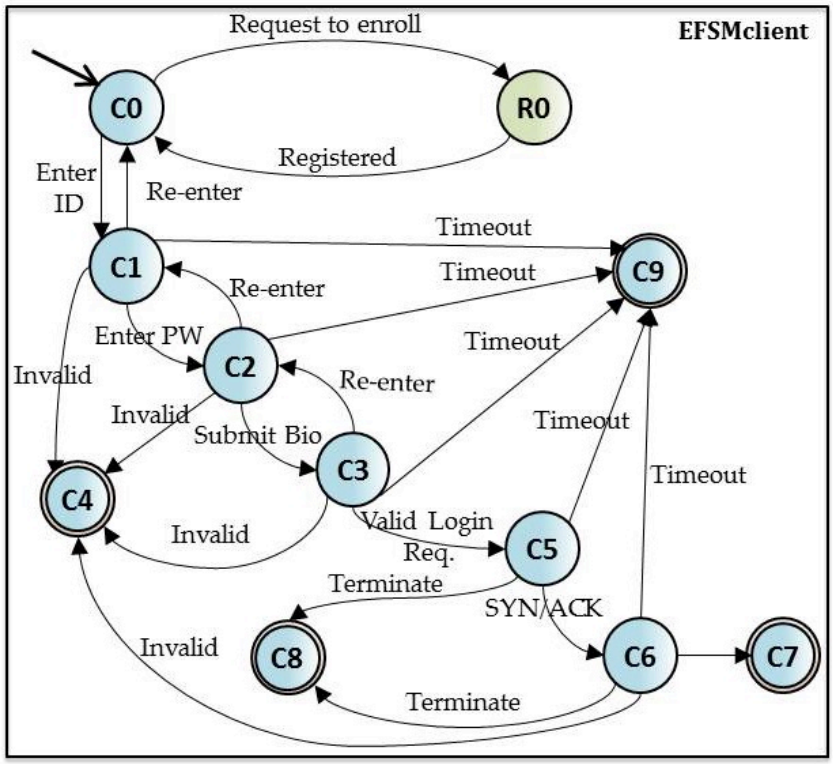


Figure 6.2: The client machine modelled by EFSM

2) In state C1, C2, C3, the FSM_{client} is waiting for validating ID, PW, and Bio. Once the client credentials are validated, the $EFSM_{client}$ triggers itself and changes to state C5.
3) In states C1, C2, C3, the client may be required to re-enter ID, PW, Bio in case they were incorrect. However, the client's account will be blocked if the number of attempts exceeds three, which changes the above states to state C4.

- $\text{ID\_attempt} < 3, \text{ID\_attempt} = \text{ID\_attempt} + 1$
- $\text{PW\_attempt} < 3, \text{PW\_attempt} = \text{PW\_attempt} + 1$
- $\text{Bio\_Attempt} < 3, \text{Bio\_attempt} = \text{Bio\_attempt} + 1$

4) In state C5, The $EFSM_{client}$ generates a random number and timestamp to calculate the encrypted login request $\{ID_{C_i}, T_{C_i}, W_1, M_3, MAC_k(ID_{C_i}, T_{C_i}, W_1, M_3)\}_a$ and sends it to the $EFSM_{server}$. This request represents the SYN part in the three-way handshake procedure.
5) While in state C5, the FSM_{client} is waiting for the $EFSM_{server}$ to respond after sending the login request in order to establish the connection.
6) In state C6, the $EFSM_{client}$ is validating the $EFSM_{server}$ response by checking the integrity of MAC_k, ΔT and $M_7 \stackrel{?}{=} H_4(M_4 \,||\, r_{C_i})$. If $\boldsymbol{S_i}$ proves legitimate, $\boldsymbol{C_i}$ authenticates $\boldsymbol{S_i}$ at this stage.
7) While in state C6, the $EFSM_{client}$ computes the shared session key $sk = H_3(ID_{C_i}, T_{C_i}, T_{S_i}, W_1, W_2, K_{C_i})$ and finalises the handshake procedure by sending the $ACK = \{M_9\}_a$ to $\boldsymbol{S_i}$.
8) In state C7, the $EFSM_{client}$ is waiting to be authenticated by server.
9) In state C8, the client terminates the current session if one of the following occurs:
    - Negative result when checking the integrity of MAC_k
    - $T^* - T_{S_i} \geq \Delta T$
    - $M_7 \stackrel{?}{=} H_4(M_4 \,||\, r_{C_i})$

At any stage of $EFSM_{client}$, $EFSM_{client}$ aborts the current session and changes to state C9 if the timeout exceeds the defined TIME_WAIT while waiting for packets. This feature helps to prevent an infinite wait when the $EFSM_{server}$ fails to respond.

6.4 REGISTER EFSM

The EFSM at the registration side represents the various on-going transmissions with the server and the client at any point in time. It is modelled using EFSM with 4 states and 7 transitions. Figure 6.3 shows the states and transitions diagram for the $EFSM_{register}$.

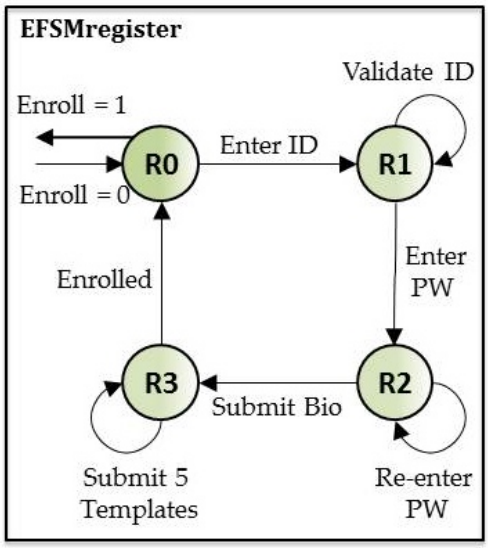


Figure 6.3: The register machine modelled by EFSM

1) First, the $EFSM_{register}$ is triggered if the client is not enrolled at state R0. That is when the request for registration is initiated by $EFSM_{client}$. While in state C0, the $EFSM_{server}$ checks whether C_i is enrolled or not.
2) Once C_i enters ID, $EFSM_{register}$ changes to state R1 and validates the format of ID. Then $EFSM_{register}$ triggers itself asking C_i to enter PW and changes to state R2.
3) In state R2, on receiving PW for the first time, $EFSM_{register}$ requires C_i to re-enter PW for confirmation. Then it triggers itself and changes to the state R3.

4) In state R3, C_i is required to submit multiple scans of the biometric data to increase accuracy. Once the acquisition process is complete, $EFSM_{register}$ triggers itself and sends a message to $EFSM_{register}$, which indicates that the enrolment is successful.

6.2 Behaviour Evaluation

The capability to detect errors and vulnerabilities is essential in protocol design implementation. Since communication protocols are partially specified, the finite state approach provides a flexible way to detect invalid inputs and ambiguous specifications, which are usually unspecified or vague in protocol design. Testing the new protocol with FSM helps to verify whether the protocol complies with its specification or not. Modelling with FSM shows that the new protocol can function correctly and behave properly even with invalid input or time delay.

The state machine in Figure 6.4 represents the result of combining the three machines together. The composite model executes according to the protocol description and handles error in a safe manner and it performs certain action in case of unreliable state. Each valid and reachable state generates a valid protocol state and the transitions can be triggered by either events or guards.

Predicating and considering all possible combinations of both desirable and undesirable states are one way to fully understand the complexity of the proposed protocol. Based on the equivalent behaviour, each machine may follow nondeterministic behaviour and produce different outputs according to the original input. For example, if $EFSM_{client}$ generates an illogical input for the authentication process then $EFSM_{client}$ rejects the session and goes to the *terminate state*.

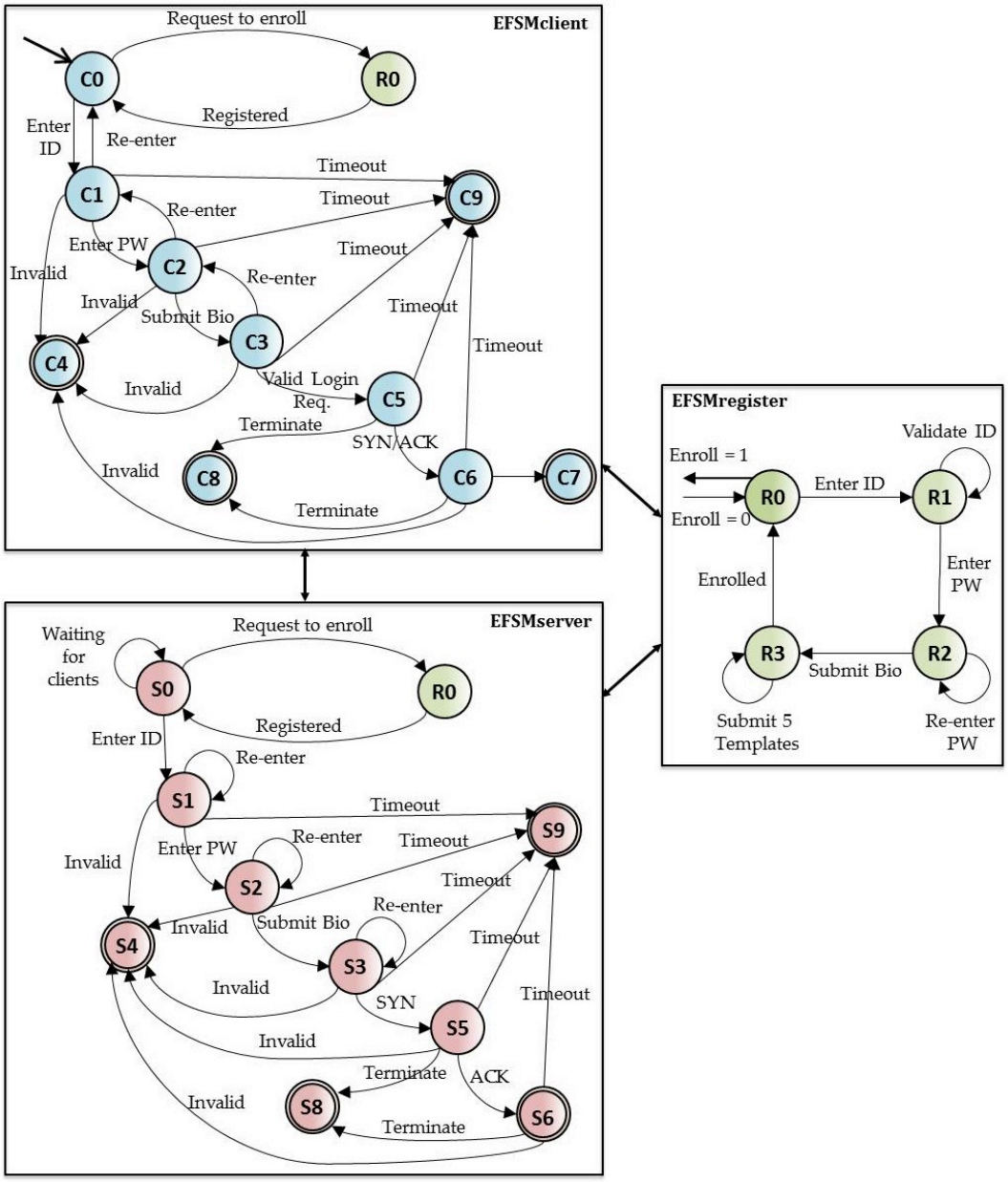


Figure 6.4: The new protocol modelled by EFSM

Note that the following states S9 and C9 are defined in terms of a timeout being reached with an inability to complete mutual authentication. The states S4 and C4 are defined in terms of an invalid input being injected due to an invalid ID, wrong

password, or unmatched biometric. The states S8 and C8 are defined in the case of unreliable actions being performed for example, if the integrity or validity check failed. Furthermore, a state machine hierarchy or hierarchical FSM is used to provide a more concrete level of refinement; $FSM_{register}$ can be refined by introducing an "Enrol" feature. This state determines if the client is pre-enrolled or not. The state R0 becomes a new EFSM with three states R1, R2, R3 as described in section 6.4.

6.3 Performance Evaluation

Theoretically, the computation cost for the proposed protocol is relatively low and efficient since lightweight algorithms are applied, such as symmetric encryption, hash operations and XOR operations. On one hand, symmetric encryption provides secrecy and prevents active attack. On the other hand, MAC provides integrity and authenticity. Another important point to stress is that the symmetric key computation for encryption and decryption is similar to hash function operations (Feldhofer and Rechberger, 2006)

The handshake in the new protocol based on ECC tends to be faster than the handshake based on RSA. Lauter (2004) and Gupta *et al*.(2002) showed that an ECC is roughly 5 to 15 times as fast as RSA at the 163-bit ECC/1024-bit RSA security level and the ratio increases between 20 and 60 at the 256-bit ECC/3072-bit RSA security level. This analysis shows the advantage of ECC over RSA. Moreover, ECC has significant advantages over other public-key cryptography because ECC provides the same security level of RSA cryptosystem, but with a shorter key length and faster computation (Yokoyama, 2000)

Even though the number of operations is greater than those of other schemes, the scheme holds some other security properties. The proposed protocol is based on a two-factor user authentication mechanism and it is obvious that it takes a few more hash operations and XOR operations for the server and client. Due to the security weaknesses in related schemes, the authenticate-then-encrypt method is applied to ensure the confidentiality and the integrity of transmitted packets. This feature makes the new scheme more efficient in terms of performance and security.

6.4 SUMMARY

This chapter started by giving a brief definition of extended finite state machines (EFSM). Then it discussed the details of the finite-state verification of the new protocol and identifies the functionality of each phase. Also, it studied the behaviour of each machine created for each phase and how they interrelate together.

The composite model executes efficiently and handles error in a safe manner according to their types. The new protocol connection progresses from one state to another based on the data pertained from the message exchanged. EFSM helps to understand the behaviour of the protocol and detects any unwanted behaviours.

7

Security Evaluation

The first step of analysis is modelling the protocol. This chapter presents a Petri net (PN) approach to model, simulate and analyse the new protocol. A formal approach like Petri nets allows one to represent communication protocols. For the sake of simplicity, a complex PN model will not be discussed until all attacks are demonstrated and the model is proved to be secure. This chapter shows how Petri nets are used to model and analyse the cryptographic protocol. First, the proposed protocol is modelled without an adversary, and then a generic adversary model is added to examine all possible behaviour of the adversary.

7.1 CRYPTOGRAPHIC PROTOCOL AND PETRI NETS

Due to the unique characteristics possessed by cryptographic protocols, analysis and evaluation tend to be more difficult than network protocols, which send data in unencrypted form such as the Hypertext Transfer Protocol (HTTP) and Telnet. Typically cryptographic protocols, also known as security protocols, tend to inhabit a complex environment by utilising various cryptographic mechanisms, such as symmetric and asymmetric encryption, hash functions, timestamps and digital signature (Ryan and Schneider, 2001).

For this reason, Petri Nets offer the opportunity to conduct an in-depth analysis and overcome security vulnerabilities and weaknesses. Moreover, they simplify the modelling of exchange messages between nodes and describe the behaviour of authentication and key agreement procedure. A number of researchers have used Petri nets to model and analyse cryptographic protocols such as Nieh and Taveres (1993), Al-Azzoni *et al*. (2005), Dresp (2005), Permpoontanalarp and Sornkhom (2009) and Xu *et al*. (2001) and there are more examples besides these.

Petri nets are a finite-state analysis approach that explicitly provides a graphical description for cryptographic protocols. They pay attention to specific properties such as liveness, deadlock, livelock, and boundedness.

Outline of the technique:

The following steps explain the methodology to model the proposed protocol with Petri Nets (PN):

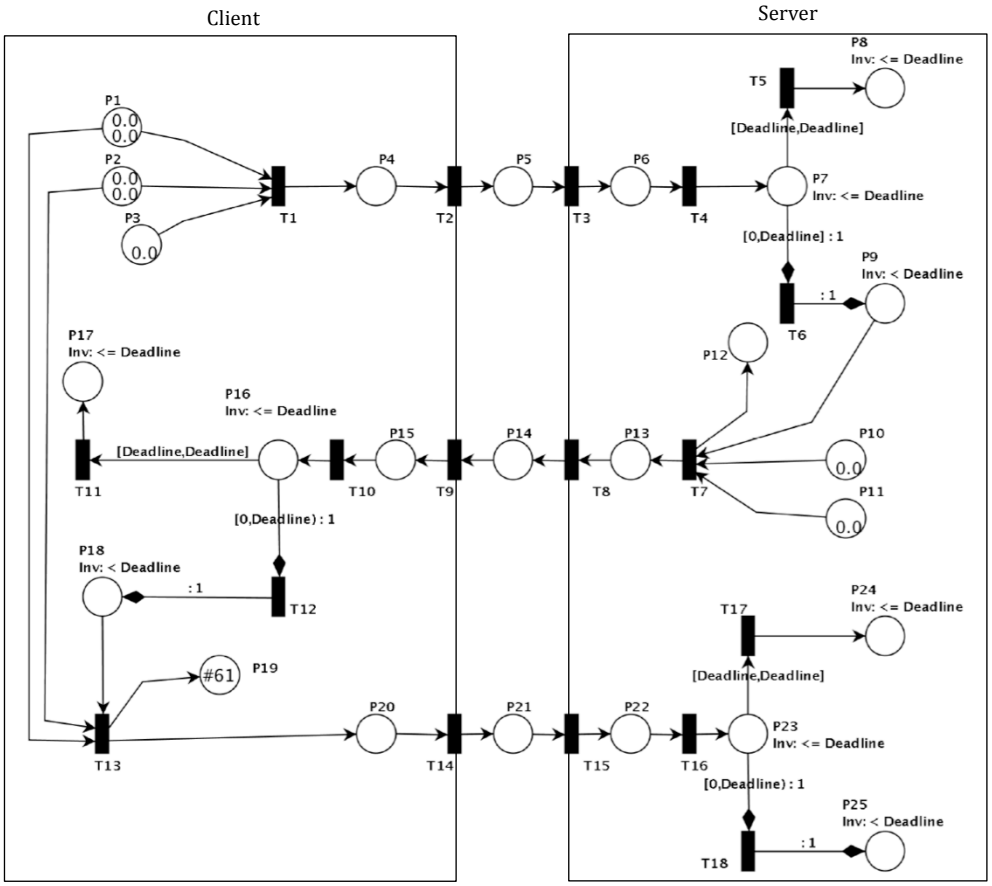
1) Build a PN trust model using TAPAAL simulation and verification software. The following steps are necessary for the process of modelling:
    (a) Define the places and transitions and declare their functionalities.
    (b) Implement a token passing scheme once the initial marking is set.
    (c) Assess the model's behaviour by examining reachability, boundedness, and liveness.
    (d) Validate the model using simulation.
2) Add an adversary entity. This step involves the following:
    (a) Extend the original model and define places and transitions for the adversary entities.
    (b) Implement the token-passing scheme with the adversary.
    (c) Model different attacks and identify any insecure behaviour.

7.2 CLIENT-SERVER TRUST MODEL

The trust model is a notation for determining the organisations should trust with its assets. For example, organisations usually verify the applicants' resumes and references to conduct background and history checks before trusting their employees. Once they are employed, they will be issued photo ID badges and parking permits. In contrast to the real world, it is challenging in the virtual world to identify individuals who are trusted and those who are not. A trust relationship between a client and a server can be obtained in different practices. Some systems use the traditional way that relies on usernames, passwords and digital certificates. Sometimes it may involve a trusted third party to operate the authentication and validation, such as the

Kerberos login protocol and Shibboleth authentication, while other systems deploy biometric automated verification systems to recognise trusted users.

In the proposed trust model, the client-server trust relationship is initiated during the registration phase. First, the client submits his/her ID, password (PW_{C_i}), and biometric data (Bio_{C_i}). Then the server will issue in return a corresponding private key ($Pr\_K_{C_i}$), secret key (a) for the symmetric encryption, and τ the predetermined threshold for biometric verification. The assumption for this model is that the client and server are trustable entities, and they never cheat. Timed-arc Petri nets are used to model the new protocol. The trust model consists of two entities: one for the client, $\boldsymbol{C}$, and the other for the server, $\boldsymbol{S}$. The protocol entities are derived from the protocol description in Chapter 5. The assumption made for this model is that each legitimate participant is honest, i.e. behaves according to the protocol rules. The Petri net model in Figure 7.1 represents the trust model for the new protocol. The definitions of the places and transitions used in this model are illustrated in Table 7.1 and Table 7.2, respectively.



(a)

P={P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13}, P_{14}, P_{15}, P_{16}, P_{17}, P_{18}, P_{19}, P_{20}, P_{21}, P_{22}, P_{23}, P_{24}, P_{25}}

T = {T_1, T_2, T_3, T_4, T_5, T_6, T_7, T_8, T_9, T_{10}, T_{11}, T_{12}, T_{13}, T_{14}, T_{15}, T_{16}, T_{17}, T_{18}}

***M_0*: {2, 2, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,0}**

$I(T_1)=\{P_1,P_2,P_3\}$	**$I(T_{10})=\{P_{15}\}$**	**$O(T_1)=\{P_4\}$**	**$O(T_{10})=\{P_{16}\}$**
$I(T_2)=\{P_4\}$	**$I(T_{11})=\{P_{16}\}$**	**$O(T_2)=\{P_5\}$**	**$O(T_{11})=\{P_{17}\}$**
$I(T_3)=\{P_5\}$	**$I(T_{12})=\{P_{16}\}$**	**$O(T_3)=\{P_6\}$**	**$O(T_{12})=\{P_{18}\}$**
$I(T_4)=\{P_6\}$	**$I(T_{13})=\{P_1,P_2,P_{18}\}$**	**$O(T_4)=\{P_7\}$**	**$O(T_{13})=\{P_{19},P_{20}\}$**
$I(T_5)=\{P_7\}$	**$I(T_{14})=\{P_{20}\}$**	**$O(T_5)=\{P_8\}$**	**$O(T_{14})=\{P_{21}\}$**
$I(T_6)=\{P_7\}$	**$I(T_{15})=\{P_{21}\}$**	**$O(T_6)=\{P_9\}$**	**$O(T_{15})=\{P_{22}\}$**
$I(T_7)=\{P_9,P_{10},P_{11}\}$	**$I(T_{16})=\{P_{22}\}$**	**$O(T_7)=\{P_{12},P_{13}\}$**	**$O(T_{16})=\{P_{23}\}$**
$I(T_8)=\{P_{13}\}$	**$I(T_{17})=\{P_{23}\}$**	**$O(T_8)=\{P_{14}\}$**	**$O(T_{17})=\{P_{24}\}$**
$I(T_9)=\{P_{14}\}$	**$I(T_{18})=\{P_{23}\}$**	**$O(T_9)=\{P_{15}\}$**	**$O(T_{18})=\{P_{25}\}$**

(b)

Figure 7.1. (a) The client-server trust model (b) Descriptions of trust model

Table 7.1. DEFINITIONS OF PLACES - THE TRUST MODEL

Place	Definition	Place	Definition
P_1	Client random number	P_{14}	Encrypted SYN/ACK
P_2	Client timestamp	P_{15}	Decrypted SYN/ACK
P_3	SYN request	P_{16}	Verification message
P_4	Login request	P_{17}	Rejected request
P_5	Encrypted login request	P_{18}	Accept request – Server is authenticated
P_6	Decrypted login req.	P_{19}	Session key
P_7	Verification message	P_{20}	ACK
P_8	Rejected request	P_{21}	Encrypted ACK
P_9	Accepted request	P_{22}	Decrypted ACK
P_{10}	Server random number	P_{23}	Verification message
P_{11}	Server timestamp	P_{24}	Rejected request
P_{12}	Session Key	P_{25}	Accept request – Client is authenticated
P_{13}	SYN/ACK		

Table 7.2. DEFINITIONS OF TRANSITIONS FOR TRUST MODEL

Trans.	Definition	Trans.	Definition
T_1	Compute login request + SYN	T_{10}	Split the packet and verify
T_2	Encrypt	T_{11}	Drop the packet
T_3	Decrypt	T_{12}	Accept
T_4	Split the packet and verify	T_{13}	Compute ACK and session key
T_5	Drop the request	T_{14}	Encrypt ACK
T_6	Accept	T_{15}	Decrypt ACK
T_7	Compute SYN/ACK and session key	T_{16}	Split the packet and verify
T_8	Encrypt SYN/ACK	T_{17}	Drop the packet
T_9	Decrypt SYN/ACK	T_{18}	Accept

The PN trust model represents a three-way handshake procedure between $\boldsymbol{C}$ and $\boldsymbol{S}$. It allows both $\boldsymbol{C}$ and $\boldsymbol{S}$ to agree on a shared session key over an insecure channel. The steps of protocol analysis for the PN trust model are described as follows:

- At first, the protocol is initiated by a client. The client entity of the PN trust model generates a random value (P_1), a timestamp (P_2), SYN request (P_3) to compute the login request (P_4) within a specific time limit. $\boldsymbol{C}$ sends the encrypted request (P_5) to $\boldsymbol{S}$.

- Upon receiving the request, $\boldsymbol{S}$ will check the age of the token. Note that computing and sending the request to $\boldsymbol{S}$ takes some units of time. $\boldsymbol{S}$ will drop the request if the time processing exceeds the deadline. This is guaranteed by the use of transport arcs that preserve the age of the tokens and the corresponding invariants. Figure (6.3) shows the PN behaviour with time delay. In the second message of the handshake, the server entity generates a random value (P_{10}), and a timestamp (P_{11}) to compute the session key (P_{12}), and a SYN/ACK request (P_{13}). Then $\boldsymbol{S}$ sends the encrypted SYN/ACK (P_{14}) to $\boldsymbol{C}$.
- Upon receiving the SYN/ACK, $\boldsymbol{C}$ checks the token age and computes the session key (P_{19}). At this stage, $\boldsymbol{C}$ authenticates $\boldsymbol{S}$ and sends an enciphered ACK (P_{21}) to $\boldsymbol{S}$.
- Finally, the server entity checks the token age and authenticates $\boldsymbol{C}$.

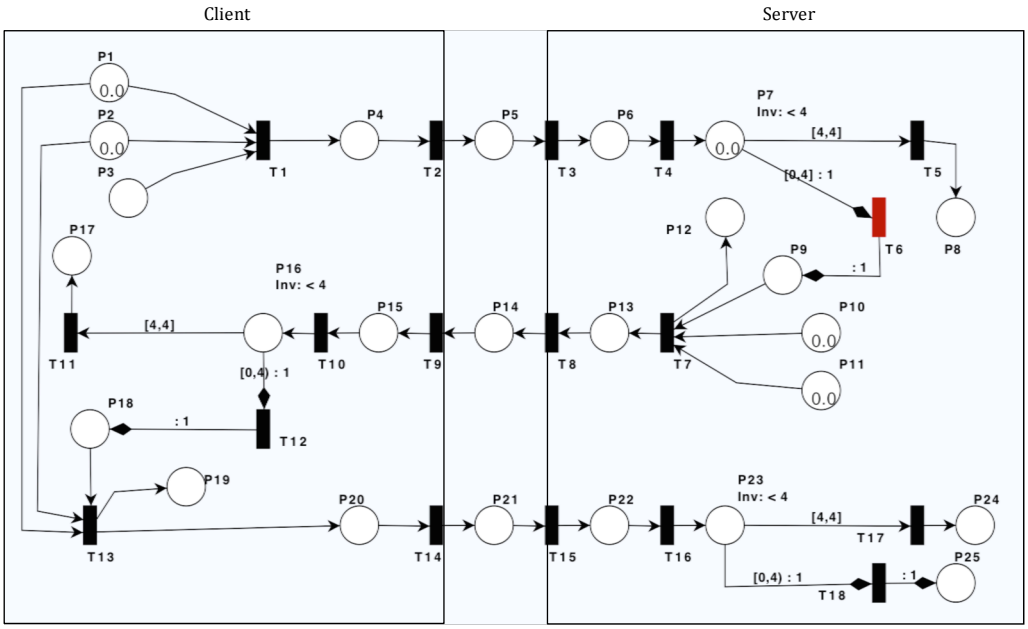
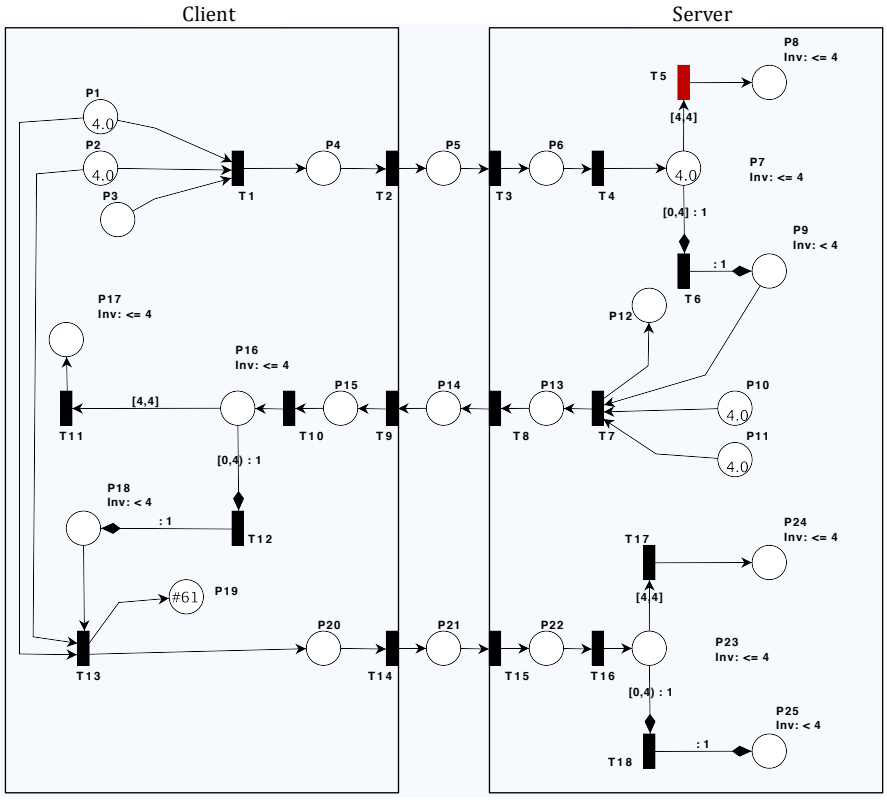
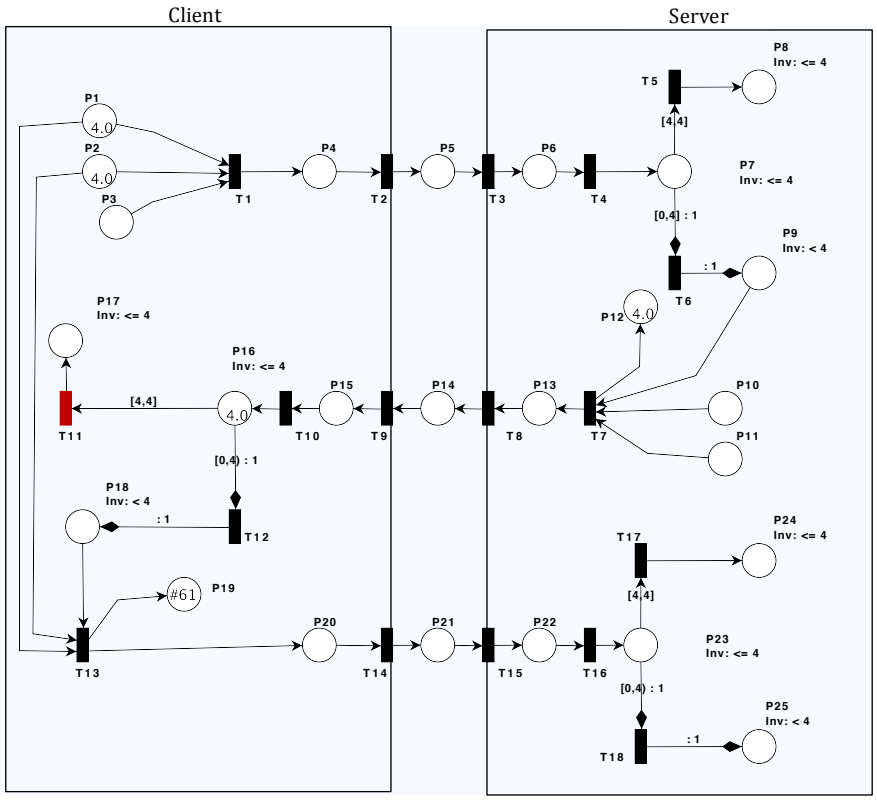


Figure 7.2. The trust model in simulation state



(a)



(b)

Figure 7.3: Trust model with time delay **(a)** Server in rejection state. **(b)** Client in rejection state

After modelling the proposed protocol, it is essential to examine the behavioural properties of the model. Detailed behavioural properties for Petri nets can be found in Murata (1989). Generating a reachability graph (Figure 7.4) allows one to identify the presence and absence behaviours of the modelled protocol.

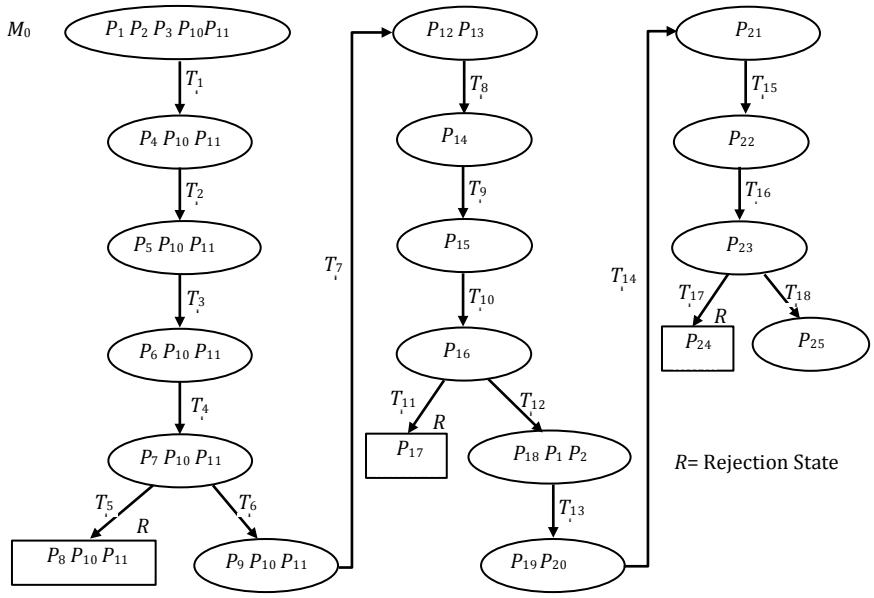


Figure 7.4: Reachability graph for the trust model

A. Reachability:

A reachability or coverability assessment can be conducted by enumerating all states, in other words, deriving all the possible marking the protocol can reach in the model. This method can clearly identify all the enabled transitions starting from the initial state and generating new states after firing transitions. The model shown in Figure 7.1 is bounded. This is evident from the reachability graph (Figure 7.4). The whole set of reachable markings M_i, where i={0,1,2,...,19} are said to be reachable, that is to say there exists a sequence of transition firings which transform one marking state to another.

B. Boundedness and safeness:

Boundedness helps to detect overflows in the modelled system. This property is an indication of the stability behaviour of the model. It is evident that the proposed model is structurally bounded, since each place in the net holds at most two tokens given an initial marking m_0. That is to say, there are a finite number of states in the modelled protocol. Thus, the model has no self-loop and satisfies the condition (Murata, 1989):

A Petri net is k-bounded if all its places are k-bounded.

A Petri net is structurally bounded if it is bounded in any initial marking.

Hence, it can be said that the net is structurally 2-bounded. However, the net is not safe because there are two nodes (P_1, P_2), which contain more than one token. It does not fulfil the safeness condition, which is *1-bounded.*

C. Liveness

The PN has a finite number of dead markings[1]. The transitions (T_5, T_{11}, T_{17}) connected to places (P_8, P_{17}, P_{24}) respectively would not be live if the protocol runs without rejections. Apart from that, the rest of the places and their corresponding firing transitions are live. The occurrence of deadlocks[2] (rejection state), as shown in Figure 7.3, would be a reason for aborting the current session between the client and the server as eventually the token age would exceed the deadline.

[1] A dead marking is a marking where no transition is enabled (Diaz, 2013).
[2] A PN is called deadlock when no transition can fire (Diaz, 2013).

7.3 TRUST MODEL WITH ADVERSARY

The purpose of this analysis is to find weaknesses and flaws in the protocol. It is essential to examine the behaviour of the protocol with the presence of a malicious adversary. An adversary entity can be a hacker, a malicious insider, a disgruntled employee, a terrorist, organised crime, or competitors.

The worst-case scenario would be if attackers obtained illegitimate access to the target system. They could install malicious software, such as a rootkit, to remove or modify data. This act of unauthorised access could lead to privilege escalation and allow the attacker to gain elevated entry to resources that are meant to be protected from other application users. Moreover, faulty protocols may allow an attacker to compromise other machines in the network to act as zombie computers to launch Denial-of-Service attacks.

PN Modelling is capable to the message flow throughout the protocol with an adversary. A high-level view of the adversary model is shown in Figure 7.5.

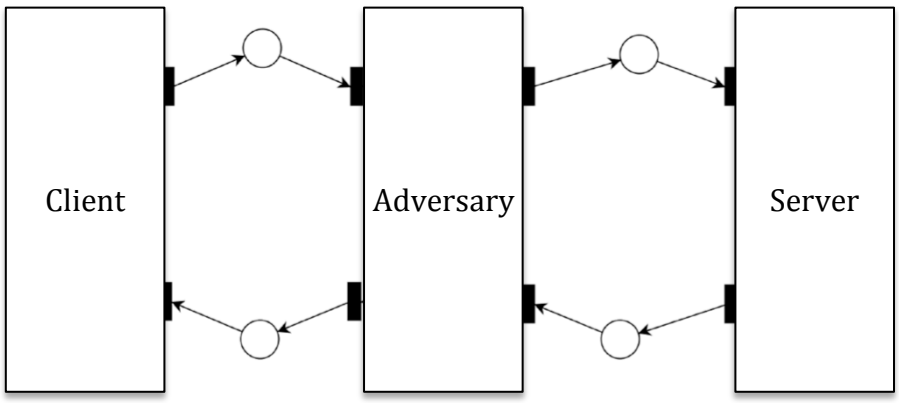


Figure 7.5: High-level view of the adversary entity attacking the protocol

The adversary entity is composed of processes, each designed for a specific function in the protocol. Each process models the adversary's possible actions to capture tokens. It can intercept messages from the channel, alter them, and pass them to the target source. Figure 7.6 below shows an example of a low-level view of an adversary process with information flow.

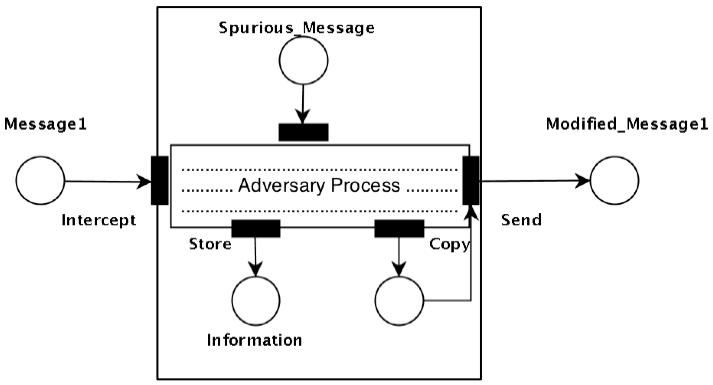


Figure 7.6: Low-level view of adversary process

Conceptually, the adversary entity is non-deterministic, in that it may perform possible actions under different client identities at a given time to ultimately compromise the target system. The following assumptions are considered for the adversary model:

1) The adversary can eavesdrop, intercept, and store a message. It may block or pass any of these messages. Additionally, it may construct forged messages and inject them into the channel.
2) The adversary has zero knowledge such that it does not possess any elements of messages transmitted between the legitimate nodes but it can learn by observing the traffic.
3) The traffic between client and server is not encrypted.

The main goal of the adversary model is to examine the protocol behaviour with the presence of an adversary while modelling attacks. In the adversary model (attack model), the description of the client and the server entities is similar to the trust model as described in section 7.2. For the adversary entity, *places* represent the adversary database, which store control and knowledge and accumulate all the intercepted messages. *Transitions* represent a set of input events and commands the adversary may perform to launch an attack. The *input token* in the adversary entity indicates that the message has been captured. The token movement from place to place through the directed arcs indicates the progress of an attack. To distinguish genuine traffic from forged traffic, the grave symbol ` is used to indicate that the variable could be modified. For example, if the adversary intercepted the message [A, B, C], the output message would be [A`, B`, C`], which means the message has been manipulated by the adversary. A malicious adversary can attempt to abuse an authentication protocol by hijacking a specific session request to gain legitimate access to the target system.

7.4 Analysis of Man-in-the-Middle Attack

After adding an adversary entity to the model, it can be noticed that there is the possibility of a man-in-the-middle between the two entities C and S. An active adversary A can intercept the communication line between a legitimate client and a trusted server as well as manipulate the protocol by using some means to successfully masquerade either as server or client. The attack model in Figure 7.7 represents the man-in-the-middle attack for the proposed protocol. The definitions of the places and transitions used in this model are illustrated in Table 7.3 and Table 7.4, respectively.

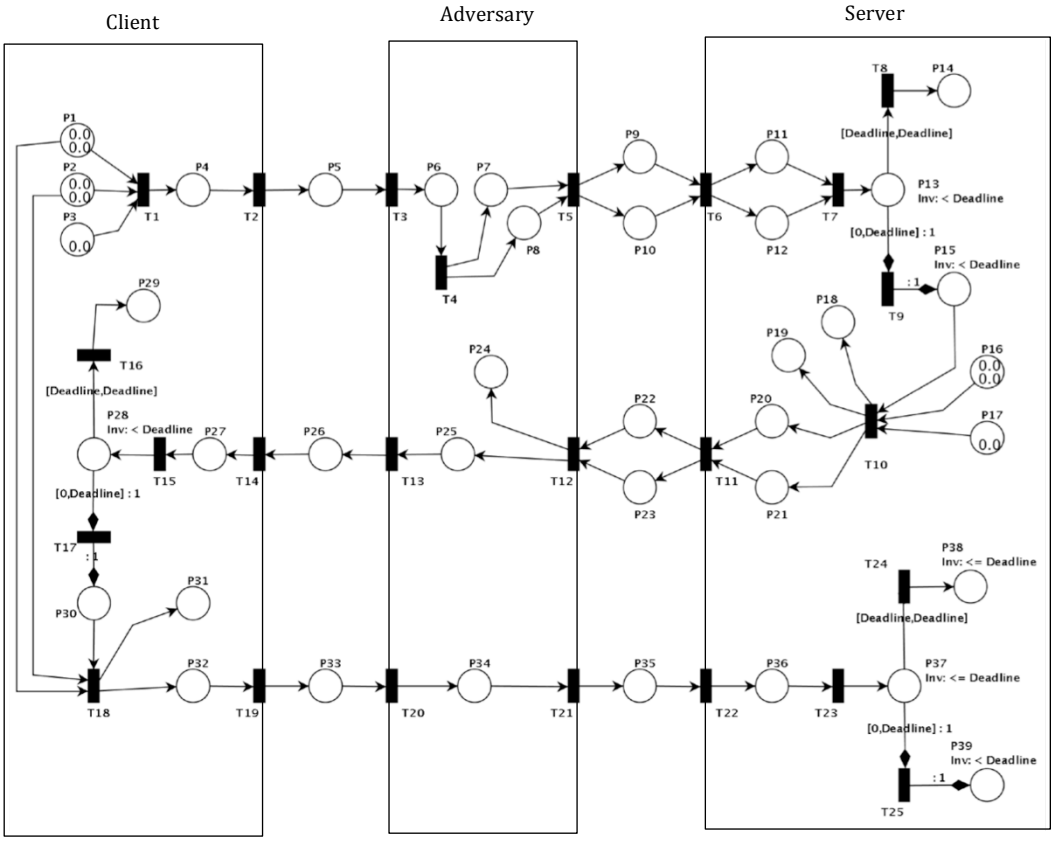


Figure 7.7: Modelling man-in-the-middle attack

Table 7.3: DEFINITIONS OF PLACES – THE-MAN-IN-THE-MIDDEL ATTACKS MODEL

Place	Definition	Place	Definition
P_1	Client random number	P_{21}	SYN/ACK for C
P_2	Client timestamp	P_{22}	Sent SYN/ACK for A
P_3	SYN request	P_{23}	Sent SYN/ACK for C
P_4	Login request	P_{24}	Received SYN/ACK for C
P_5	Sent request	P_{25}	Received SYN/ACK for A
P_6	Intercepted MSG	P_{26}	Sent forge SYN/ACK to C
P_7	Forge MSG A	P_{27}	Received forge SYN/ACK
P_8	Forge MSG C	P_{28}	Verification message
P_9	Sent forge MSG A	P_{29}	Rejected request
P_{10}	Sent forge MSG C	P_{30}	Accept request – A is authenticated
P_{11}	Received forge MSG A	P_{31}	Session key
P_{12}	Received forge MSG A	P_{32}	ACK
P_{13}	Verification message	P_{33}	Sent ACK
P_{14}	Rejected request	P_{34}	Intercepted ACK
P_{15}	Accepted request	P_{35}	Forge ACK
P_{16}	Server random number	P_{36}	Received forge ACK
P_{17}	Server timestamp	P_{37}	Verification message
P_{18}	A Session Key	P_{38}	Rejected request
P_{19}	C Session key	P_{39}	Accept request – A is authenticated
P_{20}	SYN/ACK for A		

Table 7.4: DEFINITIONS OF TRANSITIONS – THE-MAN-IN-THE-MIDDEL-ATTACK MODEL

Trans.	Definition	Trans.	Definition
T_1	Compute login request + SYN	T_{14}	Receive forge SYN/ACK
T_2	Send MSG	T_{15}	Split the packet and verify
T_3	Intercept MSG	T_{16}	Drop the request
T_4	Duplicate MSG	T_{17}	Accept
T_5	Send forge MSG	T_{18}	Compute ACK and session key
T_6	Received Forge MSG	T_{19}	Send ACK
T_7	Split the packet and verify	T_{20}	Intercept MSG
T_8	Drop the request	T_{21}	Send forge ACK
T_9	Accept	T_{22}	Receive forge ACK
T_{10}	Compute SYN/ACK and session key	T_{23}	Split the packet and verify
T_{11}	Send SYN/ACK	T_{24}	Drop the request
T_{12}	Intercept MSG	T_{25}	Accept
T_{13}	Send forge SYN/ACK		

According to Figure 7.7, the man-in-the-middle attack proceeds as follows:

- In the login phase, when the client $\boldsymbol{C}$ initiates and sends the login request P_4 to the server $\boldsymbol{S}$, an adversary $\boldsymbol{A}$ may intercept the login message. Transition T_3 represents the initial phase of the attack. $\boldsymbol{A}$ can duplicate the login message and then start two sessions with $\boldsymbol{S}$ by sending two copies of request: $P_7 = P_8 = [ID`_C, T`_C, W`_1, M`_3, MAC`_k(ID_C, T_C, W_1, M_3)]$ to $\boldsymbol{S}$ as shown in Figure 7.8.

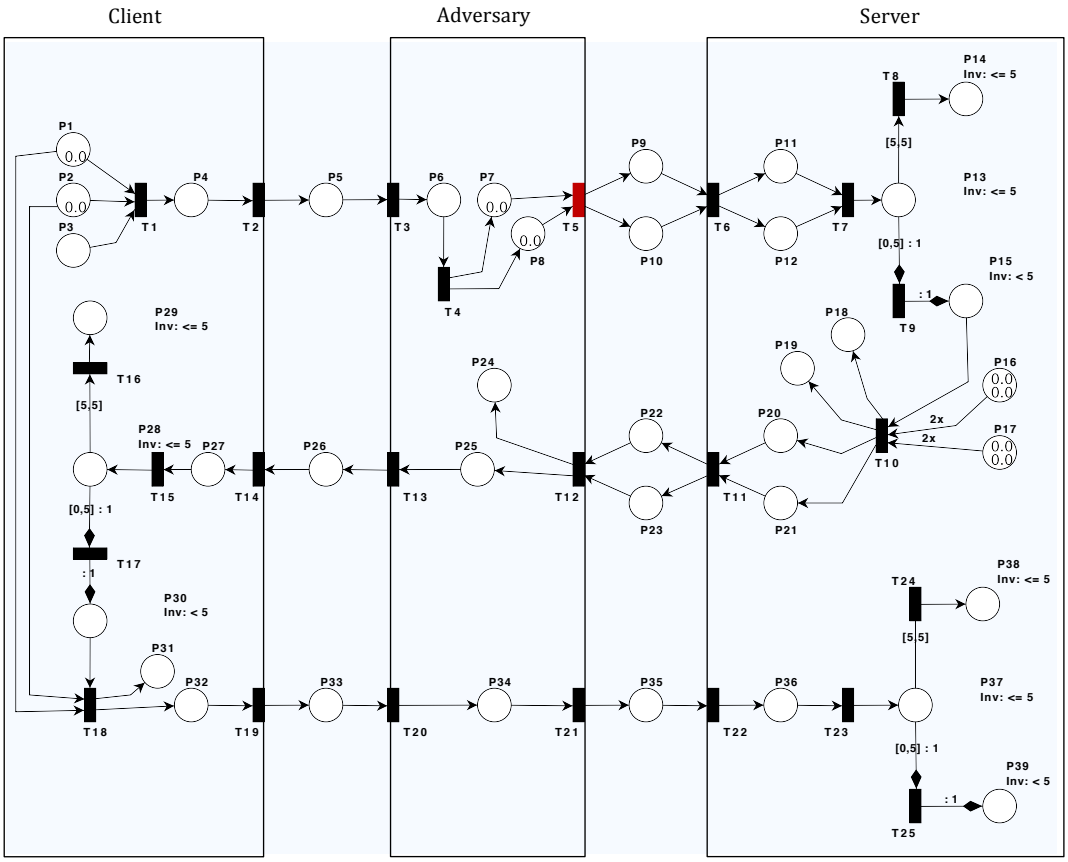


Figure 7.8: The adversary is sending forged messages to server

- Upon receiving P_{11} and P_{12}, $\boldsymbol{S}$ generates two random numbers from (P_{16}) and two timestamps from (P_{17}) and computes the following:
    - Two session keys (P_{18}, P_{19}) for $\boldsymbol{A}$ and $\boldsymbol{C}$, respectively

- Two SYN/ACK messages (P_{20}, P_{21}) for $\boldsymbol{A}$ and $\boldsymbol{C}$, respectively

Then, $\boldsymbol{S}$ sends the messages (P_{22}, P_{23}) for the two sessions respectively.

- In the meantime, $\boldsymbol{A}$ captures (P_{22}, P_{23}) and sends a forged message (P_{25}) to $\boldsymbol{C}$ as shown in Figure 7.9.

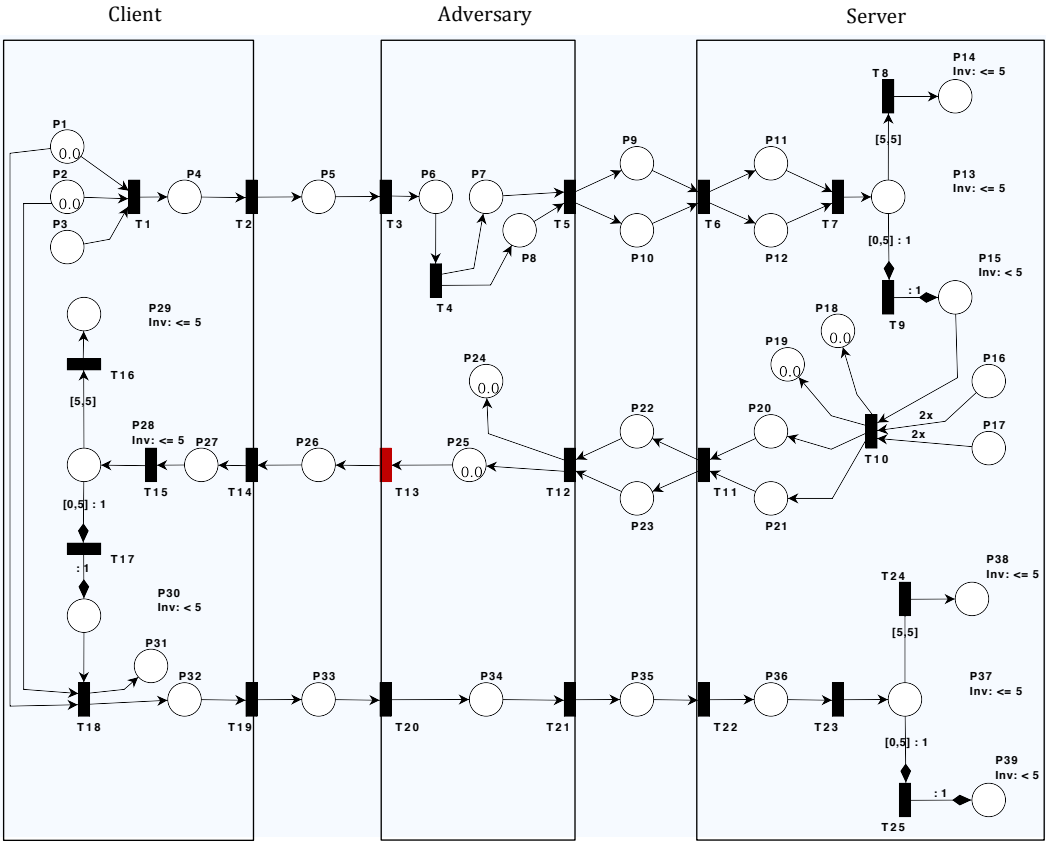


Figure 7.9: The adversary masquerading as server

- After receiving the (P_{27}), $\boldsymbol{C}$ verifies it, which in this case is a genuine request [ID_C, T_S, W_2, M_6, M_7, $MAC_k(ID_C, T_S, W_2, M_6, M_7)$]. Consequently, $\boldsymbol{C}$ authenticates $\boldsymbol{A}$ masquerading as $\boldsymbol{S}$. Then $\boldsymbol{C}$ computes the shared session key (P_{31}) and sends ACK (P_{32}) to $\boldsymbol{S}$.
- $\boldsymbol{A}$ intercepts (P_{33}) and forwards it to $\boldsymbol{S}$.

- After receiving (P_{36}), $\boldsymbol{S}$ verifies $ACK = H_4(M_6 \oplus r_S)$. Thus, $\boldsymbol{A}$ is successfully authenticated by $\boldsymbol{S}$ masquerading $\boldsymbol{C}$.

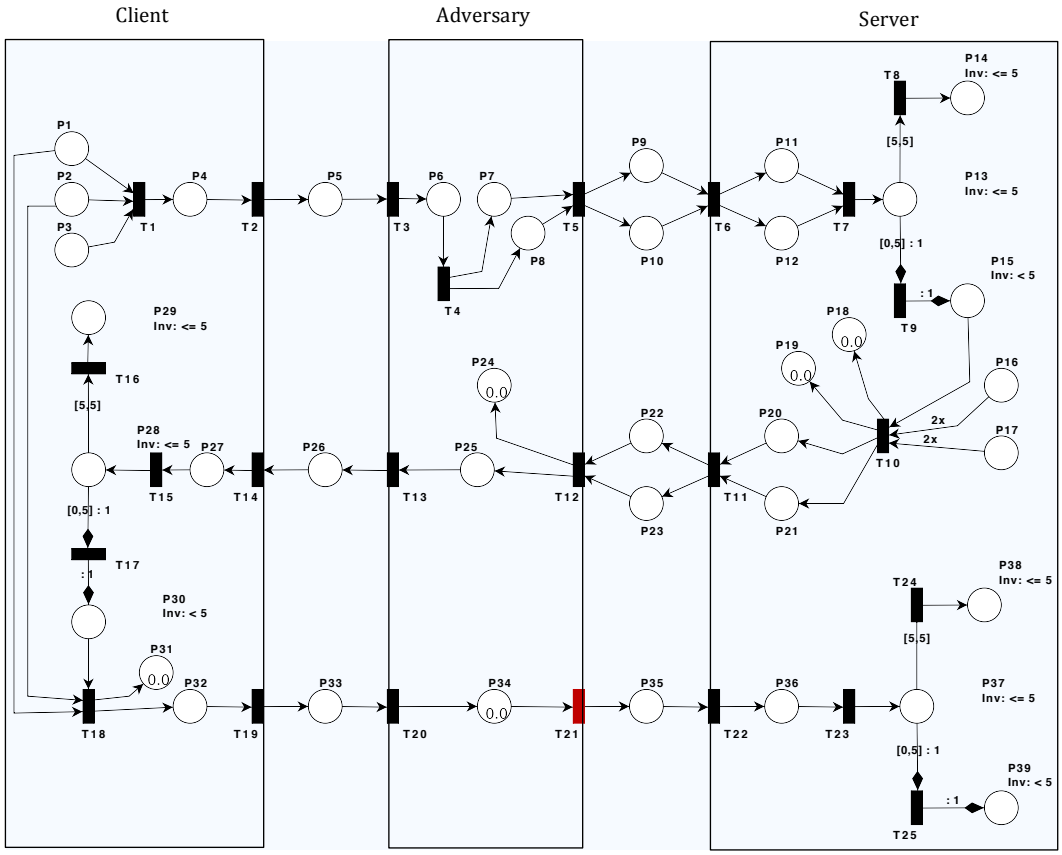


Figure 7.10: The adversary masquerading as client

By analysing the protocol, without encrypting the traffic, the proposed protocol is prone to man-in-the-middle attack. The adversary has the ability to control the negotiation between the client and the server. In fact, the adversary can clearly modify, substitute or delete all subsequent messages. It is obvious that both the client and the server have established a bogus session with the adversary.

7.5 Analysis of Reflection Attack

The Reflection Attack consists of two parties. The Adversary in this model is masquerading as the server. In this PN model, *places* represent either input or output of the protocol run. *Transitions* are used to illustrate the client and adversary actions. *Tokens* indicate the progress of the attack. Figure 7.11 describes the execution of a reflection attack for the new protocol with the presence of the client and the adversary. The definitions of the places and the transitions used in this model are illustrated in Table 7.5 and Table 7.6, respectively.

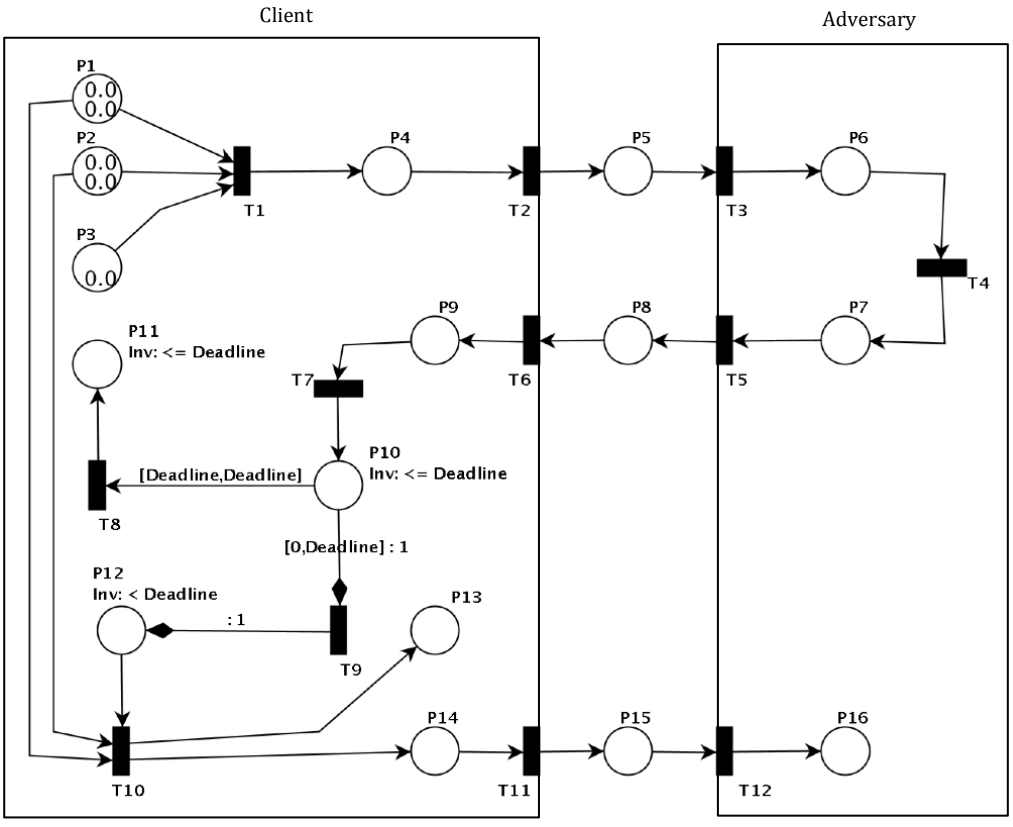


Figure 7.11: Modelling the reflection attack

Table 7.5: DEFINITIONS OF PLACES – THE REFLECTION ATTACK MODEL

Place	Definition	Place	Definition
P_1	Client random number	P_9	Received forge SYN/ACK
P_2	Client timestamp	P_{10}	Verification message
P_3	SYN request	P_{11}	Rejected request
P_4	Login request	P_{12}	Accepted request
P_5	Sent request	P_{13}	Session key
P_6	Intercepted MSG	P_{14}	ACK
P_7	Sent forge SYN/ACK	P_{15}	Sent ACK
P_8	Received forge SYN/ACK	P_{16}	Received ACK

Table 7.7: DEFINITIONS OF TRANSITIONS – THE REFLECTION ATTACK MODEL

Trans.	Definition	Trans.	Definition
T_1	Compute login request + SYN	T_7	Split the packet and verify
T_2	Send MSG	T_8	Drop the request
T_3	Intercept MSG	T_9	Accept the request
T_4	Fabricate SYN/ACK	T_{10}	Compute ACK and session key
T_5	Send fake SYN/ACK	T_{11}	Send ACK
T_6	Received fake SYN/ACK	T_{12}	Receive ACK

Since client $\boldsymbol{C}$'s login request $[ID_C, T_C, W_1, M_3, MAC_k(ID_C, T_C, W_1, M_3)]$ is symmetrical to server $\boldsymbol{S}$ response $[ID_C, T_S, W_2, M_6, M_7, MAC_k(ID_C, T_S, W_2, M_6, M_7)]$ but the differences between them can only be found in the timestamps and hash values, this symmetry flaw (Wang and Ma, 2013) leads to a reflection attack. To exploit the reflection attack, the adversary $\boldsymbol{A}$ intercepts the login request while listening to the electronic conversation between client $\boldsymbol{C}$ and server $\boldsymbol{S}$. Then, the adversary sends the same login request $[ID`_C, T`_C, W`_1, M`_3, MAC`_k(ID_C, T_C, W_1, M_3)]$ to $\boldsymbol{C}$ in a timely manner (Figure 7.12).

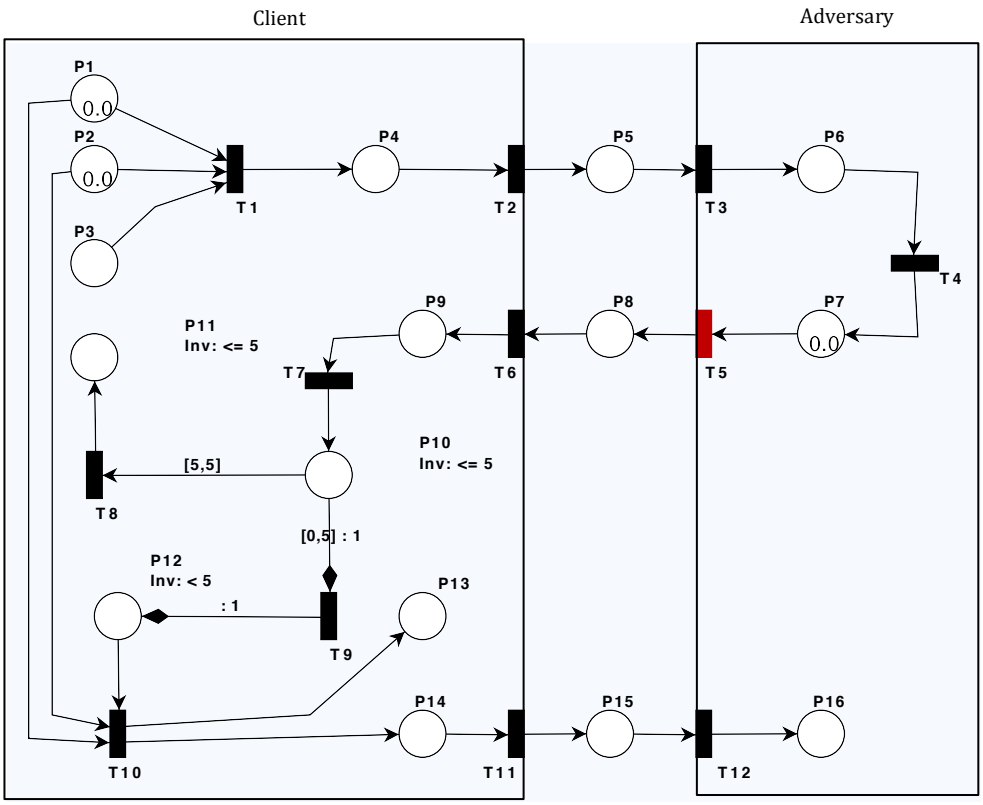


Figure 7.12: The adversary masquerading as server (SYN/ACK)

It is obvious that, upon receiving the forged server's response (which is in fact the adversary's reply request), $\boldsymbol{C}$ will automatically acknowledge the response since the computation is accomplished with the correct key, so the MAC integrity check will succeed. Consequently, $\boldsymbol{A}$ successfully masquerades as $\boldsymbol{S}$ and the protocol fails to provide mutual authentication.

Although $\boldsymbol{A}$ can cheat $\boldsymbol{C}$ into believing he is communicating with $\boldsymbol{S}$, $\boldsymbol{A}$ cannot obtain the corresponding session key *sk*. Still this type of attack is deemed to represent a breach of the basic obligation of mutual authentication with limited damage. $\boldsymbol{A}$ performed the exploit without the knowledge of key *k*, merely by intercepting the challenge and sending it back to $\boldsymbol{C}$.

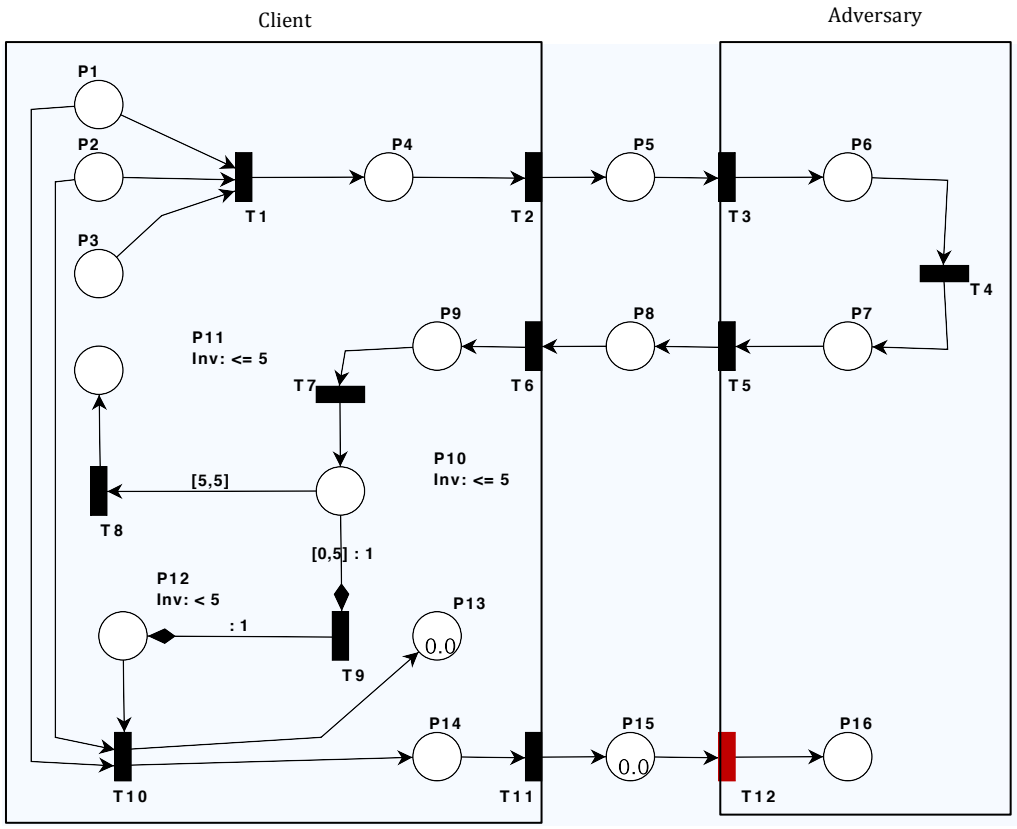


Figure 7.13: The adversary masquerading as server (ACK)

7.6 Analysis of Parallel Session Attack

Another attack, which is effective against the new model without encrypted traffic, is a parallel session attack. This attack uses deception to compromise authentication protocols. It involves selecting a valid combination of information from ongoing protocol executions. Figure 7.14 explains the exploitation of a parallel session attack on the proposed protocol with the presence of an adversary. The message exchange in this attack is mainly between the server and the adversary, leaving the client completely out of the picture. The definitions of the places and transitions for this model are given in Table 7.7 and Table 7.8, respectively.

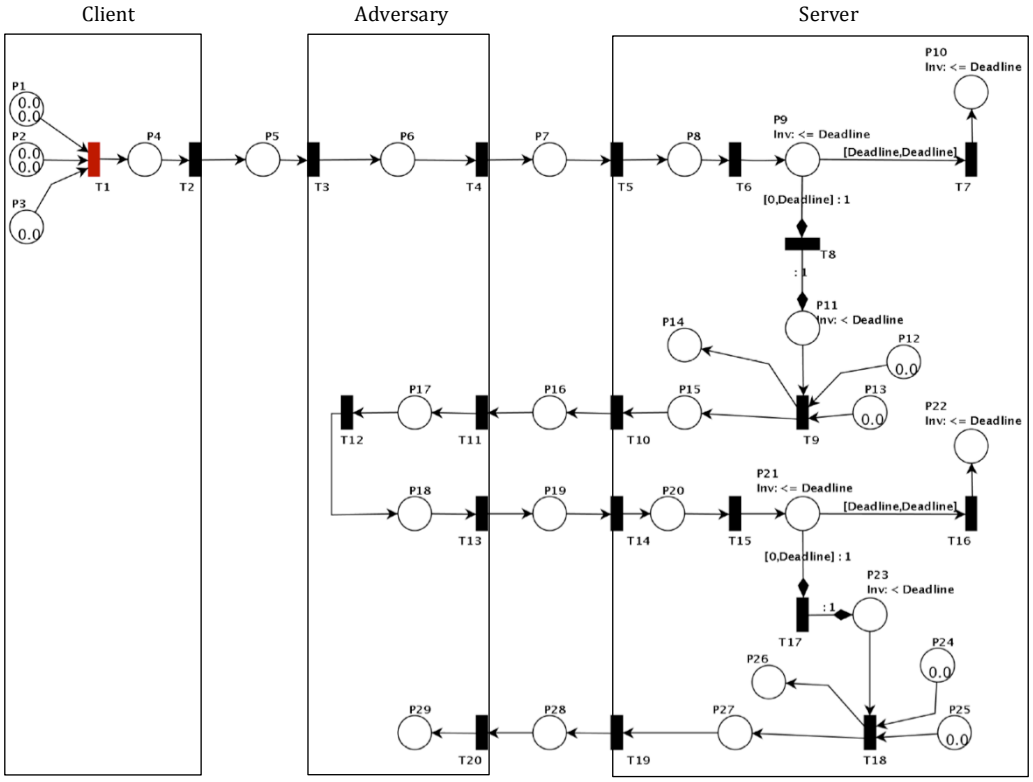


Figure 7.14: Modelling the parallel session attack

Table 7.7: DEFINITIONS OF PLACES - THE PARALLEL SESSION ATTACK MODEL

Place	Definition	Place	Definition
P_1	Client random number	P_{16}	Sent SYN/ACK
P_2	Client timestamp	P_{17}	Received SYN/ACK
P_3	SYN request	P_{18}	Fabricated Fake SYN
P_4	Login request	P_{19}	Sent fake SYN
P_5	Sent request	P_{20}	Received fake SYN
P_6	Intercepted MSG	P_{21}	Verification message
P_7	Forge MSG	P_{22}	Rejected request
P_8	Sent Forge MSG	P_{23}	Accepted request
P_9	Verification message	P_{24}	Server random number
P_{10}	Rejected request	P_{25}	Server timestamp
P_{11}	Accepted request	P_{26}	Session Key
P_{12}	Server random number	P_{27}	SYN/ACK
P_{13}	Server timestamp	P_{28}	Sent SYN/ACK
P_{14}	Session Key	P_{29}	Received SYN/ACK
P_{15}	SYN/ACK		

Table 7.8: DEFINITIONS OF TRANSITIONS - THE PARALLEL SESSION ATTACK MODEL

Trans.	Definition	Trans.	Definition
T_1	Compute login request + SYN	T_{11}	Intercept MSG
T_2	Send MSG	T_{12}	Fabricate SYN
T_3	Intercept MSG	T_{13}	Send fake SYN
T_4	Send forge MSG	T_{14}	Receive forge SYN
T_5	Received Forge MSG	T_{15}	Split the packet and verify
T_6	Split the packet and verify	T_{16}	Drop the request
T_7	Drop the request	T_{17}	Accept
T_8	Accept	T_{18}	Compute SYN/ACK and session key
T_9	Compute SYN/ACK and session key	T_{19}	Send SYN/ACK
T_{10}	Send SYN/ACK	T_{20}	Receive SYN/ACK

In the authentication phase of the new protocol, the adversary $\boldsymbol{A}$ can masquerade as an authorised client without prior knowledge of the password. The exploit starts when $\boldsymbol{A}$ eavesdrops on the communication between $\boldsymbol{C}$ and $\boldsymbol{S}$ (Figure 7.15).

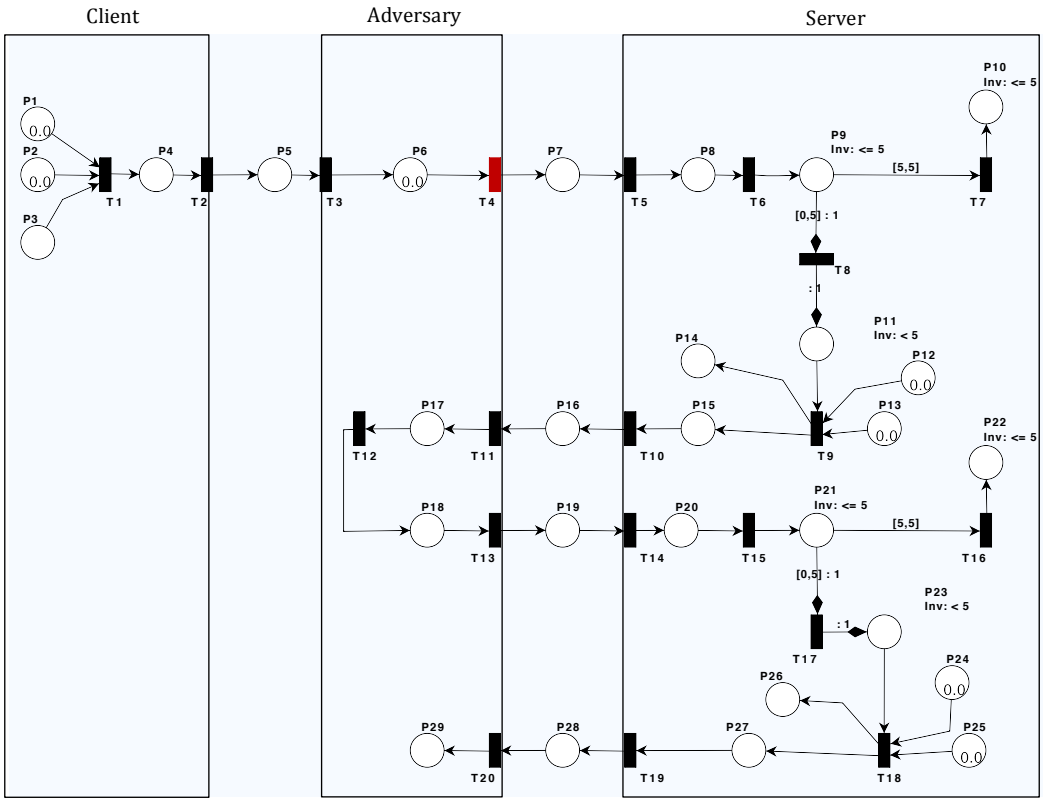


Figure 7.15: The adversary eavesdrops on the communication between C and S

A intercepts and blocks the ***S*** response message: P_{16} = [ID_{C_i}, Ts_i, W_2, M_6, M_7, $MAC_k(ID_{C_i}, Ts_i, W_2, M_6, M_7)$]. Then, ***A*** instantly impersonates ***C*** and initiates a new session with ***S*** by sending a fabricated login request: P_{19} = [$ID_A = ID`_C$, $T_A = T`_S$, $W_1 = W`_2$, $M_3 = M`_6$, M_7, $MAC`_k(ID_C, T_S, W_2, M_6, M_7)$], which is the original reply of ***S*** to ***C*** (Figure 7.16).

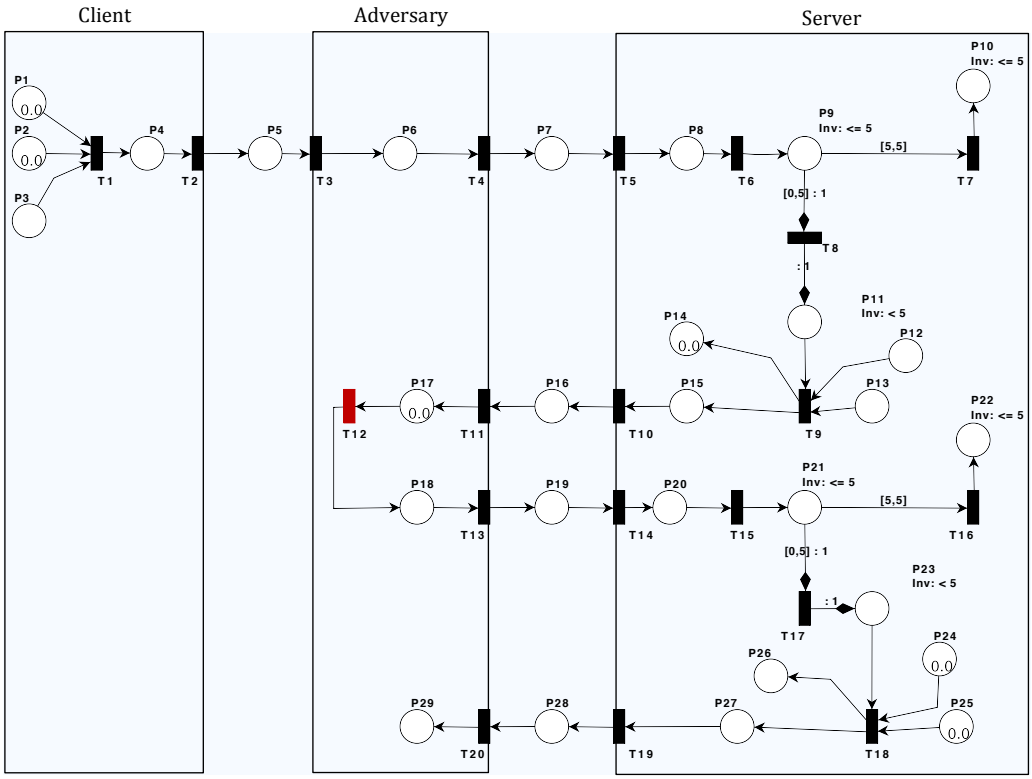


Figure 7.16: The adversary intercepts the server response (SYN/ACK)

Assume that, if the fabricated message arrives at ***S*** on time T, it will pass the verification check for the following reasons:

(1) The likelihood of correlation associated with $T` - T_C \leq \Delta T$ will be high considering the time-delay in wide-area networks is unpredictable and varies most of the time. Thus, ΔT is often set higher than the timespan of a complete round-trip (Mills, 1991; Giridhar and Kumar, 2006; Han and Jeong, 2010).

(2) The MAC integrity check will give a positive result since $MAC`_k(ID_C, T_S, W_2, M_6, M_7)$ is actually computed with the correct key k by $\boldsymbol{S}$.

Based on the above assumptions, $\boldsymbol{S}$ generates random number P_{24} and timestamp P_{25} to compute session key P_{26} and SYN/ACK response P_{28}, and sends it to $\boldsymbol{A}$ (Figure 7.17).

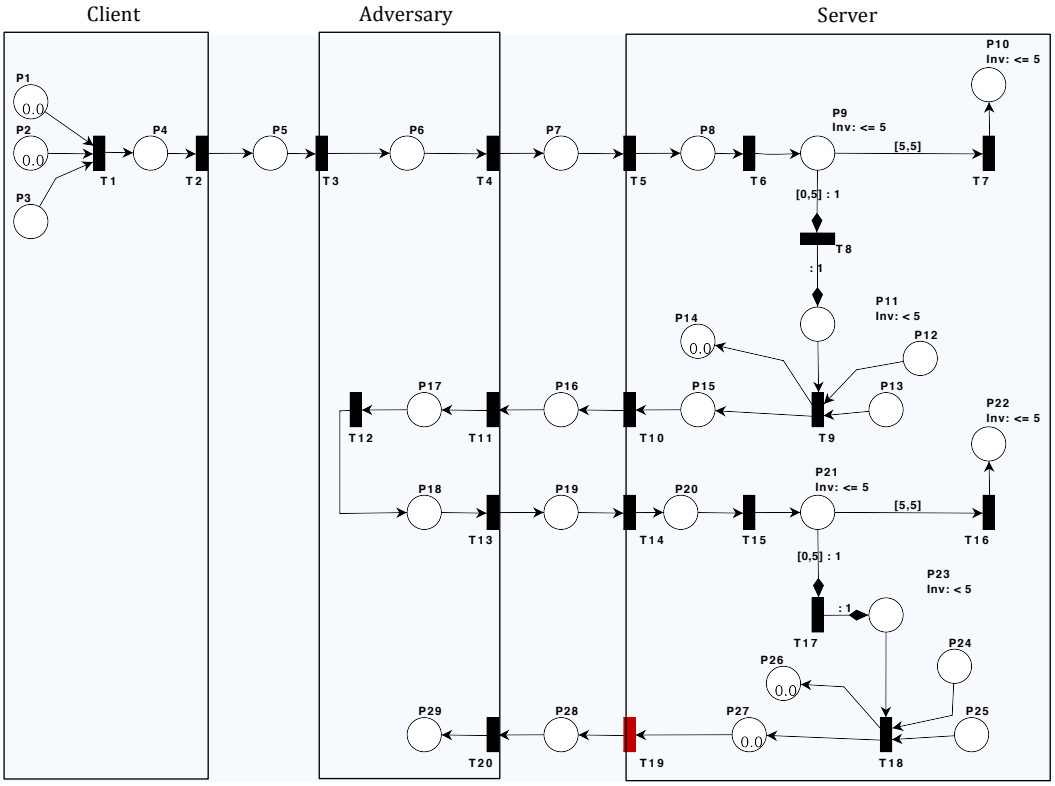


Figure 7.17: The adversary intercepts the server response (ACK)

7.7 Analysis of Impersonation Attack

One possible attack against the proposed model is impersonation attack. Based on the simulation of man-in-the-middle attack, reflection attack, and parallel session attack, the model reveals a potential risk and weakness that leads to an impersonation attack. The adversary $\boldsymbol{A}$ can mount an impersonation attack without knowing any other secret information or credentials by intercepting the login request [ID_C, T_C, W_1, M_3, $MAC_k(ID_C, T_C, W_1, M_3)$]. Hence, $\boldsymbol{A}$ can exploit the proposed protocol by using any of the methods explained previously and hijacking sessions transmitted between $\boldsymbol{C}$ and $\boldsymbol{S}$. Eventually, $\boldsymbol{A}$ succeeds in impersonating either the client or the server by pretending to be either the client or the server.

7.8 Analysis of Replay Attack

The security feature in the new protocol can withstand replay attack due to the use of the *freshness* property. This is guaranteed by applying timestamps and random numbers for each authentication session. To validate the authenticity of messages exchanged between $\boldsymbol{C}$ and $\boldsymbol{S}$, the freshness of timestamps is constantly checked. For example, the verification request will fail if $T' - T_C > \Delta T$. This will cause the session to be terminated. Moreover, a new session key is constructed in every authentication cycle. The adversary cannot compromise the old session key because it has never been transmitted in the protocol execution between the client and the server. One of the new protocol merits is that each entity computes the correct session key based on the information exchanged between them.

7.9 Analysis of Forgery Attack

The adversary cannot create a valid login from scratch without knowing the secret value and the private key of the client. Thus, the adversary cannot act as a legal client, so the attack is not feasible.

7.10 Analysis of Ciphertext Attack

Ciphertext attack is one of the realistically possible attacks that can subvert the protocol. The PN model for this attack is demonstrated in Figure 7.18, which shows the attack takes place in the first part of the three-way handshake. The definitions of the places and the transitions for this model are defined in Table 7.9 and Table 7.10, respectively. The analysis for this attack is based on the following assumptions:

1. MAC functions are secure against chosen-message attacks.
2. Symmetric encryption functions are secure against chosen-plaintext attacks.

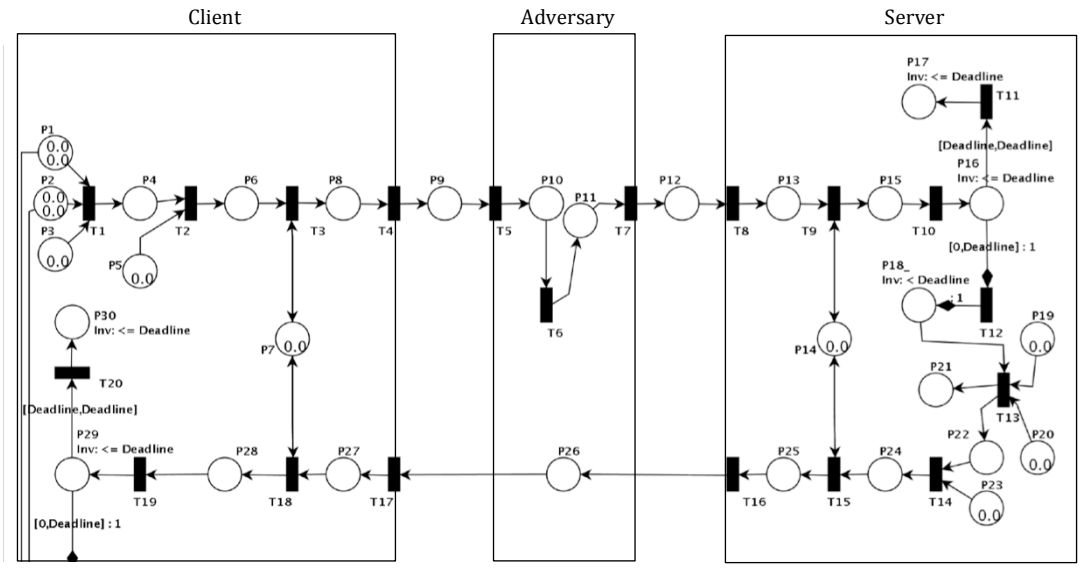


Figure 7.18: Modelling the ciphertext attack

Table 7.9: DEFINITIONS OF PLACES - THE CIPHERTEXT ATTACK MODEL

Place	Definition	Place	Definition
P_1	Client random number	P_{17}	Rejected request
P_2	Client timestamp	P_{18}	Accepted request
P_3	SYN request	P_{19}	Server random number
P_4	Login request	P_{20}	Server timestamp
P_5	MAC secret key	P_{21}	Session Key
P_6	Authenticated MSG	P_{22}	SYN/ACK for C
P_7	Symmetric key	P_{23}	MAC secret key
P_8	Ciphertext	P_{24}	Authenticated MSG
P_9	Sent ciphertext	P_{25}	Ciphertext
P_{10}	Intercepted ciphertext	P_{26}	Sent ciphertext
P_{11}	Modified ciphertext	P_{27}	Received ciphertext
P_{12}	Sent modified ciphertext	P_{28}	Decrypted ciphertext
P_{13}	Received modified ciphertext	P_{29}	Verification message
		P_{30}	Rejected request
P_{14}	Symmetric key	P_{31}	Accept request – S is authenticated
P_{15}	Decrypted ciphertext		
P_{16}	Verification message		

Table 7.10: DEFINITIONS OF TRANSITIONS - THE CIPHERTEXT ATTACK MODEL

Trans.	Definition	Trans.	Definition
T_1	Compute login request + SYN	T_{12}	Accept
T_2	Compute MAC value and append it to the MSG	T_{13}	Compute SYN/ACK and session key
T_3	Encrypt MSG	T_{14}	Compute MAC value and append it to the MSG
T_4	Send ciphertext		
T_5	Intercept ciphertext	T_{15}	Encrypt MSG
T_6	Alter	T_{16}	Send ciphertext
T_7	Send modified ciphertext	T_{17}	Receive ciphertext
T_8	Receive modified ciphertext	T_{18}	Decrypt ciphertext
T_9	Decrypt ciphertext	T_{19}	Split the packet and verify
T_{10}	Split the packet and verify	T_{20}	Drop the request
T_{11}	Drop the request	T_{21}	Accept

Suppose that $\boldsymbol{C}$ and $\boldsymbol{S}$ are exchanging messages in encrypted form using symmetric key cryptography. Typically, $\boldsymbol{C}$ creates a login request via T_1 and then authenticates the login request P_4 by calculating the MAC value using the computed key k, via T_2. Next $\boldsymbol{C}$ appends the result of the MAC calculation and produces an authenticated

message $P_6 = ID_{C_i}, T_{C_i}, W_1, M_3, MAC_k(ID_{C_i}, T_{C_i}, W_1, M_3)$. At this stage, $\boldsymbol{C}$ encrypts the authenticated message with the key a via T_3 and sends the ciphertext $P_8 = \{ID_{C_i}, T_{C_i}, W_1, M_3, MAC_k(ID_{C_i}, T_{C_i}, W_1, M_3)\}_a$ to $\boldsymbol{S}$. Now, assume there is an active adversary $\boldsymbol{A}$ listening to the conversation between $\boldsymbol{C}$ and $\boldsymbol{S}$. $\boldsymbol{A}$ can basically perform a man-in-the-middle attack even if it cannot decrypt or re-encrypt the packets as they pass through. In this scenario, $\boldsymbol{A}$ can intercept the messages interchanged between $\boldsymbol{C}$ and $\boldsymbol{S}$, trim them, alter them, and pass on the modified versions. The session between $\boldsymbol{C}$ and $\boldsymbol{S}$ breaks every time $\boldsymbol{A}$ interferes. During the exchange in Figure 7.14, $\boldsymbol{A}$ can intercept the ciphertext P_{10} from $\boldsymbol{C}$ to $\boldsymbol{S}$ that is equivalent to $C_1=\{ID_{C_i}, T_{C_i}, W_1, M_3, MAC_k(ID_{C_i}, T_{C_i}, W_1, M_3)\}_a$, and mangle it to get ciphertext $C_1`=\{ID_{C_i}`, T_{C_i}`, W_1`, M_3`, MAC_k(ID_{C_i}, T_{C_i}, W_1, M_3)\}_a$ and send it to $\boldsymbol{S}$.

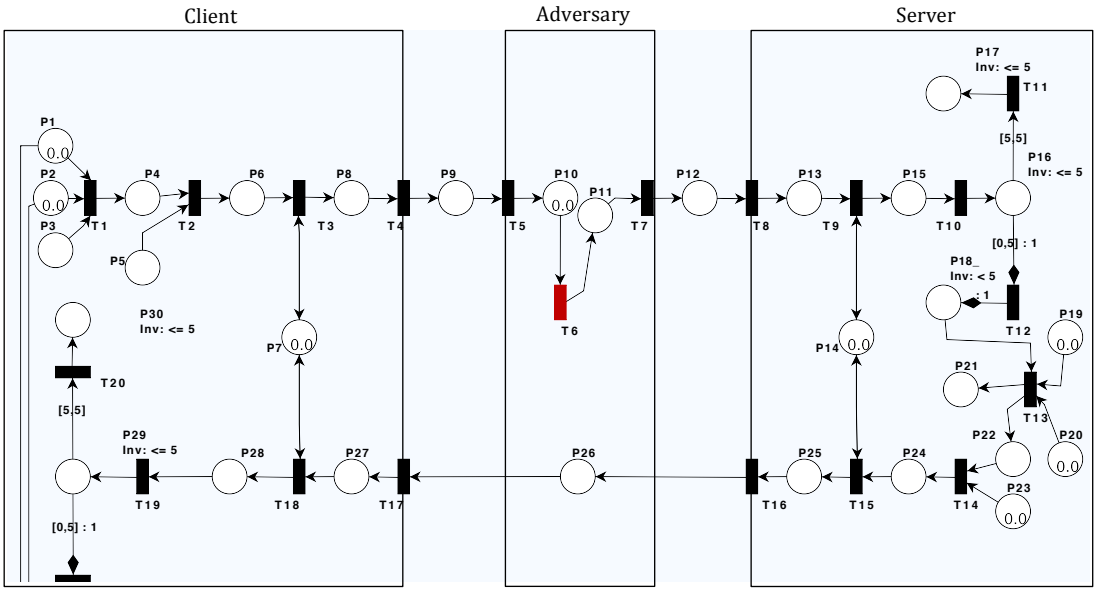


Figure 7.19: The adversary intercepts the client's request

This attack relies on the fact that the MAC value is encrypted along with the raw data. When $\boldsymbol{S}$ receives the encrypted message, it needs to validate as follows:

1. Decrypt the received data (Figure 7.20).
2. Compute the MAC value and validate the checksum (Figure 7.21).

It is true that $\boldsymbol{S}$ will terminate the session once it decrypts because when $\boldsymbol{S}$ computes the MAC value for the modified message it will not match the received MAC value. Also, it is worth considering the wasted time the process $\boldsymbol{S}$ takes to realise the message is invalid and terminates the session due to a technical error from the point of view of $\boldsymbol{S}$. $\boldsymbol{S}$ never recognises that the encrypted message has been tampered with.

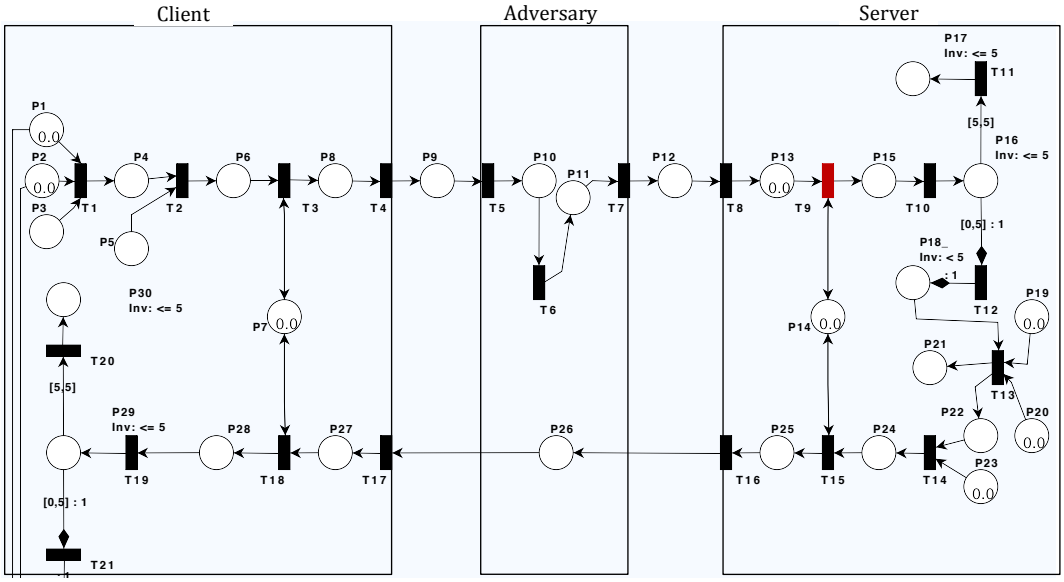


Figure 7.20: The server decrypts the forged request

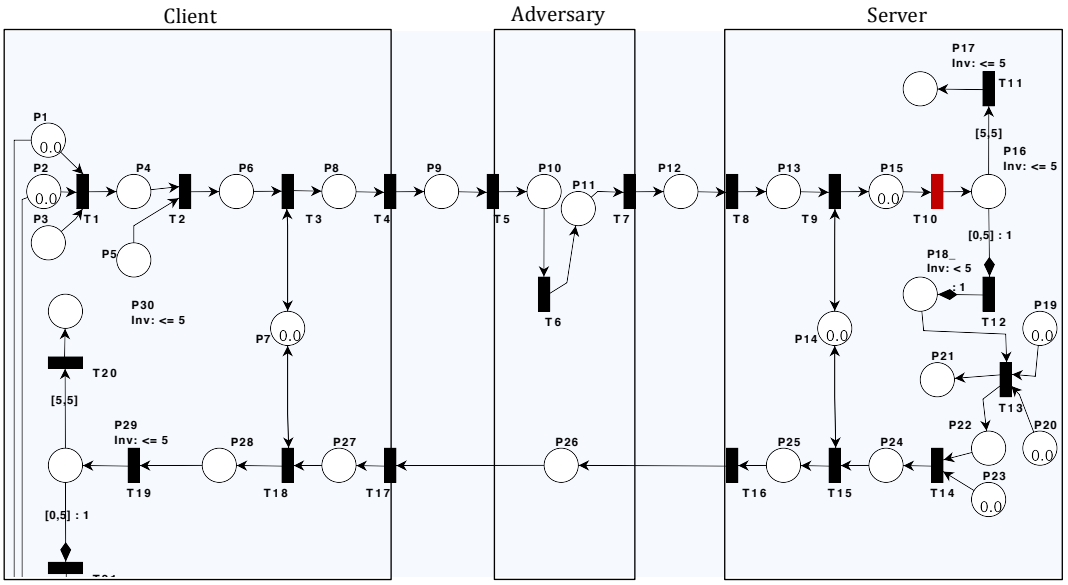


Figure 7.21: The server verifies the decrypted request

The analysis determines that the attack can be successful in subverting the main goal of the protocol. To make the point clearer, $\boldsymbol{S}$ believed the message came from $\boldsymbol{C}$ because the decryption process was a success. However, it was up to $\boldsymbol{S}$ to validate the integrity of the message by verifying the integrity checksum based on the MAC.

Another attack is effective against the new protocol is the attack illustrated by Krawczyk (2001). He exposed a vulnerability in the authenticate-then-encrypt method. This attack can be applied to the new protocol and it works as long as the adversary can learn if a given ciphertext is valid, even if it cannot obtain full decryption. The following encryption scheme is used in the attack scenario (Katz and Lindell, 2007):

- *Let Transform(m) be as follows: any 0 in m is transformed to 00, and any 1 in m is transformed arbitrarily to 01 or 10. The decoding of a message works by mapping 00 back to 0, and 01 and 10 back to 1. However, a pair of bits 11 will result in decoding the message back to* $\perp$ *(irrespective of the other bits).*

- *Define Enc'$_k$ (m) = Enc$_k$(Transform(m)), where Enc is a stream cipher that works by generating a new pseudorandom stream for each message to encrypt, and then XORs the stream with the input message. For example, this can be obtained by using a pseudorandom function (secure block cipher) in CTR mode, with a new random IV for each encryption. Note that both the encryption schemes Enc and Enc' are CPA secure.*

An adversary $\boldsymbol{A}$ can willingly observe a transmitted ciphertext P_{10}: $C=\{ID_{C_i}, T_{C_i}, W_1, M_3, MAC_k(ID_{C_i}, T_{C_i}, W_1, M_3)\}_a$ and it can learn the first bit while intercepting the ciphertext C. $\boldsymbol{A}$ can simply flip the first two bits (c_1, c_2) of C and send the modified ciphertext $C\hat{}$ to its destination. $\boldsymbol{A}$ can find out that the resulting ciphertext is valid if the original bit is equals to 1. The bit change in ciphertext will result in the same decrypted plaintext and then the MAC check will succeed. This is because if the first bit of the original message equals 1, then the first two bits of *Transform(m)* can be 01 or 10. Thus, the match of these two bits still maps to the same initial bit 1. On the other hand, if the original bit is equal to 0, the decrypted plaintext will have a 1 instead, then MAC will fail. This is because 0 is mapped to 00 and so flipping these bits results in 11, which is an incorrect encoding. Thus, the plaintext is $\perp \neq m$ but the MAC is still computed over m. All $\boldsymbol{A}$ needs is to obtain the information whether the MAC succeeded or not (Krawczyk, 2001; Katz and Lindell, 2007).

The above analysis unfortunately exhibits the fragility of the security of the authenticate-then-encrypt method and it shows that the combination is not secure against chosen-ciphertext attacks. Thus, the new protocol shows weaknesses and fails to achieve the security goals, which are in this case integrity and secrecy.

7.10 Security Analysis and Discussion

Security analysis is a crucial process in evaluating communication and cryptographic protocols. Also, it aids in identifying flaws and weaknesses existing in protocols. The analysis shows that there are few flaws in the proposed protocol. These flaws can be quickly removed by considering three techniques. The first amendment is to include the ID_S of the server. The absence of server identity allows an adversary to simply masquerade as a trusted server. It is possible to optimise the protocol with a simple technique, such as adding the server ID_S, which can address the problem. As for the second amendment, encrypting the traffic between client and server creates a private channel to transmit a confidential conversation and calculate the session key. Variations of these attacks were modelled in all phases of mutual authentication and key agreement of the cycle. Modelling and simulation revealed that the unencrypted traffic does not provide a full secure transmission and allows a sensitive credential information travel in clear forms. However, a major issue to be highlighted here is that encryption provides only secrecy and it does not guarantee integrity. In conjunction, the authenticate-then-encrypt method does not quite accomplish the integrity of the ciphertext, even if these mechanisms are secure as standalone functions. This leads to the third amendment, which encourages employing the encrypt-then-authenticate method instead of the authenticate-then-encrypt. The reasonable reaction to overcome this flaw is to validate the ciphertext integrity by calculating the MAC value of the ciphertext and appending the value to it. This way, both $\boldsymbol{S}$ and $\boldsymbol{C}$ will be able to validate the integrity of the incoming message and authenticate the cipher messages before decryption. By applying this technique, the proposed protocol will be effective in circumventing attacks on ciphertexts such as

known-plaintext attack (KPA), chosen ciphertext attack (CCA1), and adopted chosen ciphertext attack (CCA2).

7.12 SUMMARY

Security analysis is an essential process in evaluating communication and cryptographic protocols. This chapter presents a formal approach for enumerating the vulnerabilities and flaws in proposed protocols and determining suitable countermeasures to fix them. First, PNs are used to model the client-server trust model. Then, an adversary entity is added to the trust model to analyse various attacks and understand the possible behaviours of the adversary. Each attack scenario has been simulated using PNs to exploit vulnerabilities in both cases without the symmetric encryption applied and with it.

It is evident that the most viable countermeasure to defend authentication attacks is to encrypt then authenticate the message exchange between the client and server. Since the traffic is encrypted between the client and server, this proves that the proposed protocol is resistant to man-in-the-middle attack, reflection attack, parallel session attack, and impersonation attack but not a ciphertext attack. Also, this chapter shows that replay attack and forgery attack are not effective because of the freshness property and the difficulty of creating a login request without learning any prior credentials.

8

The Modified Protocol

This chapter presents the modified protocol that can overcome the security flaws of the original proposed protocol. Before conducting the security evaluation of the proposed protocol, there was no safe way to avoid security flaws during the protocol design. Security issues were not properly addressed even though security measures were taken into account during the protocol design.

To solve the flaws found in Chapter 6 and provide further improvements on the proposed protocol, this chapter presents an enhanced version of the proposed protocol, which can defeat attacks. It employs the same concept of the proposed protocol but adds another valuable element to it. The concept of maintaining confidentiality and integrity during transmission is assured by adopting the encrypt-then-authenticate method

---

8.1 MODIFIED PROPOSED PROTOCOL

The modified version of the proposed protocol should improve security and provide users with better authentication and data confidentiality. To address and correct the perceived security weakness in the proposed protocol, authenticating the ciphertext by applying the encrypt-then-authenticate method is considered to be one of the most secure methods for security protocols (Krawczyk, 2001). The previous message exchange in the proposed protocol was constructed like this:

$$Encrypt\ (Message \mid\mid MAC)$$

The new modification for the message exchange will be constructed as this:

$$Encrypt\ (Message) \mid\mid MAC$$

This way the MAC is covering the entire ciphertext to preserve the integrity of the cipher message. The MAC value is then appended to the encrypted message. When the recipient receives the authenticated encrypted message, the MAC should be evaluated before attempting to decrypt the ciphertext. If the MAC verification fails, the recipient will terminate the session immediately. This process will be more efficient by eliminating the time spent to going through the manipulated data.

The enhancements for the proposed protocol will only affect part of the registration phase and the authentication and key agreement phase. Additionally, enclosing the identity of the server along with the client's identity can mitigate the impact of masquerading attack. The ID's of entities must be unique in the network. Thus, the entities that wish to communicate are aware of each other.

8.1.1 REGISTRATION PHASE

The registration process will remain the same except for one change in the last step of the process. The secret key for MAC will no longer be computed during the handshake. Instead, the key will be agreed on previously and will be sent via a secure channel during registration. The modification that will apply to Step 4 is:

Step 4: R_i stores $\{ID_{C_i}, H_4(.), MAC_K(), Enc\{\}_a/Dec\{\}_a, f_i, e_i, \tau, Pr\_K_{C_i}\}$ on a secure database and sends it to the user via a secure channel, where:

- $MAC_K()$ is a message authentication code with secret key k
- $Enc\{\}_a/Dec\{\}_a$ is a symmetric encryption with secret key a
- f is the biometric template
- $e_i = H_4(ID_{C_i} || y) \oplus H_4(PW_{C_i} || f_i)$
- τ is a predetermined threshold for biometric verification.
- $Pr\_K_{C_i}$ client's private key.

8.1.2 LOGIN PHASE

After the client C_i successfully logs in, the client begins the authentication process and negotiates the session key. The client generates a random number and a timestamp, then computes the following:

$$f_i = H_4(Bio_{C_i})$$

$$z`_i = H_4(PW_{C_i} || f_i)$$

$$M_1 = e_i \oplus z`_i = H_4(ID_{C_i} || y)$$

$$W_1 = r_{C_i}.P$$

$$M_2 = r_{C_i}.Pr\_K_{C_i}$$

$$M_3 = M_1 \oplus r_{C_i}$$

Where $r_{C_i} \in Z^*_n$ is a random number generated by the user. For this step, the random value r_{C_i} is introduced to mask the hash of the secret value $H_4(ID_{C_i}||y)$.

Step 4: C_i encrypts the login request contains the initial components of the negotiated session key: ID_{C_i}, T_{C_i}, W_1 as contribution of the session key.

$C_1 = Enc\{ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3\}$ with the secret key a

Step 5: C_i authenticates the ciphertext by calculating the MAC value and appends it to encrypted message.

$mac_1 = MAC_k(ID_{C_i}, \mathrm{ID}_{S_i}, T_{C_i}, W_1, M_2, M_3)$

$A_1 = C_1 \,||\, mac_1$

C_i sends the authenticated ciphertext to the server S_i.

The authenticated encrypted message includes C_i's timestamps to provide freshness guarantees; the value of W_1 is a multiplication of the C_i's random number with P point on elliptic curve E with order n.

7.1.3 Authentication and Key Agreement Phase

After receiving the request login message, S_i and C_i will perform the following steps for mutual authentication:

Step 1: S_i checks the authenticity of the ciphertext and ensures the encrypted message has not been altered. This can be accomplished by recalculating the hash value of the received ciphertext and comparing it with the appended

hash value that was attached with the ciphertext. If the MAC values are identical, then the ciphertext is authenticated and the integrity is checked.

Step 2: If Step 1 holds true, S_i decrypts the message $\{ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3\}_a$, then checks the validity of ID_{C_i} and the freshness of T_{C_i}. The freshness of T_{C_i} is checked by performing $T` - T_{C_i} \leq \Delta T$, where $T`$ is the time when S_i receives the above message and ΔT is a valid time interval. In the case where ID_{C_i} is not valid or T_{C_i} is not fresh, then S_i aborts the current session.

Step 3: If Step 2 holds true, S_i computes the following:

$$M`_2 = (x + H_1(ID_{C_i})^{-1}. W_1$$

$$= Pr\_K_{C_i} . r_{C_i}$$

$$= M_2$$

S_i will quit the current session if the values of $M`_2$ and M_2 are not equal.

Step 4: If Step 3 holds true, S_i chooses a random number $R_{S_i} \in Z^*_n$ and computes the following:

$$M_4 = H_4 (ID_{C_i} || y)$$

$$W_2 = r_{S_i} . P$$

$$K_{S_i} = r_{S_i} . W_1$$

Now S_i is able to complete the protocol and compute the absolute value of the session key $sk = H_3 (ID_{C_i}, ID_{S_i}, T_{C_i}, T_{S_i}, W_1, W_2, K_{S_i})$, where T_{S_i} is a timestamp denoting the current time

$$M_5 = M_3 \oplus M_4 = r_{C_i}$$

$$M_6 = M_4 \oplus r_{S_i}$$

$$M_7 = H_4(M_3 \,||\, M_5)$$

Where M_5 is the random value r_{C_i} of the user $\boldsymbol{C_i}$ and only $\boldsymbol{S_i}$ can unmask the value because it can compute $H_4\ (ID_{C_i} || y)$.

Step 4: Then, $\boldsymbol{S_i}$ encrypts the message with shared secret key a.

$$C_2 = Enc\ \{ID_{C_i}, ID_{S_i}, T_{S_i}, W_2, M_6, M_7\}_a$$

Step 5: $\boldsymbol{S_i}$ authenticates the encrypted message by calculating the MAC value of the ciphertext and appends it along with the ciphertext. Then $\boldsymbol{S_i}$ sends the authenticated ciphertext to the client $\boldsymbol{C_i}$.

$$Mac_2 = MAC_k\ (ID_{C_i}, ID_{S_i}, T_{S_i}, W_2, M_6, M_7)$$

$$A_2 = C_2 \,||\, mac_2$$

Step 6: Upon receiving $\boldsymbol{S_i}$'s encrypted message, $\boldsymbol{C_i}$ first checks the authenticity of the ciphertext and ensures the encrypted message has not been altered. This can be accomplished by recalculating the hash value of the received ciphertext and comparing it with the appended hash value that was attached to the ciphertext. If the MAC values are identical, then the ciphertext is authenticated and the integrity is checked.

Step 7: $\boldsymbol{C_i}$ decrypts $\{ID_{C_i}, ID_{S_i}, T_{S_i}, W_2, M_6, M_7\}_a$, and checks the freshness of T_{S_i} by performing $T' - T_{S_i} \leq \Delta T$, where T' is the time when C_i receives the above message and ΔT is the expected time interval for the transmission delay.

Step 8: C_i verifies whether $M_7 \stackrel{?}{=} H_4 (M_3 \,||\, r_{C_i})$. C_i will quit the current session if the comparison is not equal.

Step 9: If it holds, then C_i believes that S_i is authenticated and then computes the following:

$$K_{C_i} = r_{C_i} . W_2$$

$$\text{The session key } sk = H_3 (ID_{C_i}, ID_{S_i}, T_{C_i}, T_{S_i}, W_1, W_2, K_{C_i})$$

$$M_8 = M_6 \oplus M_1 = r_{S_i}$$

$$M_9 = H_4(M_6 \,||\, M_8)$$

Where M_9 is the random value r_{S_i} of the server S_i and only the client C_i, which know $M_1 = H_4 (ID_{C_i} || y)$, can send back the correct hashed value of $M_9 = H_4 (H_4 (ID_{C_i} || y) \oplus r_{S_i}) || r_{S_i})$.

Step 10: C_i encrypts the message $(ID_{C_i}, ID_{S_i}, T_{C_i}, M_9)$ then authenticates it and sends it to S_i

$$C_3 = Enc\{ID_{C_i}, ID_{S_i}, T_{C_i}, M_9\}_a$$

$$mac_3 = MAC_k (ID_{C_i}, ID_{S_i}, T_{C_i}, M_9)$$

$$A_3 = C_3 \,||\, mac_3$$

Step 11: After receiving C_i's message, S_i checks the integrity of mac_3. It then decrypts C_3.

Step 12: Next, S_i verifies whether $M_9 \stackrel{?}{=} H_4 (M_6 \,||\, r_{S_i})$. If it holds, S_i authenticates C_i or otherwise rejects it.

8.2 Behaviour Evaluation

As discussed previously, modelling with finite-state machines helps to understand the behaviour of complex protocols. There will be one amendment to the state machine, which is creating two EFSMs inside $EFSM_{client}$ and $EFSM_{server}$. This amendment assists us to understand the interaction of the encrypt-then-authenticate method by validating the authenticity of the encrypted message. The goal for these machines is to verify and distinguish good ciphertexts from bad ones. The next section will discuss the new EFSM for verification and review the Server EFSM and the Client EFSM with these amendments.

8.2.1 Verifier EFSM

The $EFSM_{verifier}$ is an embedded machine within $EFSM_{client}$ and $EFSM_{server}$ where states themselves can have other machines. To be precise, it is a set of sub-states that are integrated as a nested finite state machine which are nested inside the states S5 and S6 in $EFSM_{server}$ and state C6 in the $EFSM_{client}$. It is only activated when the authentication and key agreement have started. The $EFSM_{verifier}$ is triggered when it obtains authentication information from $EFSM_{client}$ or $EFSM_{server}$. It represents various transitions during the authentication and validation process. This machine is modelled using 5 states and 8 transitions. Table 8.1 describes the transitions specifications and Figure 8.1 illustrates the verifier modelled by EFSM.

Table 8.1: THE TRANSITIONS SPECIFICATION OF THE VERIFIER EFSM

Transition	Transition Direction	Guards/Condition
Validate	C5 → V0 S5 → V0 S6 → V0	
Authenticity check	V0 → V1	
Invalid	V1 → V0	Client_MAC != Server_MAC
Integrity checked	V1 → V2	Client_MAC == Server_MAC
Decrypted the ciphertext	V2 → V3	
Freshness checked	V3 → V4	$T` - T_{C_i} \leq \Delta T$
Invalid	V3 → V0	$T` - T_{C_i} > \Delta T$
ID valid	V4 → V0	
ID invalid	V4 → V0	Invalid ID

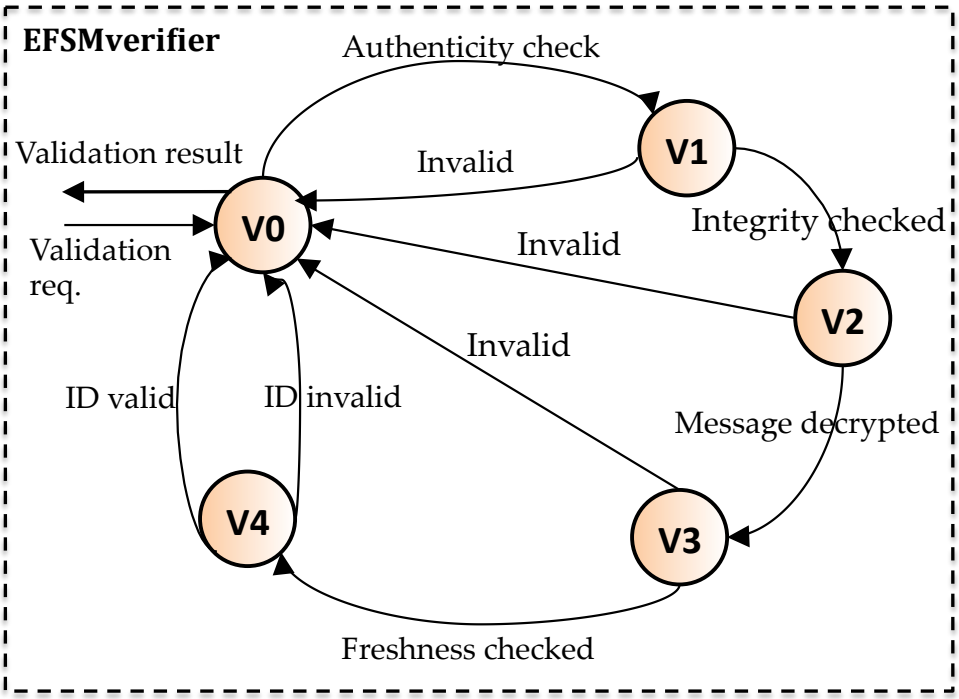


Figure 8.1: The verifier machine modelled by EFSM

- State V0: this state accepts the authentication information that needs to be verified and sends an authenticity-checking request to V1.
- State V1: the $EFSM_{verifier}$ verifies the integrity of the received cipher message by recalculating the MAC value of the received message and comparing it with the attached MAC value. If the MAC values are identical, the machine triggers itself to the next state, V2, since the condition is fulfilled. However, if the comparison shows a different result, this would trigger to invalid state that then leads to termination.
- State V2: while in this state, $EFSM_{verifier}$ decrypts the ciphertext since the MAC integrity check has been successful. After decryption is successful, the $EFSM_{verifier}$ transitions to the state V3.
- State V3: the $EFSM_{verifier}$ checks the freshness of T via $T` - T_{C_i} \leq \Delta T$. If the freshness is valid, the $EFSM_{verifier}$ triggers itself to the next state. Otherwise, it produces invalid input if the freshness of $T` - T_{C_i} \geq \Delta T$ and changes to state V0.
- State V4: while in state V4, the $EFSM_{verifier}$ checks the validity of ID and based on the result it changes to state V0 either with event of valid ID or invalid ID.

8.2.2 Server EFSM

The EFSM at the server side represents the various on-going communications with the client at any point in time. It is modelled using 10 states, 24 transitions, and two nested EFSMs as detailed in Table 8.2. Figure 8.2 illustrates the server machine modelled by EFSM.

Table 8.2: THE TRANSITIONS SPECIFICATION OF THE SERVER-SIDE EFSM

Transition	Transition Direction	Guards/Condition
Waiting for clients	S0 → S0	-
Request to enrol	S0 → R0	ClientEnrol == True
Client is registered	S0 → S1 R0→S0	ClientReg == True
Enter ID	S0 → S1	ID Valid
Enter Password	S1 → S2	Password Valid
Submit Biometric	S2 → S3	Biometric Valid
Request client login (SYN received)	S3 → S5	
Re-enter ID/Password/Biometric	S2→S2 S3→S3 S4→S4	ID_attempt < 3, ID_attempt = ID_attempt +1 PW_attempt < 3, PW_attempt = PW_attempt +1 Bio_Attempt == < 3, Bio_attempt = Bio_attempt +1
Invalid ID/Password/Biometric	S2→S4 S3→S4 S4→S4 S5→S4 S6→S4	ID_attempt == 3 PW_attempt == 3 Bio_Attempt == 3 Invalid ID
Send SYN/ACK and C2	S5→S6	Validation check is valid
Client ACK and C3 received	S6→S7	Validation check is valid
Terminate	S5→S8 S6→S8	
Timeout	S1→ S0 S2→S0 S3→S0	

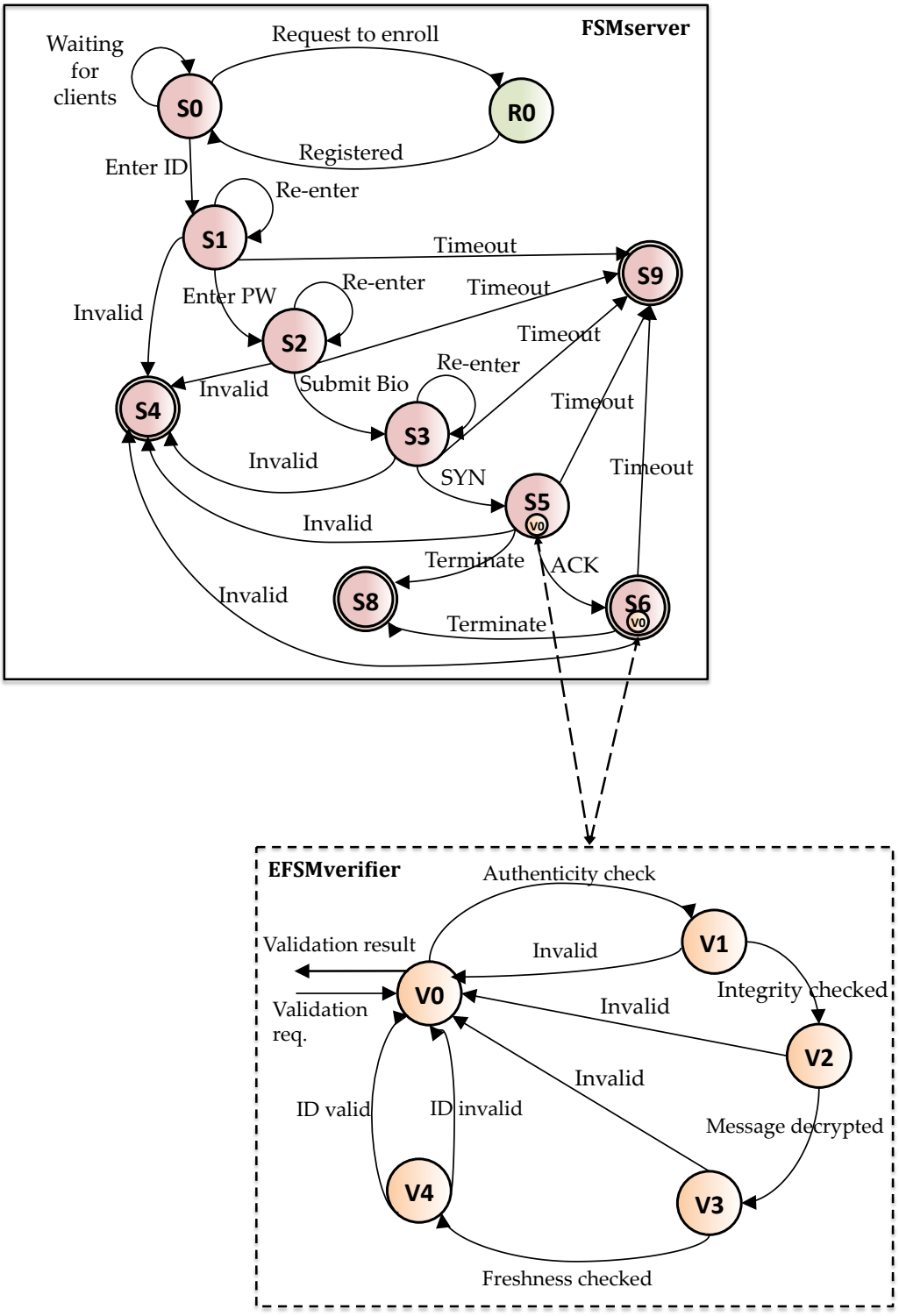


Figure 8.2: The server machine modelled by EFSM

9) The $EFSM_{server}$ will loop continuously while the server is waiting for clients. The machine advances to the next state once it is triggered by a login/enrol transition.

10) When the $EFSM_{server}$ is in the state S1, it checks the validity of the received ID. If ID is proved to be incorrect, S_i will request C_i to enter the valid ID up to three times and $EFSM_{server}$ will loop until C_i enters the valid ID or if the attempts exceed three times. In the latter case, the C_i's account will be blocked and $EFSM_{server}$ will change to state S4 from state S1. Generally, three attempts are made through our protocol steps to allow common errors.

11) When the $EFSM_{server}$ is in the state S2, it is triggered by a valid ID and it is now waiting for a valid PW. Once S_i receives PW, it verifies the validity of PW. If PW is proved to be invalid, S_i will request C_i to enter the valid PW up to three times and $EFSM_{server}$ will loop until C_i enters the valid PW or if the attempts exceed three times. In the latter case, the C_i's account will be blocked and $EFSM_{server}$ changes state to S4 from state S2.

12) When the $EFSM_{server}$ is in the state S3, it is triggered by a valid PW and it is now waiting for a valid Bio. Once S_i receives Bio, it verifies the validity of Bio by comparing the imprinted Bio with the template stored. If Bio does not match the stored template, S_i will request C_i to enter the valid Bio up to three times and the $EFSM_{server}$ will loop until C_i enters the valid Bio or if the attempts exceed three times. In the latter case, the C_i's account will be blocked and the $EFSM_{server}$ changes state to S4 from state S3.

13) In state S5, the $EFSM_{server}$ waits until it receives the login request $SYN = A_1 = C_1 \,||\, mac_1$ from the FSM_{client} to establish a connection by performing the three-way handshake.

14) While in state S5, the $EFSM_{server}$ activates the nested $EFSM_{verifier}$ and it waits for the validation check result.

15) Once the validation has proved to be true. S_i generates a random number and timestamp, then S_i replies with authenticated SYN/ACK $= A_2 = C_2 \,||\, mac_2$ to the $EFSM_{client}$, which is a combination of $C_2 = Enc\,\{ID_{C_i}, ID_{S_i}, T_{S_i}, W_2, M_6, M_7\}_a$ and $Mac_2 = MAC_k\,(ID_{C_i}, ID_{S_i}, T_{S_i}, W_2, M_6, M_7)$.

16) In state S6, $EFSM_{server}$ waits until it receives ACK from the $EFSM_{client}$. Once the authenticated ACK = $A_3 = C_3 \,||\, mac_3$ is received, the $EFSM_{server}$ activates the nested $EFSM_{verifier}$ and waits for the validation check result.

17) Once the validation check is proved to be true, the $EFSM_{server}$ verifies $M_9 \stackrel{?}{=} H_4\,(M_6 \,||\, rs_i)$. In this point, S_i authenticates C_i as a legitimate user.

18) At state S5 and state S6, $EFSM_{server}$ terminates the current session if any of the following situations occurs:

- The client ID is invalid
- The freshness of $T' - T_{C_i} \geq \Delta T$
- A negative result when checking the integrity of mac_1 and mac_3
- $M_2 != (x + H_1(ID_{C_i})^{-1}.\, W_1$
- $M_9 != H_4\,(M_6 \,||\, rs_i)$

At any stage of $EFSM_{server}$ activity, $EFSM_{server}$ aborts the current session and changes to state S9 if the timeout exceeds the defined TIME_WAIT while waiting for packets. This feature helps to prevent an infinite wait when the $EFSM_{client}$ fails to respond.

8.2.3 CLIENT EFSM

The EFSM at the client side represents the various on-going transmissions with the server at any point in time. It is modelled using 9 states, 22 transitions, and one nested EFSM as detailed in Table 8.3. Figure 8.3 shows the transitions diagram for the $EFSM_{client}$.

1) First, the $EFSM_{client}$ is in the initial state C0. That is when the request for register/login is initiated by itself. While in state C0, the $EFSM_{server}$ checks whether C_i is enrolled or not. The next state will be determined according to the condition $ClientReg == True$.
2) In state C1, C2, C3, the FSM_{client} is waiting for validating ID, PW, and Bio. Once the client credentials are validated, the $EFSM_{client}$ triggers itself and changes to state C5.
3) In states C1, C2, C3, the client may be required to re-enter ID, PW, Bio in cases where they were incorrect. However, the client's account will be blocked if the number of attempts exceeds three, which changes the above states to state C4.

    - $ID\_attempt < 3, ID\_attempt = ID\_attempt + 1$
    - $PW\_attempt < 3, PW\_attempt = PW\_attempt + 1$
    - $Bio\_Attempt < 3, Bio\_attempt = Bio\_attempt + 1$

Table 8.3: THE TRANSITIONS SPECIFICATION OF THE CLIENT-SIDE EFSM

Transition	Transition Direction	Guards/Condition
Request to enrol	C0 → R0	ClientEnrol == True
Client is registered / Enter ID	C0 → C1	ClientReg == True
Enter Password	C1 → C2	ID valid
Submit Biometric	C2 → C3	Password valid
Send login request SYN (C_1)	C3 → C5	Biometric valid
Re-enter ID/Password/Biometric	C1→C1 C2→C2 C3→C3	ID_attempt < 3, ID_attempt = ID_attempt +1 PW_attempt < 3, PW_attempt = PW_attempt +1 Bio_Attempt < 3, Bio_attempt = Bio_attempt +1
Invalid ID/Password/Biometric	C1→C4 C2→C4 C3→C4	ID_attempt == 3 PW_attempt == 3 Bio_Attempt == 3
Client receives SYN/ACK (C2)	C5→C6	
Client sends ACK (C3)	C6→C7	Validation check is valid
Authenticated by server	C7→C8	
Terminate	C5→C8 C6→C8	
Timeout	C1→C0 C2→C0 C3→C0	

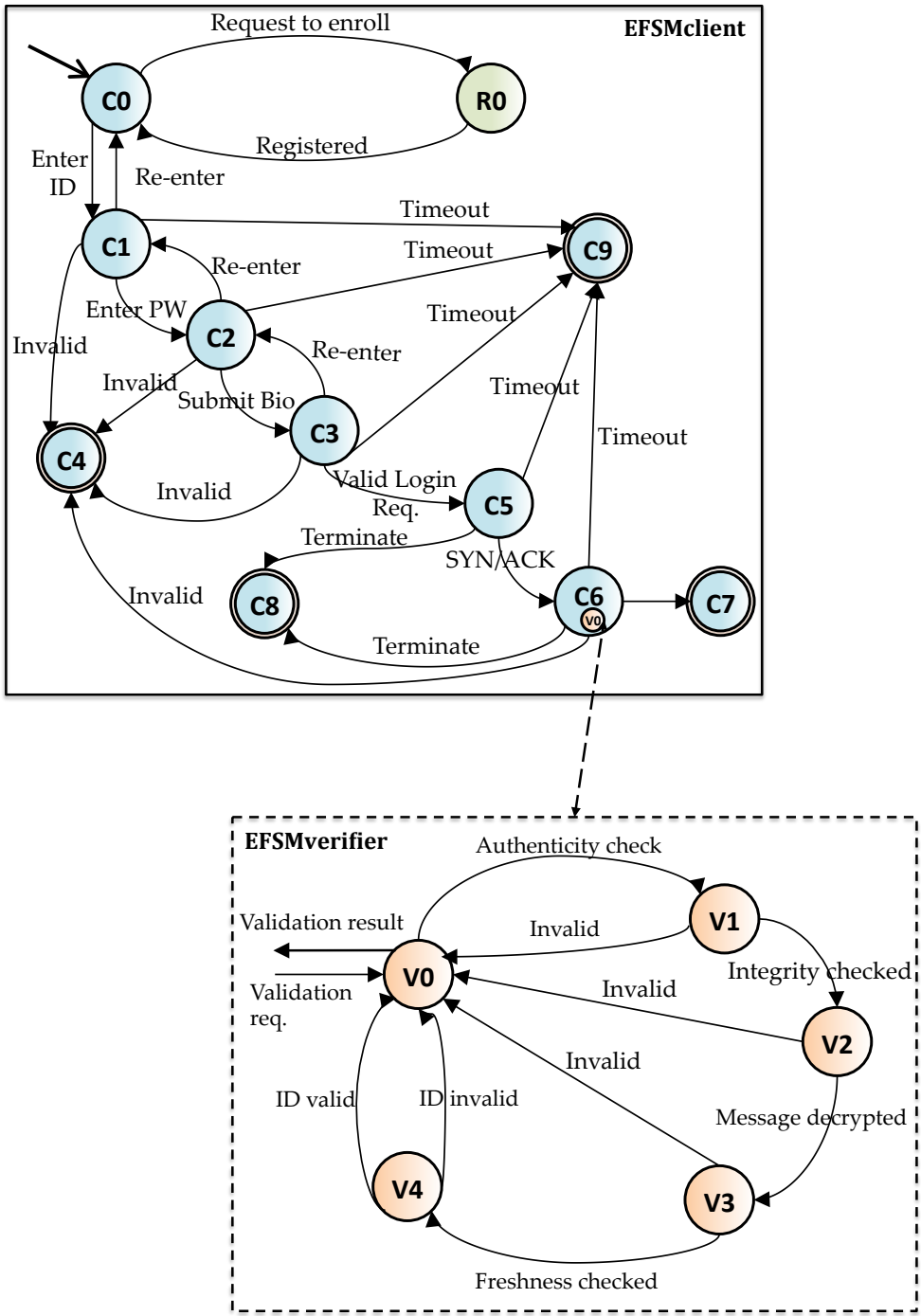


Figure 8.3: The client machine is modelled by EFSM

4) In state C5, The $EFSM_{client}$ generates a random number and a timestamp to calculate the encrypted login request $\{ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3\}_a$ and then computes $mac_1 = MAC_k(ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3)$. It sends $A_1 = C_1 \,||\, mac_1$ to the $EFSM_{server}$. This request represents the SYN part in the three-way handshake procedure.

5) While in state C5, the FSM_{client} is waiting for the $EFSM_{server}$ to respond after sending the login request to establish the connection. Once the authenticated SYN/ACK = $A_2 = C_2 \,||\, mac_2$ is received, the FSM_{client} changes to state C6.

6) In state C6, the $EFSM_{client}$ activates the nested $EFSM_{verifier}$ and waits for the validation check result. Once the validation check is proved to be true, the $EFSM_{client}$ is validating the $EFSM_{server}$ response $M_7 \stackrel{?}{=} H_4(M_4 \,||\, r_{C_i})$. If $\boldsymbol{S_i}$ is proved to be honest, $\boldsymbol{C_i}$ authenticates $\boldsymbol{S_i}$ at this stage.

7) While in state C6, the $EFSM_{client}$ computes the shared session key $sk = H_3(ID_{C_i}, T_{C_i}, T_{S_i}, W_1, W_2, K_{C_i})$ and finalises the handshake procedure by sending authenticated encrypted ACK = $A_3 = C_3 \,||\, mac_3$ to $\boldsymbol{S_i}$, which is a combination of $C_3 = Enc\{ID_{C_i}, ID_{S_i}, T_{C_i}, M_9\}_a$ and $Mac_3 = MAC_k(ID_{C_i}, ID_{S_i}, T_{C_i}, M_9)$.

8) In state C7, the $EFSM_{client}$ is waiting to be authenticated by $\boldsymbol{S_i}$.

9) In state C8, the client terminates the current session if one of the following occurs:

   - Negative result when checking the integrity of mac_2
   - $T^{`} - T_{S_i} \geq \Delta T$
   - The server ID is invalid

- $M_7 != H_4 (M_4 || r_{C_i})$

8.2.4 DISCUSSION

The state machine in Figure 8.4 represents the result of combining the three machines together after the modifications. The composite model executes efficiently and handles errors in a safe way according to their types. The modified protocol connection progresses from one state to another based on the data obtained from the messages exchanged. EFSM helps one to understand the behaviour of the protocol and logs the unwanted behaviours. This mechanism is very useful for determining the types of errors the protocol experiences during running and it can be useful to investigate later on what causes these errors and learn from them.

Based on the parallel behaviour, each machine goes through stages until it reaches the accepted state. For example, after successful authorisation, the $EFSM_{client}$ switches to the authorised state and proceeds to reach the next state, which is authentication.

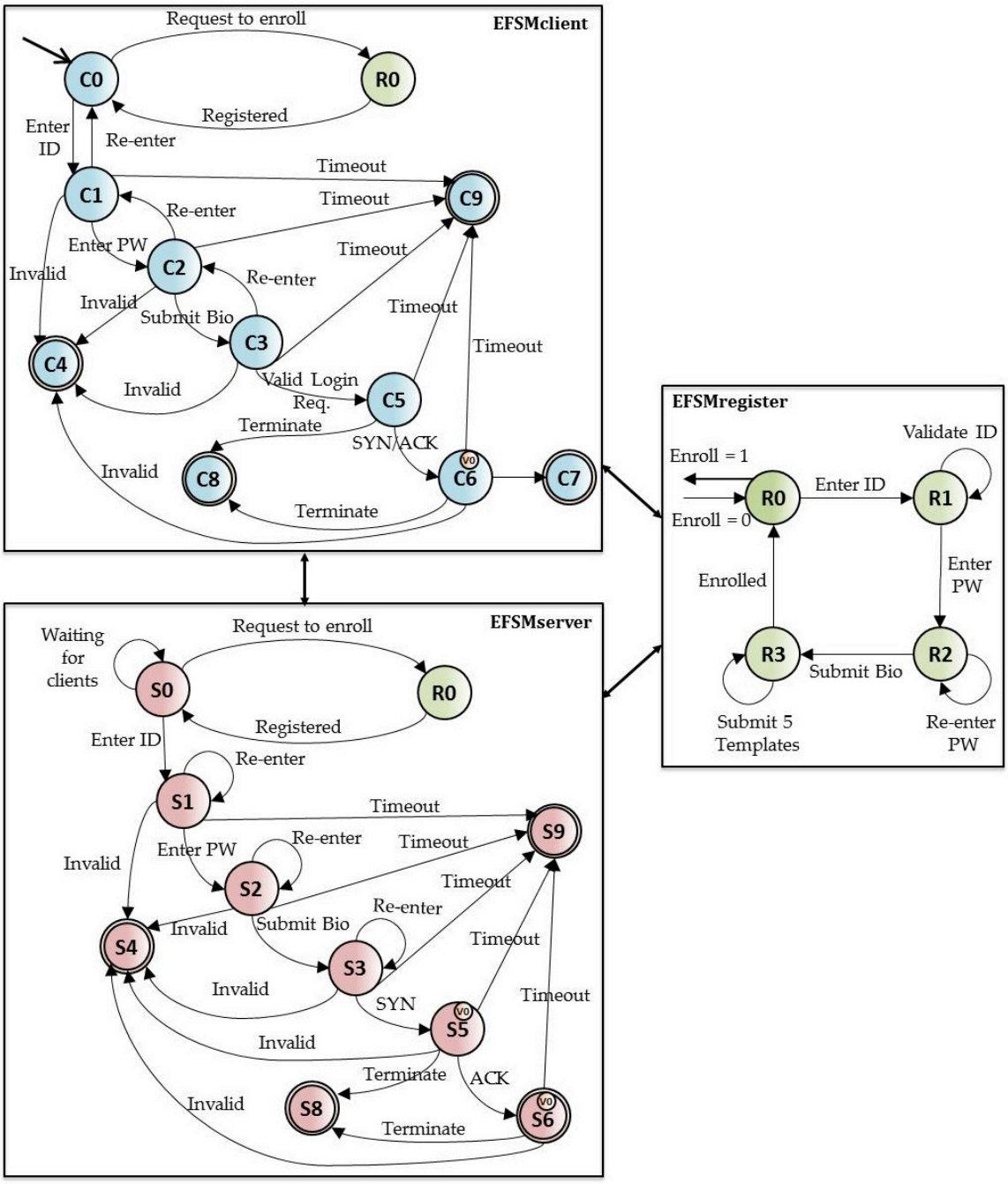


Figure 8.4: The modified protocol modelled by EFSM

This comprehensive analysis distinguishes three types of errors that can be detected during the protocol run:

- ***Type I: Timeout errors***

This error occurs when the waiting time exceeds the predefined time interval or it occurs when the freshness check exceeds ΔT.

- ***Type II: Invalid errors***

This error is generated in case of invalid inputs, for example, invalid ID, invalid password, or invalid biometric.

- ***Type III: Terminate error***

This error detects if something suspicious occurs in cases where values did not match. A typical example of this error can be found in the integrity check, when the recomputed MAC value does not match the received MAC value. Another example is when there is a discrepancy in the results of the following equations:

- $M_2 != (x + H_1(ID_{C_i})^{-1}. W_1$
- $M_7 != H_4 (M_3 || r_{C_i})$
- $M_9 != H_4 (M_6 || r_{S_i})$

This error can pose a serious threat because it would only occur if the data has been modified or injected.

8.3 Review of Security Properties

Security properties are considered one of the main pillars that effectively contribute to mitigate or eliminate vulnerabilities. They improve protocol efficiency in order to withstand any potential threat or weakness. Continually evaluating cryptography protocols and keeping up to date with the latest security threats and vulnerabilities are the key to maintain strong and robust protocols. A security hole in the protocol is like a gateway for attackers to invade a system. From the attacker's point of view, any flaw in cryptographic protocols gives them the opportunity to gain unauthorised access and privileges. In addition, the successful result of any other exploits would give the attacker an advantage to take complete control of the affected target, i.e. install programmes, delay, modify or delete data. The next section formalises the types of security goals the modified protocol is capable of achieving.

8.3.1 Mutual Authentication and Session Key Agreement

The modified protocol accomplishes mutual authentication and secret session key agreement based on ECC between a remote client and the server by establishing a three-way challenge-response handshake technique. First, the client C_i sends an authenticated encrypted login request message $A_1 = C_1 \,||\, mac_1$ to the server S_i. Then S_i verifies the received ciphertext by checking the MAC integrity. After validating, S_i sends an authenticated encrypted challenge message $A_2 = C_2 \,||\, mac_2$ to C_i. Next, C_i checks the integrity of the encrypted message, then the validity of the received message $M_7 \stackrel{?}{=} H_4 (M_3 \,||\, r_{C_i})$ and accepts or rejects the server request according to the verification result. Finally, C_i sends an authenticated encrypted response message $A_3 = C_3||mac_3$ to S_i. Upon receiving the message, S_i checks the integrity of the

ciphertext then verifies if $M_9 \stackrel{?}{=} H_4(M_6 \,||\, r_{S_i})$ holds. If so, $\boldsymbol{S_i}$ authenticates client $\boldsymbol{C_i}$ and allows it access. During the process, both S_i and C_i compute the session key $sk = H_3(ID_{C_i}, ID_{S_i}, T_{C_i}, T_{S_i}, W_1, W_2, (r_{S_i}.r_{C_i}.P))$ successfully.

8.3.2 CONFIDENTIALITY

Confidentiality or, as it is sometimes called, secrecy, is the capability to prevent an intruder from being able to capture sensitive data transmitted between two legitimate entities. In other words, confidentiality will be breached if a malicious intruder is able to listen in and derive an element from a set of plaintext messages passing between the honest nodes. There are three types of cryptographic algorithm that provide privacy and confidentiality:

1) Symmetric cryptography that uses secret shared keys between entities
2) Asymmetric cryptography that uses different key pairings for encryption and decryption.

The modified protocol conceals the contents of transmitted data by using symmetric encryption. Encryption can handle the problem of privacy and it can protect the traffic from passive attacks such as eavesdropping and may be traffic analysis in case IPV6 is implemented. Also, hash functions can protect sensitive data and computation values from tampering.

8.3.3 INTEGRITY

Integrity is relates to the trustworthiness of data and resources in term of preventing improper and unauthorised modifications. MAC is one of the mathematical approaches providing a high level of integrity. The modified protocol relies on the

fact that integrity checks are performed before decrypting data since the MAC plays a significant role in data integrity and message authentication. Thus, it provides protection of the ciphertext as encryption is only susceptible to active attacks. Verification of data integrity requires the recipient to calculate the hash value of the MAC and then decrypt the ciphertext if the integrity check is passed. Otherwise, the recipient will terminate the session. This mechanism helps to distinguish between incorrect MACs and correct ones and discard any message with accidental modifications such as errors, or intentional modifications such as altered data contents.

8.3.4 AUTHENTICITY

Authentication ensures that the transmitted data is authentic and has not been tampered with. Authentication can be categorised into two ways: data origin authentication and entity authentication. The former is concerned with validating the authenticity of message contents and that the message originated from the claimed source. The latter is related to identifying the identity of the sender and ensuring the entity communicating with is indeed the correct agent that it is claimed to be (Ryan and Schneider, 2001; Dong and Chen, 2012).

Using the cryptographic one-way hash function (COWH) ensures the authorship of the content due to secret key encryption. This method works as modification detection as well as it preserves data integrity. Another important point to stress is that COWH is more practical and increases efficiency instead of using a digital signature for the entire message. A keyed MAC is also used to validate the encrypted message as well as to verify the source of the sent ciphertext. The modified protocol

accomplishes data origin authenticity by certifying the authenticity of the encrypted message through the MAC. Entity authenticity is accomplished by verifying the following between the client and the server:

- The identity of the client ID_{C_i}
- The client's password and biometric $z`_i = H_4\ (PW_{C_i} \,||\, f_i)$
- The identity of the server ID_{S_i}
- Verification through client's private key:

$$M`_2 = (x + H_1(ID_{C_i})^{-1}.W_1$$

$$= Pr\_K_{C_i} \,.\, r_{C_i}$$

$$= M_2$$

- Authenticating the server by the client through verifying the value of $M_7 \stackrel{?}{=} H_4\ (M_3 \,||\, r_{C_i})$
- Authenticating the client by the server through verifying the value $M_9 \stackrel{?}{=} H_4\ (M_6 \,||\, r_{S_i})$

8.3.5 NON-REPUDIATION

Non-repudiation is the assurance that ensures the entities that are involved in the communication cannot later deny having sent or received the message. In the modified protocol, the generated MAC acts as an indicator of who sent the message and offers assurance of the source of the message. Since the client and the server have the same secret key, both entities can re-compute the MAC using their shared variables. In other words, the MAC confirms the authenticity of the message originator to be verified by the recipient.

8.4 SECURITY EVALUATION

Petri Nets (PN) are used to model the concurrency of a complex version of the proposed protocol but with a significant modification as mentioned previously. The method of encrypt-then-authenticate will definitely improve the security of the protocol. The complex protocol consists of two honest entities, the client and the server. First, PN is used to model and analyse the modified protocol. Then, an adversary entity is added to the trust model to analyse various attacks and test the protocol security.

8.4.1 THE CLIENT-SERVER TRUST MODEL

The trust model for the modified protocol is based on the same assumptions in section 7.2. The Petri net model for the modified protocol is illustrated in Figure 8.5. The definitions of the places and the transitions used in this model are listed in Table 8.4 and Table 8.5, respectively.

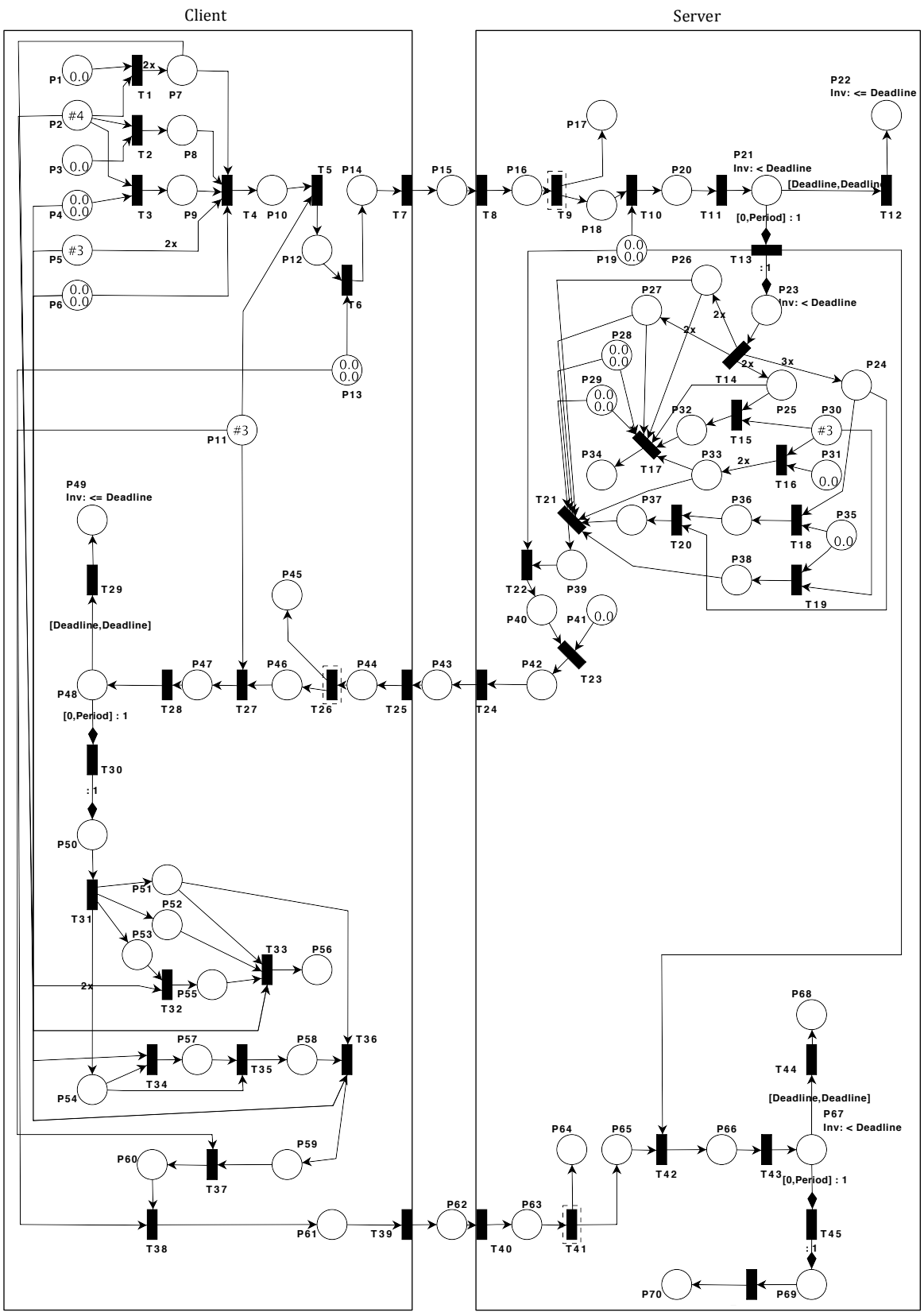


Figure 8.5: Modelling the modified trust model

Table 8.4: DEFINITIONS OF PLACES - THE MODIFIED TRSUST MODEL

Place	Definition	Place	Definition
P_1	A point on elliptic curve E with order n	P_{35}	M_4
		P_{36}	$M_5 = M_3 \oplus M_4$
P_2	Client random number	P_{37}	$M_7 = H_4(M_3 \| M_5)$
P_3	Client private key	P_{38}	$M_6 = M_4 \oplus r_{S_i}$
P_4	$M_1=e_i \oplus z'_i$	P_{39}	SYN/ACK = ID_{C_i}, ID_{S_i}, T_{S_i}, W_2, M_6, M_7
P_5	Client ID		
P_6	Client timestamp	P_{40}	Encrypted SYN/ACK
P_7	$W_1=r_{C_i} . P$	P_{41}	MAC Secret Key *k*
P_8	$M_2= r_{C_i} . Pr\_K_{C_i}$	P_{42}	Authenticated C_2
P_9	$M_3= M_1 \oplus r_{ci}$	P_{43}	Sent A_2
P_{10}	$SYN=ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3$	P_{44}	Received A_2
		P_{45}	Message is not authentic
P_{11}	Shared secret key *a*	P_{46}	Message is authentic
P_{12}	Encrypted message C_1	P_{47}	Decrypted C_2
P_{13}	MAC Secret Key *k*	P_{48}	Verification message
P_{14}	Authenticated ciphertext A_1	P_{49}	Rejected request
P_{15}	Sent A_1	P_{50}	Accepted request
P_{16}	Received A_1	P_{51}	Server ID
P_{17}	Message is not authentic	P_{52}	Server timestamp
		P_{53}	W_2
P_{18}	Message is authentic	P_{54}	M_6
P_{19}	Shared secret key *a*	P_{55}	Computed Kc
P_{20}	Decrypted C_1	P_{56}	Computed session key
P_{21}	Verification message	P_{57}	M_8
P_{22}	Rejected request	P_{58}	M_9
P_{23}	Accepted request	P_{59}	ACK
P_{24}	M_3	P_{60}	C_3=Encrypted ACK
P_{25}	W_1	P_{61}	A_3=Authenticated ACK
P_{26}	Client timestamp	P_{62}	Sent A_3
P_{27}	Client ID	P_{63}	Received A_3
P_{28}	Server timestamp	P_{64}	Message is not authentic
P_{29}	Server ID	P_{65}	Message is authentic
P_{30}	Server random number	P_{66}	Decrypted C_1
P_{31}	A point on elliptic curve E with order n	P_{67}	Verification message
		P_{68}	Rejected request
P_{32}	Computed Ks	P_{69}	Accepted request
P_{33}	$W_2= r_{S_i}.P$	P_{70}	Client is authenticated
P_{34}	Computed session key		

Table 8.5: DEFINITIONS OF TRANSITIONS - THE MODIFIED TRUST MODEL

Trans.	Definition	Trans.	Definition
T_1	Perform multiplication operation to compute w_1	T_{24}	Transmit A_1
T_2	Perform multiplication operation to compute M_2	T_{25}	Receive A_1
T_3	Perform XOR operation to compute M_3	T_{26}	Shared transition that check the integrity of A_2
T_4	Create SYN request	T_{27}	Decrypt C_2
T_5	Encrypt SYN with a	T_{28}	Verify
T_6	Compute the MAC value of C_1	T_{29}	Drop the request
T_7	Transmit A_1	T_{30}	Accept
T_8	Receive A_1	T_{31}	Split the packet
T_9	Shared transition that check the integrity of A_1	T_{32}	Compute Kc
T_{10}	Decrypt C_1	T_{33}	Compute the session Key SK
T_{11}	Verify	T_{34}	Compute M_8
T_{12}	Drop the request	T_{35}	Compute M_9
T_{13}	Accept	T_{36}	Create ACK = C_3
T_{14}	Split the packet	T_{37}	Encrypt
T_{15}	Compute Ks	T_{38}	Compute the MAC value of C_3
T_{16}	Compute W_2	T_{39}	Transmit A_3
T_{17}	Compute the session key	T_{40}	Receive A_3
T_{18}	Perform XOR operation to compute M_5	T_{41}	Shared transition that check the integrity of A_3
T_{19}	Perform XOR operation to compute M_6	T_{42}	Decrypt C_1
T_{20}	Concatenate M_3 and M_5 and hash the output to produce M_7	T_{43}	Verify
T_{21}	Create SYN/ACK	T_{44}	Drop the request
T_{22}	Encrypt SYN/ACK = C_2	T_{45}	Accept
T_{23}	Compute the MAC value of C_2	T_{46}	Authenticate the client

Figure 8.5 shows the complex PN model for the modified protocol. The left part of the model represents the client $\boldsymbol{C}$ and the right part of model represents the server $\boldsymbol{S}$. The client-server trust model contains 70 places and 46 transitions including three shared transitions. The *places* in the modelled protocol represent the state of the net, storage for requests, messages, ciphers, or session keys. Each place can be assigned with one or more *tokens*, and each token represents a specific data item. The *transitions* in the modelled protocol define particular functions or procedures. The *marking* of the PN model determines the actual state of the net, which constitutes the

number of tokens in the specific places. The simulation of the modified trust model focuses on the messages exchanged between the entities and mutual authentication. The behaviour of the net can be divided into four stages as follows:

Simulating Stage 1:

This is the initial phase where $\boldsymbol{C}$ attempts to communicate with $\boldsymbol{S}$ and establish a secure session key. $\boldsymbol{C}$ consumes a token from each place: P_1, P_2, P_3, and P_4 to generate P_7, P_8, and P_9, by firing transitions T_1, T_2, T_3. This simulation corresponds to the following:

- $W_1 = r_{C_i}.P$
- $M_2 = r_{C_i}.Pr\_K_{C_i}$
- $M_3 = M_1 \oplus r_{C_i}$

Next, $\boldsymbol{C}$ consumes one token for the timestamp P_6 and two tokens of P_5, (one token for ID_C and another for ID_S) together with the generated tokens in P_7, P_8, and P_9 to compute the SYN request via T_4. This simulation creates the login request, which corresponds to $(ID_C, ID_S, T_C, W_1, M_2, M_3)$. At this stage, the method of encrypt-then-authenticate is applied by enabling the T_5 and consuming one token of P_{11} as the secret key to encrypt P_{10}. This part of the simulation achieves only the first segment of the mechanism to produce the encrypted message P_{12}. The second segment to complete the other part of the mechanism is simulated by firing T_6 and consuming one token from P_{13}. This allows the net to calculate the MAC value of the encrypted message and append it to the ciphertext. Finally, $\boldsymbol{C}$ sends P_{15} to $\boldsymbol{S}$.

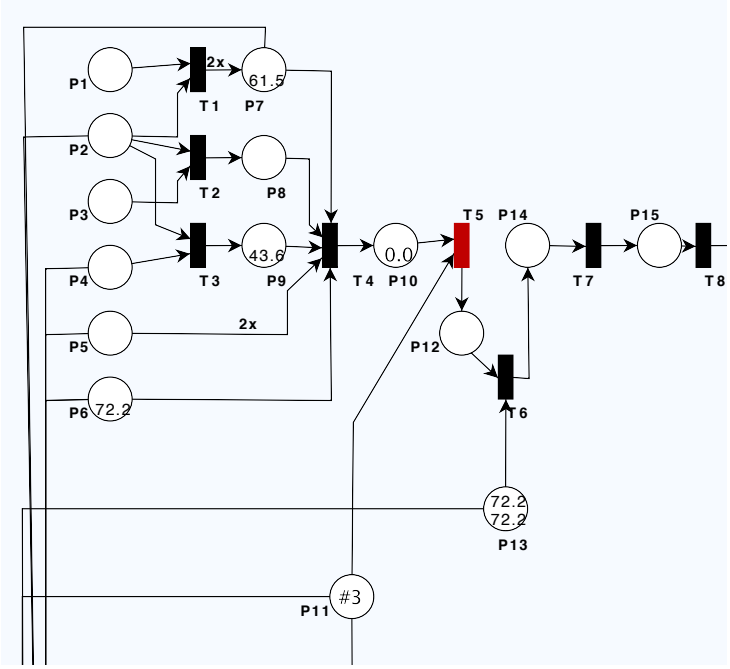


Figure 8.6. The client encrypts SYN request

Simulating Stage II:

This stage represents the second part of the handshake. $\boldsymbol{S}$ must ensure the authenticity of received encrypted SYN = P_{10}. The transitions T_9 and T_{11} help $\boldsymbol{S}$ to validate the SYN request. Transition T_9 is a shared transition that checks the integrity of the received ciphertext. T_9 is a nested component of the net that consists of six places and three transitions (Figure 8.6). The goal of this component is checking the integrity of the ciphertext. This is achieved by computing the MAC value of the ciphertext and then comparing it with the received MAC value. If the values are not equal, $\boldsymbol{S}$ terminates the session, otherwise it proceeds to T_{11}. The next step is to verify the freshness of time via T_{11} and based on the verification result $\boldsymbol{S}$ will drop the session or proceed.

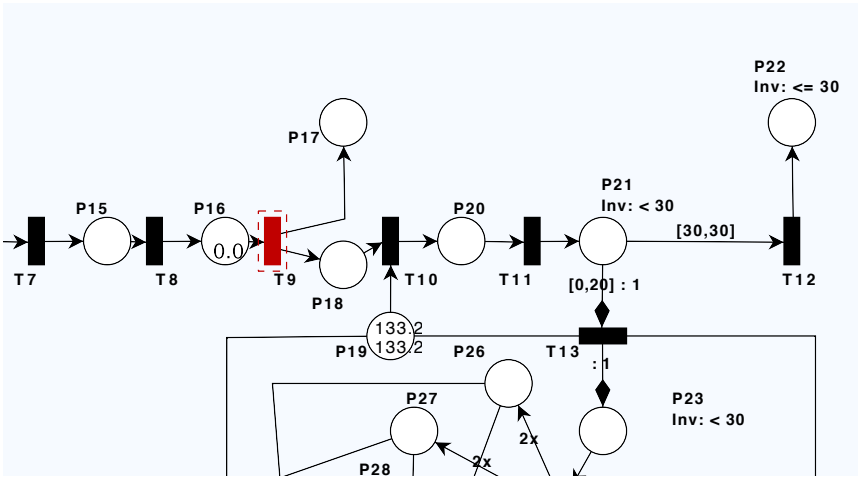


Figure 8.7: The server checks the integrity of encrypted SYN request

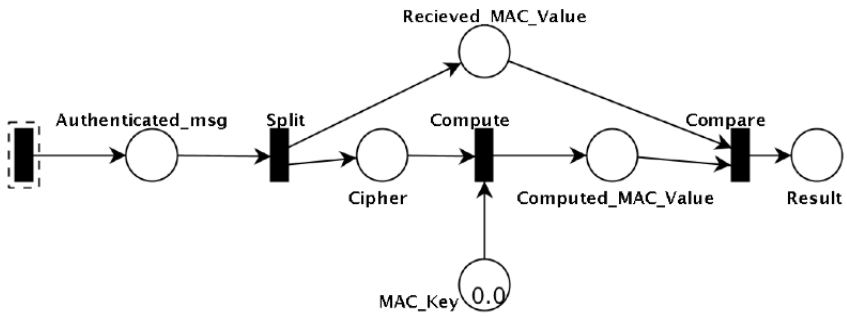


Figure 8.8: Modelling the shared transitions

Once the validation and verification are checked, ***S*** splits the packets via T_{14} and distributes tokens to the corresponding places P_{24}, P_{25}, P_{26}, and P_{27} in order to compute the session key P_{34}. This simulation produces new values for the following places:

- P_{33}: $W_2 = r_{S_i}.P$
- P_{32}: $K_{S_i} = r_{S_i}.W_1$

- P_{34}: $sk = H_3\ (ID_{C_i}, ID_{S_i}, T_{C_i}, T_{S_i}, W_1, W_2, K_{S_i})$

The next simulation computes P_{36}, P_{37} and P_{38}, via T_{18}, T_{20}, and T_{19} respectively, which correspond to the following:

- $M_5 = M_3 \oplus M_4 = r_{C_i}$
- $M_6 = M_4 \oplus r_{S_i}$
- $M_7 = H_4(M_3 \,||\, M_5)$

At this stage, $\boldsymbol{S}$ is ready to formulate the P_{39} =*SYN/ACK* message via T_{21}. In order for $\boldsymbol{S}$ to apply the mechanism encrypt-then-authenticate, the SYN/ACK must be first encrypted via T_{22} with key P_{19} then authenticated via T_{23}. Then $\boldsymbol{S}$ sends the authenticated encrypted message to $\boldsymbol{C}$ via T_{24}.

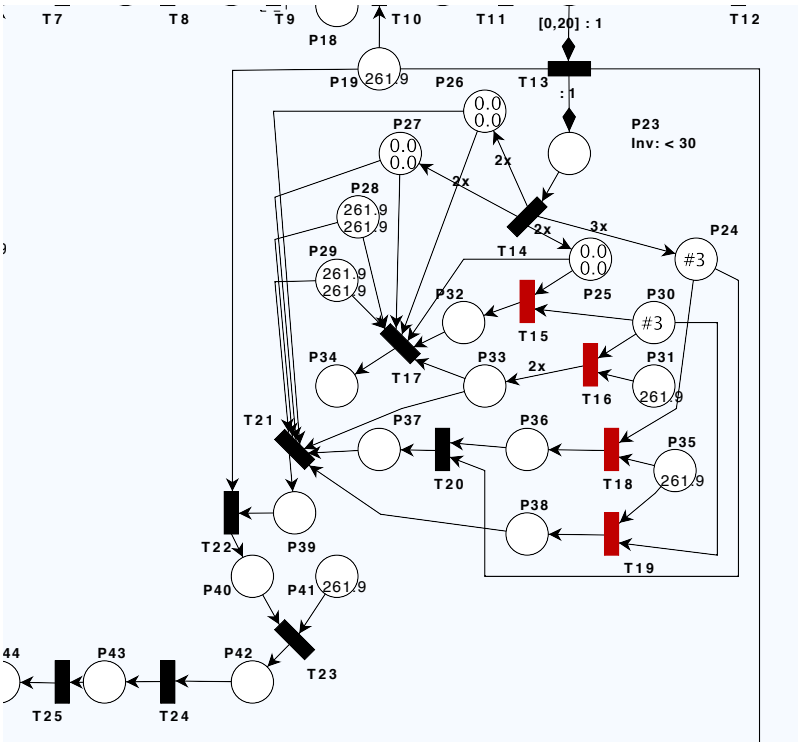


Figure 8.9: The server computes the session key and SYN/ACK

Simulating Stage III:

This stage represents the third part of the handshake, where $\boldsymbol{C}$ receives SYN/ACK and replies with an ACK. When $\boldsymbol{C}$ receives P_{44} it checks for the integrity of the ciphertext via T_{26}. This transition is a shared transition and its functionality is very similar to T_9. Once the verification for the integrity of the ciphertext is proved to be authentic, the next simulation enables T_{27} to decrypt P_{46} with secret key P_{11}. Then transition T_{28} verifies the freshness of the message. The next simulation relies on the packet received to calculate the session key. Transition T_{31} splits the packet and generates tokens to P_{51}, P_{52}, and P_{53} and T_{32} is fired to compute $P_{55} = K_C$. At this stage, $\boldsymbol{C}$ can securely compute the session key P_{56} via T_{33}. At this moment, $\boldsymbol{C}$ must generate an ACK message and send it to $\boldsymbol{S}$ to complete the authentication key agreement phase. The simulation fires T_{34} to generate P_{57} and T_{35} to generate P_{58} by consuming one token from P_4 and P_{54}, and from P_{54} and P_{57}, respectively. This step corresponds to the following in the protocol:

- $M_8 = M_6 \oplus M_1$
- $M_9 = H_4(M_6 \,||\, M_8)$

At this stage, $\boldsymbol{C}$ is ready to formulate the $P_{59} = ACK$ message via T_{36}. In order for $\boldsymbol{C}$ to apply the mechanism encrypt-then-authenticate, the ACK must be first encrypted via T_{37} with the shared key P_{11} then authenticated via T_{38}. Then $\boldsymbol{C}$ sends the authenticated encrypted message to $\boldsymbol{C}$ via T_{39}.

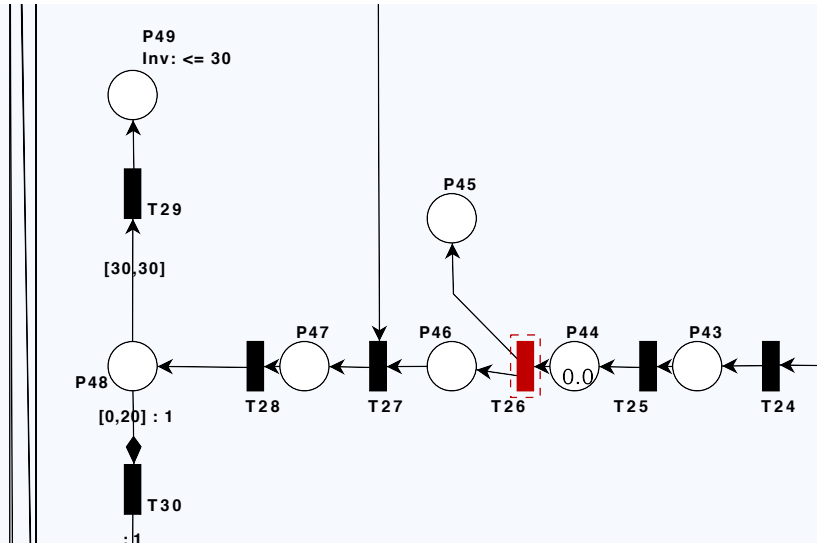


Figure 8.10: The client checks the integrity of the encrypted SYN/ACK request

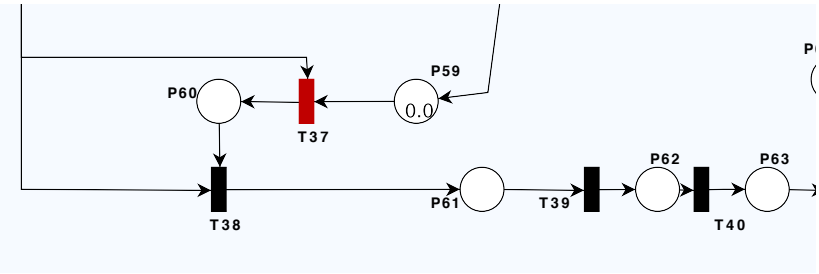


Figure 8.11: The client applies the encrypt-then-authenticate method to ACK

Simulating Stage IV:

This stage represents the final part of the handshake, where ***S*** receives the ACK and authenticates ***C***. When ***S*** receives P_{63} it checks for the integrity of the ciphertext via T_{41}. This transition is a shared transition and its functionality is very similar to T_9 and T_{26}. Once the verification for integrity of ciphertext is proved to be authentic, the

next simulation enables T_{42} to decrypt P_{65} with secret key P_{19}. Then transition T_{28} verifies the freshness of the message. $\boldsymbol{S}$ authenticates $\boldsymbol{C}$ via T_{46}.

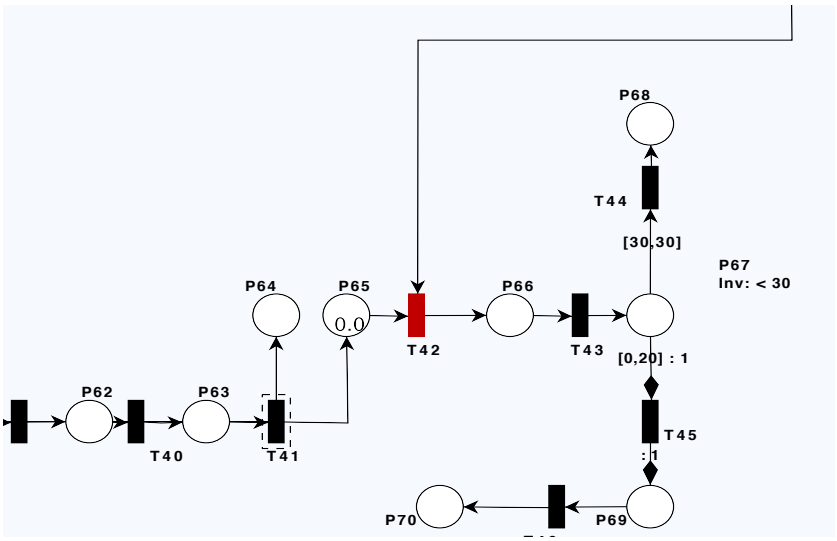


Figure 8.12: The server checks the integrity of the encrypted ACK

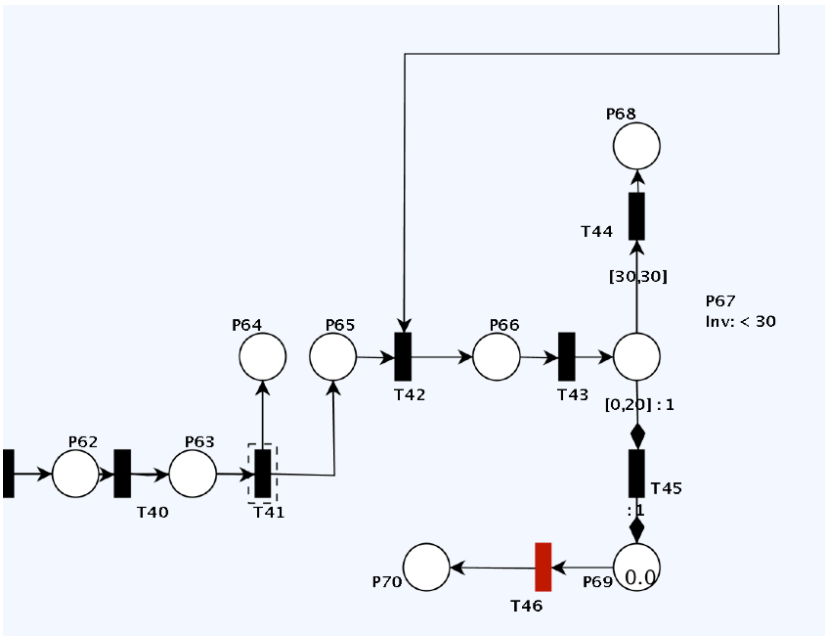


Figure 8.13: The server authenticates the client

8.4.2 TRUST MODEL WITH ADVERSARY

The modified protocol should be designed to withstand attacks and should prove its soundness even if an adversary has control over the communication channel and attempts to delay, delete, or modify the contents of the original messages. To verify whether the modified protocol satisfies its desired specifications, it is fundamental to model the modified protocol and test its performance against attacks. Adding an adversary entity for the modified client-server trust model allows predicating the protocol behaviour. The adversary is modelled as a separate entity that can control the channel between the client and the server. The following assumptions are considered for the adversary model:

1) The adversary can eavesdrop, intercept, and store a message. It may block or pass any of these messages. Additionally, it may construct forged messages from captured data and inject them into the channel.
2) The adversary has zero knowledge, in such that it does not possess any elements of messages transmitted between the legitimate nodes, but it can learn by observing the traffic.
3) The traffic between client and server is encrypted then authenticated.
4) MAC functions are secure against chosen-message attacks.
5) Symmetric encryption functions are secure against chosen-plaintext attacks.

The attack model for the modified protocol is illustrated in Figure 8.14. The definitions of the places and the transitions used in this model are listed in Table 8.6 and Table 8.7 respectively.

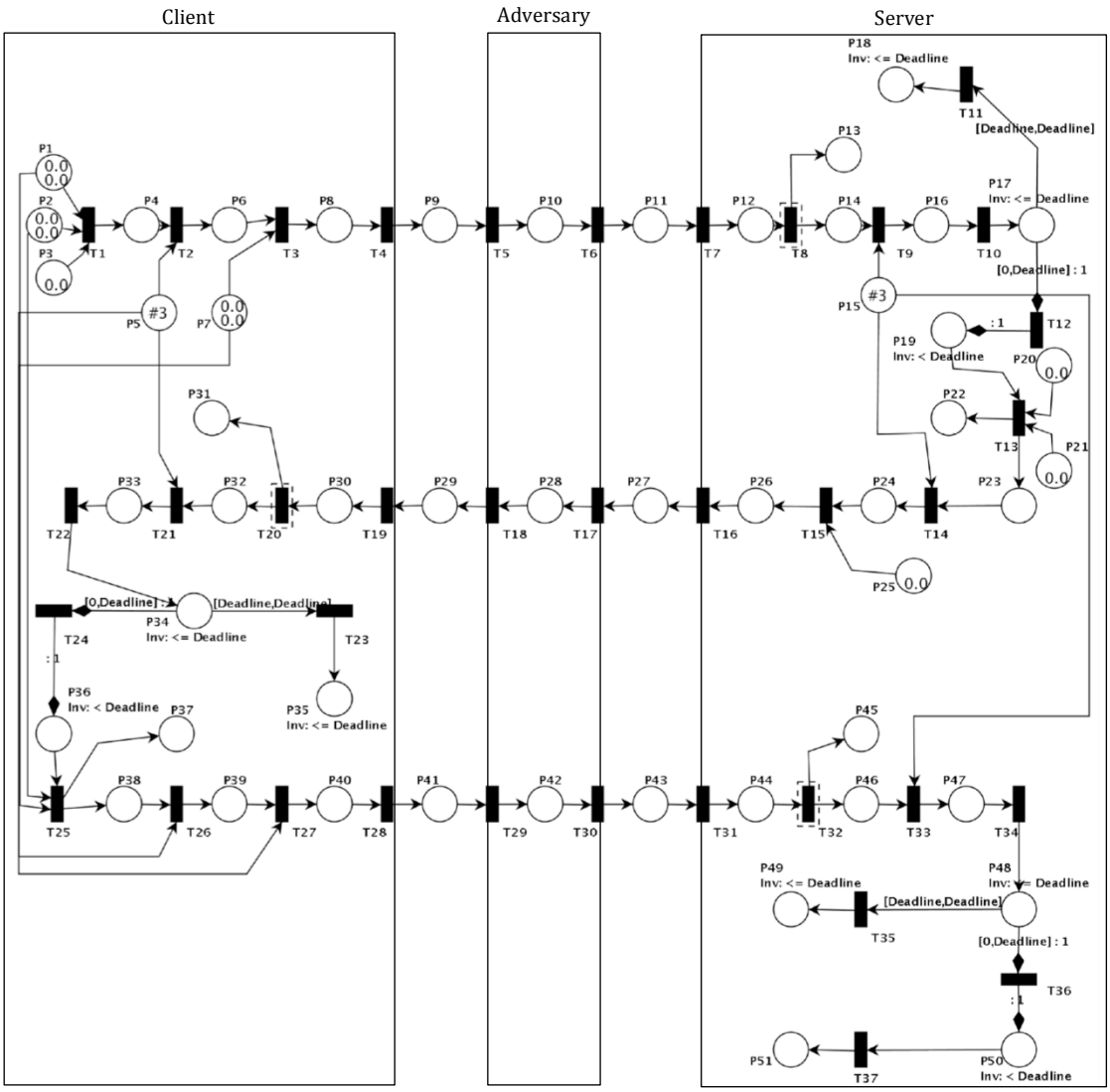


Figure 8.14: The modified trust model with adversary

Table 8.6: DEFINITIONS OF PLACES - THE MODIFIED TRUST MODEL WITH ADVERSARY

Place	Definition	Place	Definition
P_1	Client random number	P_{27}	Sent A_2
P_2	Client timestamp	P_{28}	Intercepted A_2
P_3	SYN request	P_{29}	Passed A_2
P_4	Login request	P_{30}	Received A_2
P_5	Symmetric key	P_{31}	Message is not authentic
P_6	Ciphertext C_1	P_{32}	Message is authentic
P_7	MAC secret key	P_{33}	Decrypted C_1
P_8	Authenticated ciphertext	P_{34}	Verification message
P_9	Sent A_1	P_{35}	Rejected request
P_{10}	Intercepted A_1	P_{36}	Accepted request – S is
P_{11}	Passed A_1		authenticated
P_{12}	Received A_1	P_{37}	Session Key
P_{13}	Message is not authentic	P_{38}	ACK
P_{14}	Message is authentic	P_{39}	Ciphertext
P_{15}	Symmetric key	P_{40}	Authenticated ciphertext
P_{16}	Decrypted C_1	P_{41}	Sent A_3
P_{17}	Verification message	P_{42}	Intercepted A_3
P_{18}	Drop request	P_{43}	Passed A_3
P_{19}	Accepted request	P_{44}	Received A_3
P_{20}	Server random number	P_{45}	Message is not authentic
P_{21}	Server timestamp	P_{46}	Message is authentic
P_{22}	Session key	P_{47}	Decrypted C_1
P_{23}	SYN/ACK	P_{48}	Verification message
P_{24}	Ciphertext C_2	P_{49}	Drop request
P_{25}	MAC secret key	P_{50}	Accepted request
P_{26}	Authenticated ciphertext	P_{51}	Client is authenticated

Table 8.7. DEFINITIONS OF TRANSITIONS – THE MODIFIED TRUST MODEL WITH ADVERSARY

Trans.	Definition	Trans.	Definition
T_1	Compute login request	T_{19}	Receive A_1
T_2	Encrypt MSG	T_{20}	Shared transition that check the integrity of A_2
T_3	Compute MAC value and append it to the ciphertext	T_{21}	Decrypt C_2
T_4	Send authenticated ciphertext	T_{22}	Verify
		T_{23}	Drop the request
T_5	Intercept	T_{24}	Accept
T_6	Pass	T_{25}	Compute session key and ACK
T_7	Receive	T_{26}	Encrypt MSG
T_8	Shared transition that check the integrity of A_1	T_{27}	Compute MAC value and append append it to the ciphertext
T_9	Decrypt C_1	T_{28}	Transmit A_3
T_{10}	Verify	T_{29}	Intercept
T_{11}	Drop the request	T_{30}	Pass
T_{12}	Accept	T_{31}	Receive A_3
T_{13}	Compute SYN/ACK and session key	T_{32}	Shared transition that check the integrity of A_3
T_{14}	Encrypt MSG	T_{33}	Decrypt C_3
T_{15}	Compute MAC value and append it to the ciphertext	T_{34}	Verify
		T_{35}	Drop the request
T_{16}	Transmit A_1	T_{36}	Accept
T_{17}	Intercept	T_{37}	Authenticate
T_{18}	Pass		

By simulating the modified protocol in Figure 8.14, both the client and the server function exactly as the trust model discussed previously in section 8.4.1 and the adversary entity only passes the intercepted token via transitions T_6, T_{17}, T_{36}. Note that the adversary may listen to conversations between the client and the server but since the traffic between them is encrypted, it is hard for it to decrypt the ciphertext without knowing the corresponding decryption key. This proves the benefit gained from encrypting the traffic and how it creates a private channel between entities. The modified protocol will also detect any modification applied even if the adversary flips a bit in the ciphertext. Verifying the encrypted message using the authentication code allows the modified protocol to discard any illegitimate messages.

8.4.3 SECURITY ANALYSIS

The modified authentication and key agreement protocol is secure and improves several aspects. The analysis suggests that the modified protocol is well designed for data confidentiality by using symmetric cryptography during the handshake procedure. Also, it ensures data integrity by applying a Message Authentication Code function (MAC) to the ciphertext. Typically, both the client and the server transmit the MAC value during transmission. However, both the client and the server will be aware if an adversary alters the ciphertext because the integrity check of the MAC value will fail. Besides, when the communication session between C_i and S_i is over, the session key sk is discarded and a new session key is established in every protocol run. The modified protocol is aimed at initiating secure authentication and communication between the client and server by building a robust mechanism between communicating parties. The presented protocol may be described as a three-way handshake procedure to establish a reliable connection and ensure secure data sharing. Moreover, it shows resistance to various attacks as follows.

8.4.3.1 Resistance to impersonation attacks

It is extremely difficult for an attacker to mount a successful impersonation as a legitimate user or server. From the user side, the attacker cannot fabricate a feasible encrypted message $Enc\{ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3\}_a \,||\, MAC_k(ID_{C_i}, ID_{S_i}, T_{C_i}, W_1 M_2, M_3)$ without knowing the secret value of y in $H_4(ID_{C_i}||\, y)$. Similarly, the attacker cannot extract $e_i = H_4(ID_{C_i}||\, y) \oplus H_4(PW_{C_i}||\, f_i)$ from the central database without C_i's password and biometrics data. Therefore, if the attacker sends a fake login message, S_i will reject the request by the verification test of $H_4(ID_{C_i}\,||\, y)$ after the

decryption of the message $\{ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3\}_a \,||\, MAC_k(ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3)$. From the server side, the attacker cannot produce a feasible encrypted message $\{ID_{C_i}, ID_{S_i}, T_{S_i}, W_1, M_6, M_7 \,||\, MAC_k(ID_{C_i}, ID_{S_i}, T_{S_i}, W_1, M_6, M_7)\}$ without knowing the secret value of $H_4(ID_{C_i} || y)$ or the secret value of a or k. Therefore, if the attacker sends a fake authentication message to $\boldsymbol{C_i}$, the attack will be detected when $\boldsymbol{C_i}$ verifies the MAC value. Thus, the modified protocol is secure against impersonation attacks.

8.4.3.2 Resistance to man-in-the-middle attacks, reflection attacks, and parallel session attacks

The modified protocol provides mutual authentication with the key agreement protocol so both parties are assured of the other's identity. The modified protocol includes the identifier of the client (ID_C), as well as the identifier of the server (ID_S). Including both client and server identifiers in every message prevent attacks such as parallel session attacks.

Since the protocol is resistant to impersonation attack. The adversary cannot fabricate feasible messages without knowing the secret key for symmetric encryption or MAC secret key. Those secret keys are agreed on between C_i and $\boldsymbol{S_i}$ via a secure channel. If the adversary attempts to send a fake encrypted message, it will be detected by the verification of the MAC value. Thus, the modified protocol is secure against the man-in-the-middle attack, reflection attack, and parallel sessions attack.

8.4.3.3 Resistance to denial-of-service attacks

The modified version of the proposed protocol can withstand denial-of-service attack, because when the client C_i imprints the personal biometrics $Bio^*_{C_i}$, the S_i will check the validity of $Bio^*_{C_i}$ with stored template by checking whether $d(Bio_{C_i}, Bio^*_{C_i}) < \tau$ holds. According to Li *et al*. (2011) the $Bio^*_{C_i}$ could pass the verification process even though there is some slight difference between Bio_{C_i}, $Bio^*_{C_i}$.

Another way to tackle denial-of-service-attack is applying MAC to the ciphered message. When a ciphered message is received, the MAC is validated first before decrypting. This mechanism allows the source to discard invalid packets and determine if the packets truly correspond to the sent packets. This helps to filter the traffic and hinders any prior disruption to the target machine. Thus, this denies any spoofing illegitimate requests. Another advantage can be seen with appending the MAC to the ciphertext is to identify if an adversary has injected encrypted pieces of data in the original ciphertext and to be able to check the integrity of the transmitted data.

8.4.3.4 Resistance to replay attacks

In order to validate the authenticity of messages exchanged between C_i and S_i, the freshness of timestamps is constantly checked as to whether they are within an allowable time period or not. For example, the verification request will fail if $T' - T_{C_i} > \Delta T$. This will cause the session to be terminated. Also, both the client and the server generate a new random number and a timestamp for every new session. Even if an adversary intercepts the authenticated ciphertext, it cannot decrypt the

ciphertext since it does not know the secret key. Thus, he/she cannot forge a fake login message or use it later to launch a replay attack.

8.4.3.5 Resistance to passive attacks

Due to the difficulty in detecting passive attacks, the modified protocol is sufficient against eavesdropping and traffic analysis. Typically, encrypting the message traffic is sufficient to prevent the success of these attacks. Authenticating the ciphertext is a significant way to ensure integrity and authenticity.

8.4.3.6 Resistance to ciphertext attacks

There is crucial difference between encryption and authenticated encryption. Encryption alone does not guarantee the authenticity of the encrypted message or whether the message has been modified while in transit or storage. Relying only on encryption would compromise the integrity of data. Furthermore, symmetric key encryption is susceptible to known-plaintext attacks, chosen plaintext attacks, differential and linear cryptanalysis (Courtois *et al.*, 2008; Acton, 2013). The modified proposed protocol relies on the encrypt-then-authenticate approach, which can achieve the highest level of security in authenticated encryption (Krawczyk, 2001; Courtois *et al, 2008*). This approach can recognise improperly constructed ciphertext and prevent any attempts to gain an advantage against encrypted data. The client and the server check whether the message is authentic by validating the integrity of the encrypted message.

8.5 SUMMARY

This chapter started with modifying the protocol design by applying the encrypt-then-authenticate method. Then it explains the details of the finite-state verification of the modified protocol and identifies the functionality of each phase with the new enhancements. Also, it analyses the behaviour of each machine created for each phase and how they interrelate together. The composite model executes efficiently and handles errors in a safe way according to their types. The modified protocol connection progresses from one state to another based on the data obtained from the message exchanged. The use of EFSM helps to understand the behaviour of the protocol and logs unwanted behaviours. This mechanism is very useful for determining the types of errors the protocol experiences during running and these can be useful to retrospectively investigate what causes these errors and to learn from them.

Furthermore, the chapter deals with the simulation of the modified protocol. it describes the behaviour of the modified protocol using the Petri net formalism to verify and improve the protocol by employing encrypt-then-authenticate routine to the modified protocol. This proves that the modified protocol is resistant to man-in-the-middle attacks, reflection attacks, parallel session attacks, impersonation attacks, replay attacks and forgery attacks. The analysis shows that the modified protocol is efficient and provides secure communication over insecure channels. The identification of the requirement for these particular modifications was the result of the exhaustive analysis, which helps to determine any faults with the protocol.

Registratio	**Client C_i** (1) ID_{ci}, PW_{ci}, Bio_{ci},	(3) ID_{C_i}, $H_4(.)$, Enc{}a/Dec{ }a, $MAC_K(\ )$, f_i, e_i, τ, $Pr\_K_{C_i}$ ←	**Registration Centre R_i** (2) Computes: • $f_i = H_4(Bio_{ci})$ • $e_i = H_4(ID_{ci}\|\|y) \oplus H_4(PW_{Ci}\|\|f_i)$ • $Pr\_K_{ci} = (x + H_4(ID_{c_i}))^{-1}.P$
Login	**Client C_i** (2) Enters ID'_{C_i} and PW'_{C_i} (3) Inputs Bio'_{C_i} (5) Computes: • $z'_i = H_4(PW_{C_i}\|\|f_i)$ • $M_1 = e_i \oplus z'_i$ • $W_1 = r_{C_i} . P$ • $M_2 = r_{C_i} . Pr\_K_{C_i}$ • $M_3 = M_1 \oplus r_{ci}$ (6) $C_1 = Enc\{ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3\}_a$ (7) $mac_1 = MAC_k(ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3)$	(8) $A_1 = C_1 \|\| mac_1$ →	**Server S_i** (2)Verifies the authenticity of ID'_{C_i} and PW'_{C_i} (4) Verifies Accept if $d(Bio_{C_i}, Bio^*_{C_i}) < \tau$ Reject if $d(Bio_{C_i}, Bio^*_{C_i}) \geq \tau$
Authentication	**Client C_i** (8) Checks the integrity of $A_2 = C_2 \|\| mac_2$ (9) Decrypts C_2, then checks validity of ID_{S_i} and freshness of T_{S_i} (10) Verifies $M_7 ?= H_4(M_4\|\|r_{C_i})$ ***Server S_i is authenticated*** (11) Computes: • $K_{C_i} = r_{C_i} . W_2$ • $Sk = H_3(ID_{C_i}, T_{C_i}, T_{S_i}, W_1, W_2, K_{C_i})$ • $M_8 = M_6 \oplus M_1 = r_{S_i}$ • $M_9 = H_4(M_6\|\|M_8)$ (12) $C_3 = Enc\{ID_{C_i}, ID_{S_i}, T_{C_i}, M_9\}_a$ (13) $mac_3 = MAC_k(ID_{C_i}, ID_{S_i}, T_{C_i}, M_9)$	(7) $A_2 = C_2 \|\| mac_2$ ← (14) $A_3 = C_3 \|\| mac_3$ →	**Server S_i** (1) Checks the integrity of $A_1 = C_1 \|\| mac_1$ (2) Decrypts C_1, then checks validity of ID_{c_i} and freshness of T_{c_i} (3) Computes and verifie: $M`_2 = (x + H_1(ID_{C_i})^{-1}. W_1$ $= Pr\_K_{C_i} . r_{C_i} = M_2$ (4) Computes: • $M_4 = H_4(ID_{C_i}\|\|y)$ • $W_2 = r_{S_i} . P$ • $K_{S_i} = r_{S_i} . W_1$ • $Sk = H_3(ID_{C_i}, T_{C_i}, T_{S_i} W_1, W_2, K_{S_i})$ • $M_5 = M_3 \oplus M_4 = r_{C_i}$ • $M_6 = M_4 \oplus r_{S_i}$ • $M_7 = H_4(M_3\|\|M_5)$ (5) $C_2 = Enc\{ID_{C_i}, ID_{S_i}, T_{S_i}, W_2, M_6, M_7\}_a$ (6) $mac_2 = MAC_k(ID_{C_i}, ID_{S_i}, T_{S_i}, W_2, M_6, M_7)$ (15) Checks the integrity of $A_3 = C_3 \|\| mac_3$ (16) Decrypts C_3, then checks validity of ID_{C_i} and freshness of T_{C_i} (17) Verifies $M_9 ?= H_4(M_6 \oplus r_{S_i})$ ***Client C_i is authenticated***

Protocol 8.1: The modified protocol

9

Conclusions, Limitations and Future Works

9.1 Conclusions

Organisations globally look for strong authentication solutions because maintaining a robust level of security and adequate efficiency are considered a long-term investment. Authentication can be accomplished in different ways but it is important to choose an appropriate environment and methods. This thesis offers a unique authentication protocol that uses a variety of cryptographic mechanisms to secure the authentication process and to securely establish a protected channel and key exchange. The main contribution of this thesis is the development of an authentication protocol that integrates two-factor authentication, which requires two distinctive forms of identification when validating a client. The security of the

proposed protocol is increased by including something the client physically has (biometric data, in this case) and something the client knows (password). As a result, the authentication process is not susceptible to password guessing and password attacks. The scope of the thesis has been carefully crafted to develop a robust security protocol that fulfils the following:

1. Mutual authentication between the client and the server via a three-way handshake over Elliptic Curve Cryptography (ECC).
2. Freshness is always assured by random numbers and timestamps.
3. The integrity and secrecy of the protocol accomplished via the encrypt-then-authenticate method.

Cryptography can be thought of as an art, which requires researchers and developers to mix and combine various techniques and methods in order to secure protocols. This thesis combines the results of two schemes as a foundation to derive a multifactor authentication protocol. It focuses comprehensively on answering the question of whether these schemes provide secure communications. Unfortunately, the result of combination does not completely guarantee confidentiality, integrity and authenticity and it is found to be vulnerable to attacks. One of the flaws found is the risk of eavesdropping, which can be damaging. To avoid this, a symmetric encryption is applied to provide secrecy. However, encryption alone does not provide integrity for the ciphertext: an adversary can flip a bit in the encrypted message and transmit the modified ciphertext. For this reason, message authentication is used to ensure ciphertext integrity. As a result, the composition of encryption and authentication provides truly secure communication when is

embedded in the modified protocol; both secrecy and integrity are achieved. Protocol 9.1 summaries the messages flow for the proposed protocol.

Protocol 9.1: Summary of the message flow and contents between the client C and server S

Protocol step	Message flow	Message contents
1	C → S	$\mathrm{Enc}\{ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3\}_a \,||\, MAC_k(\{ID_{C_i}, ID_{S_i}, T_{C_i}, W_1, M_2, M_3\}_a)$
2	S→ C	$\mathrm{Enc}\{ID_{C_i}, ID_{S_i}, T_{S_i}, W_2, M_6, M_7\}_a \,||\, MAC_k(\{ID_{C_i}, T_{S_i}, W_2, M_6, M_7\}_a)$
3	C → S	$\mathrm{Enc}\{ID_{C_i}, ID_{S_i}, T_{C_i}\, M_9\}_a \,||\, MAC_k(\{ID_{C_i}, ID_{S_i}, T_{C_i}\, M_9\}_a)$

The existence of design weaknesses or implementation errors can lead to unexpected and undesirable events, compromising system security. Therefore, the Finite State Machine analysis is used to provide a mechanism for error detection and error reporting. In addition, Petri nets are used to ensure the soundness of the protocol analysis. This approach is a very useful tool for modelling and simulating a range of possible attacks on the proposed protocol. The key features of using Petri nets can be summarised as follows:

1. The ability to model the concurrency of the protocol progress with tokens.
2. The ability to model intermediate and final objectives as places.
3. The ability to model transitions as commands and inputs.

Adding an adversary to the model encourages discovery and discussion of scenarios where the system is under malicious attack. The range of attacks tests the behaviour of the protocol while validating it with PN. It reveals the necessity to provide the

server ID to prevent attacks such as reflection attack while maintaining secrecy of the traffic between the client and server. Chapter 6 answers one of the questions raised in Chapter 4 that the authenticate-then-encrypt method is not a very secure approach. Section 7.5 shows that the adversary still has the ability to freely manipulate ciphertexts even when assuming that the symmetric key encryption is a well secured scheme and that the MAC is strongly unforgeable. It is also noted in the analysis that the server spends extra time to deal with decryption first then to validate the MAC value. Chapter 8 demonstrates the modifications needed to improve the proposed protocol. FSM was used once again to evaluate the desired functionalities and behaviour while PN was used to test whether the modified protocol satisfies the security requirements. The modified protocol is proven to be resilient to various attacks and it sustains a good balance between security and efficiency (Table 9.1).

Table 9.1: Summary of security analysis

Security Factors	The new Protocol	Mechanism
Multifactor authentication	Yes	Biometric, sender and recipient's IDs are presented
Session key agreement	Yes	Based on ECC
Man-in-the-middle attack resistance	Yes	Symmetric encryption
Replay attack resistance	Yes	Random numbers and timestamps
Reflection attack resistance	Yes	Symmetric encryption and ID
Parallel session attack resistance	Yes	Symmetric encryption
Impersonation attack resistance	Yes	
Forgery attack resistance	Yes	Secret value
Ciphertext attack resistance	Yes	Encrypt-then-authenticate

In light of this, this thesis makes the argument that authentication based on biometric and ID-based cryptography offers a competitive authentication practice with the strongly desirable properties of confidentiality, integrity and authenticity (Table 9.2).

Table 9.2: Summary of the relationship between the protocol security services and mechanisms

Services	Mechanism			
	Encryption	**MAC**	**Data integrity**	**Authentication exchanged**
Entity authentication	Yes	Yes		Yes
Data origin authentication	Yes	Yes		
Confidentiality	Yes			
Traffic flow confidentiality	Yes			
Data integrity	Yes	Yes	Yes	
Nonrepudiation		Yes	Yes	

9.2 LIMITATIONS

There were some unavoidable limitations due to the time limit. First, an extensive study needs to be conducted during the handshake. The protocol may be suspected to SYN flood. This attack leads to DoS or DDoS attack and it take place when multiple external hosts start but do not finish the three way handshake, exhausting the system with a half open connection network queue. These attacks can be mitigated by adopting approaches like SYN cache and SYN cookies to prevent this issue.

Second, An in-depth analysis should to be conducted on the performance evaluation. The performance of the protocol can be evaluated in two aspects: security strength and the cost of computation. Theoretically, the computation cost for the protocol is relatively low and efficient due to utilising fast operations such as symmetric encryption, hash operations and XOR operations. Also, having the protocol based on ECC adds another advantage in terms of fast performance and reliable security. Then, the result of the performance test needs to be compared with current similar protocols to measure efficiency and performance.

Finally, biometric authentications are based on probabilistic measures. Characteristically, the process of authentication depends on the decision of confidence scores, which are in the range between 0% and 100%. The performance of biometric systems is highly sensitive and it can be significantly affected by change in the acquisition of biometrics, for example, due to skin damage or injury. Consequently, using hash functions to protect biometric data might not be the best solution because any slight change that occurs during acquisition of the biometric data can produce a different hash value. Therefore, it was challenging to find a suitable lightweight algorithm that handles biometric data accurately and achieves the revocability property within the time limit of the research.

9.3 FUTURE WORK

In the future, it will be more efficient and practical to investigate the new protocol in multi-server environments and with multi-clients such that it can be applied to more applications in electronic government. The most straightforward way to simulate and validate this approach is using coloured Petri net (CPN). The reason behind

considering CPN over PN is that each client and server can be assigned a unique colour, making the evaluation processes easier and more efficient (Al-zzoni *et al.,* 2005). CPN is a high-level nets that are widely used for many different practical purposes. One of the reasons for the large success for CPN is that they allow more succinct and manageable descriptions without loosing the possibility of formal analysis (Jensen and Kristensen, 2009).

Another area worth investigating is securing the biometric templates since they are prone to vulnerabilities such as circumvention, covert acquisition, collusion and coercion, denial of Service, and repudiation (Maltoni *et al*., 2009).

Another potential possibility for future work involves chaotic systems (Dachselt *et al*., 2001; Kocarev *et al*., 2001) and developing a novel key agreement protocol based on chaotic maps and ID-based encryption. Chaotic systems have been used to design secure communication protocols (Pecora and Carroll, 1990; Dachselt *et al*., 2001; Kocarev *et al*., 2001; Wong 2002)

Finally, perhaps the most interesting area for future work involves utilising biometric data as the identity of the client instead of using the ID of the user. Then applying this change to the proposed protocol in this thesis. This transition would produce a fuzzy protocol similar to the work of researchers such as Sahai *et al.* (2005), Dodis *et al*. (2006), Beak *et al*. (2007), or Scheirer *et al*. (2007).

To conclude, this thesis demonstrates a new authentication protocol based on biometric and ID-based cryptography over ECC. The new protocol has been thoroughly validated and formally verified via formal approaches. One of the new protocol merits is to provide a solid structure that one can implement stronger defence mechanisms. For example, the MAC mechanism used in the protocol can be

replaced by a stronger one such as HMAC-SHA-1 depending on the desired security level. The same goes for symmetric encryption and one-way hash functions. Besides other advantages such as secure mutual authentication and key agreement, this protocol can be successfully implemented in distributed systems such as e-Government and it can facilitate secure authentication.

Bibliography

- ABIDIN, A., MATSUURA, K. and MITROKOTSA, A., 2014. Security of a Privacy-Preserving Biometric Authentication Protocol Revisited. *Cryptology and Network Security.* Springer, pp. 290-304.
- ABRAHAM, A., MAURI, J.L., BUFORD, J., SUZUKI, J. and THAMPI, S.M., 2011. *Advances in Computing and Communications, Part I: First International Conference, ACC 2011, Kochi, India, July 22-24, 2011. Proceedings.* Springer Science & Business Media.
- ACTON, Q.A., 2013. *Algorithms—Advances in Research and Application: 2013 Edition* ScholarlyEditions.
- ACTON, Q.A., 2013. *Algorithms—Advances in Research and Application.* ScholarlyEditions.
- AL-AZZONI, I., DOWN, D.G. and KHEDRI, R., 2005. Modelling and verification of cryptographic protocols using coloured petri nets and design/CPN. *Nordic Journal of Computing,* **12**(3), pp. 201.
- AL-RIYAMI, S. and PATERSON, K., 2003. Certificateless public key cryptography. *Advances in Cryptology-ASIACRYPT 2003,* , pp. 452-473.
- ALAGAR, V.S., 2011. *Specification of software systems.* 2nd edn. England: Springer.
- ALJEAID, D., MA, X. and LANGENSIEPEN, C., 2014. Biometric identity-based cryptography for e-Government environment, *Science and Information Conference (SAI), 2014* 2014, IEEE, pp. 581-588.
- ALJEAID, D., MA, X. and LANGENSIEPEN, C., Modelling and Simulation of a Biometric Identity-Based Cryptography. *International Journal of Advanced Research in Artificial Intelligence (IJARAI),* **3**(10),.
- AMBALAKAT, P., 2005. Security of biometric authentication systems, *Computer Science Seminar, Rensselaer at Hartford* 2005.
- ANDERSON, R., 2008. *Security engineering: a guide to building dependable distributed systems.* 2nd edn. Hoboken, N.J.; Chichester: Wiley; John Wiley distributor.
- ANDERSON, R.J., 2010. *Security Engineering: A guide to building dependable distributed systems.* Wiley.
- ANDRESS, J., 2014. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice.* Syngress.
- ANDROUTSOPOULOS, K., CLARK, D., HARMAN, M., LI, Z. and TRATT, L., 2009. Control dependence for extended finite state machines. *Fundamental Approaches to Software Engineering.* Springer, pp. 216-230.
- BAEK, J., SUSILO, W. and ZHOU, J., 2007. New constructions of fuzzy identity-based encryption, *Proceedings of the 2nd ACM symposium on Information, computer and communications security* 2007, ACM, pp. 368-370.
- BALLAD, B., BALLAD, T. and BANKS, E., 2010. *Access control, authentication, and public key infrastructure.* Jones & Bartlett Publishers.

- BASAGIANNIS, S., KATSAROS, P. and POMBORTSIS, A., 2007. Intrusion attack tactics for the model checking of e-commerce security guarantees. *Computer Safety, Reliability, and Security.* Springer, pp. 238-251.
- BELLARE, M., NAMPREMPRE, C. and NEVEN, G., 2009. Security proofs for identity-based identification and signature schemes. *Journal of Cryptology,* **22**(1), pp. 1-61.
- BENNETT, S., MCROBB, S. and FARMER, R., 2006. *Object-oriented systems analysis and design using UML.* McGraw-Hill Berkshire, UK.
- BIRD, R., GOPAL, I., HERZBERG, A., JANSON, P., KUTTEN, S., MOLVA, R. and YUNG, M., 1993. Systematic design of a family of attack-resistant authentication protocols. *Selected Areas in Communications, IEEE Journal on,* **11**(5), pp. 679-693.
- BISSESSAR, D., ADAMS, C. and STOIANOV, A., 2016. Privacy, Security and Convenience: Biometric Encryption for Smartphone-Based Electronic Travel Documents. *Recent Advances in Computational Intelligence in Defense and Security.* Springer, pp. 339-366.
- BOBBIO, A., 1990. System modelling with Petri nets. *Systems reliability assessment.* Springer, pp. 103-143.
- BONEH, D. and BOYEN, X., 2004. Efficient selective-ID secure identity-based encryption without random oracles, *Advances in Cryptology-EUROCRYPT 2004* 2004, Springer, pp. 223-238.
- BONEH, D. and FRANKLIN, M., 2001. Identity-based encryption from the Weil pairing, *Advances in Cryptology—CRYPTO 2001* 2001, Springer, pp. 213-229.
- BONEH, D., BOYEN, X. and GOH, E.J., 2005. Hierarchical identity based encryption with constant size ciphertext. *Advances in Cryptology–EUROCRYPT 2005,* , pp. 440-456.
- BOYD, C. and MATHURIA, A., 2003. *Protocols for authentication and key establishment.* Springer Science & Business Media.
- BOYEN, X. and WATERS, B., 2006. Anonymous hierarchical identity-based encryption (without random oracles). *Advances in Cryptology-CRYPTO 2006,* , pp. 290-307.
- BOYEN, X., DODIS, Y., KATZ, J., OSTROVSKY, R. and SMITH, A., 2005. Secure remote authentication using biometric data. *Advances in Cryptology–EUROCRYPT 2005,* , pp. 561-561.
- BUCHMANN, J.A., KARATSIOLIS, E. and WIESMAIER, A., 2013. *Introduction to public key infrastructures.* Springer Science & Business Media.
- BURNETT, A., BYRNE, F., DOWLING, T. and DUFFY, A., 2007. A biometric identity based signature scheme. *International Journal of Network Security,* **5**(3), pp. 317-326.
- BURROWS, M., ABADI, M. and NEEDHAM, R.M., 1989. A logic of authentication. *Proceedings of the Royal Society of London.A.Mathematical and Physical Sciences,* **426**(1871), pp. 233-271.
- CAKULEV, V. and SUNDARAM, G., 2012. IBAKE: Identity-Based Authenticated Key Exchange.
- CALOYANNIDES, M., COPELAND, D.R., DATESMAN, G.H. and WEITZEL, D.S., 2003. US e-government authentication framework and programs. *IT professional,* , pp. 16-21.
- Chang Y-F, Chang C-C, Su Y-W. A secure improvement on the user-friendly remote authentication scheme with no time concurrency mechanism. In: Proceedings of 20th

international conference on advanced information networking and applications, IEEE CS, 2006

- CHANG, Y., CHANG, C. and SU, Y., 2006. A secure improvement on the user-friendly remote authentication scheme with no time concurrency mechanism, *Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on* 2006, IEEE, pp. 5 pp.
- CHAPPLE, M., BALLAD, B., BALLAD, T. and BANKS, E., 2013. *Access Control, Authentication, and Public Key Infrastructure.* Jones and Bartlett Publishers, Inc.
- CHARLES, P. and PFLEEGER, S.L., 2012. *Analyzing Computer Security: A Threat/vulnerability/countermeasure Approach.* Prentice Hall.
- CHIOLA, G. and FERSCHA, A., 1993. Distributed simulation of Petri nets. *IEEE Concurrency,* **1**(3), pp. 33-50.
- CLARK, J.A. and JACOB, J.L., 1997. A survey of authentication protocol literature: Version 1.0.
- CONRAD, E., MISENAR, S. and FELDMAN, J., 2012. *CISSP study guide.* Newnes.
- COURTOIS, N., NOHL, K. and O'NEIL, S., 2008. Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. *IACR Cryptology ePrint Archive*, pp. 166.
- DEBIAO, H., JIANHUA, C. and JIN, H., 2012. An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security. *Information Fusion,***13**(3), pp. 223-230.
- DENNING, D.E. and SACCO, G.M., 1981. Timestamps in key distribution protocols. *Communications of the ACM,* **24**(8), pp. 533-536.
- DI COSTANZO, R.E. and CHIRINOS, L., 2014. A NOVEL METHODOLOGY TO DESIGN SECURITY PROTOCOLS BASED ON A NEW SET OF DESIGN PRINCIPLES. *European Scientific Journal,* **10**(3),.
- DI COSTANZO, R.E. and CHIRINOS, L., 2014. A NOVEL METHODOLOGY TO DESIGN SECURITY PROTOCOLS BASED ON A NEW SET OF DESIGN PRINCIPLES.*European Scientific Journal,* **10**(3),.
- DIAZ, M., 2013. *Petri nets: fundamental models, verification and applications.* John Wiley & Sons.
- DIFFIE, W., GILMORE, J., NEUMANN, P.G., RIVEST, R.L. and SCHILLER, J.I., 1997. The risks of key recovery, key escrow, and trusted third-party encryption. *World Wide Web Journal,* **2**(3), pp. 241-257.
- DODIS, Y., KATZ, J., REYZIN, L. and SMITH, A., 2006. Robust fuzzy extractors and authenticated key agreement from close secrets. *Advances in Cryptology-CRYPTO 2006,* , pp. 232-250.
- DODIS, Y., OSTROVSKY, R., REYZIN, L. and SMITH, A., 2006. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *Arxiv preprint cs/0602007,* .
- DODIS, Y., REYZIN, L. and SMITH, A., 2004. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, *Advances in cryptology-Eurocrypt 2004* 2004, Springer, pp. 523-540.
- DONG, L. and CHEN, K., 2012. Automated Analysis of Cryptographic Protocols Based on Trusted Freshness. *Cryptographic Protocol.* Springer, pp. 341-369.
- DRAHANSKÝ, M., 2011. Liveness Detection in Biometrics. *Advanced Biometric Technologies}*, pp. 179-198.

- DRESP, W., 2005. Security analysis of the secure authentication protocol by means of coloured petri nets, *Communications and Multimedia Security* 2005, Springer, pp. 230-239.
- DUFFY, A. and DOWLING, T., 2004. An object oriented approach to an identity based encryption cryptosystem, *Software Engineering and Applications* 2004, ACTA Press.
- EVANS, D. and YEN, D.C., 2005. E-government: An analysis for implementation: Framework for understanding cultural and social impact. *Government Information Quarterly,* **22**(3), pp. 354-373.
- FELDHOFER, M. and RECHBERGER, C., 2006. A case against currently used hash functions in RFID protocols, *On the move to meaningful internet systems 2006: OTM 2006 workshops* 2006, Springer, pp. 372-381.
- FENG, H. and WAH, C.C., 2002. Private key generation from on-line handwritten signatures. *Information Management & Computer Security,* **10**(4), pp. 159-164.
- GALINDO, D., HERRANZ, J. and KILTZ, E., 2006. On the generic construction of identity-based signatures with additional properties. *Advances in Cryptology–ASIACRYPT 2006,* , pp. 178-193.
- GENTER, G., BOGDAN, S., KOVACIC, Z. and GRUBISIC, I., 2007. Software tool for modeling, simulation and real-time implementation of Petri net-based supervisors, *Control Applications, 2007. CCA 2007. IEEE International Conference on* 2007, IEEE, pp. 664-669.
- GENTRY, C. and SILVERBERG, A., 2002. Hierarchical ID-based cryptography. *Advances in Cryptology—ASIACRYPT 2002,* , pp. 149-155.
- GIBSON, D., 2012. *CISSP Rapid Review.* Pearson Education.
- GIRIDHAR, A. and KUMAR, P., 2006. Distributed clock synchronization over wireless networks: Algorithms and analysis, *Decision and Control, 2006 45th IEEE Conference on* 2006, IEEE, pp. 4915-4920.
- GOH, A. and NGO, D., 2003. Computation of cryptographic keys from face biometrics. *Communications and Multimedia Security Advanced Techniques for Network and Data Protection,* , pp. 1-13.
- GONG, L., NEEDHAM, R. and YAHALOM, R., 1990. Reasoning about belief in cryptographic protocols, *Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on*1990, IEEE, pp. 234-248.
- GREGG, M., 2014. *Certified Ethical Hacker (CEH) Cert Guide.* Pearson IT Certification.
- GRÖNLUND, Å. and HORAN, T.A., 2005. Introducing e-gov: history, definitions, and issues. *Communications of the Association for Information Systems,* **15**(1), pp. 39.
- GUILLOU, L. and QUISQUATER, J.J., 1990. A "paradoxical" identity-based signature scheme resulting from zero-knowledge, *Advances in Cryptology—Crypto'88* 1990, Springer, pp. 216-231.
- GUPTA, V., GUPTA, S., CHANG, S. and STEBILA, D., 2002. Performance analysis of elliptic curve cryptography for SSL, *Proceedings of the 1st ACM workshop on Wireless security* 2002, ACM, pp. 87-94.
- GURTOV, A., 2008. *Host Identity Protocol (HIP): Towards the Secure Mobile Internet.* Wiley.
- HAN, J. and JEONG, D., 2010. A practical implementation of IEEE 1588-2008 transparent clock for distributed measurement and control systems. *Instrumentation and Measurement, IEEE Transactions on,* **59**(2), pp. 433-439.

- HAO, F., ANDERSON, R. and DAUGMAN, J., 2005. Combining cryptography with biometrics effectively. *University of Cambridge Computer Laboratory, Tech.Rep*.
- HEEKS, R., 2002. e-Government in Africa: Promise and practice. *Information Polity,* **7**(2), pp. 97-114.
- HERRANZ, J., 2007. Identity-based ring signatures from RSA. *Theoretical Computer Science,* **389**(1-2), pp. 100-117.
- HONG, S., SHIN, J., LEE-KWANG, H. and YOON, H., 1998. A new approach to server-aided secret computation. *ICISC* 1998, Citeseer, pp. 33-45.
- HOPCROFT, J.E., Je rey D. Ullman. 1979. Introduction to automata theory, languages, and computation.
- HORWITZ, J. and LYNN, B., 2002. Toward hierarchical identity-based encryption, *Advances in Cryptology—EUROCRYPT 2002* 2002, Springer, pp. 466-481.
- HWANG, M., LEE, C. and TANG, Y., 2002. A simple remote user authentication scheme. *Mathematical and Computer Modelling,* **36**(1), pp. 103-107.
- INUMA, M., OTSUKA, A. and IMAI, H., 2009. Theoretical framework for constructing matching algorithms in biometric authentication systems. *Advances in Biometrics*. Springer, pp. 806-815.
- ISLAM, S.H. and BISWAS, G., 2012. An improved ID-based client authentication with key agreement scheme on ECC for mobile client-server environments. *Theoretical and Applied Informatics,* **24**(4), pp. 293-312.
- J. Lopez, R. Roman, I. Agudo et al., "Trust Management System for Wireless Sensor Networks:Best Practise," Computer Communications, 2010.
- JAEGER, P.T. and THOMPSON, K.M., 2003. E-government around the world: lessons, challenges, and future directions. *Government Information Quarterly,* **20**(4), pp. 389-394.
- JAHANKHANI, H., WATSON, D.L., ME, G. and LEONHARDT, F., 2010. *Handbook of electronic security and digital forensics.* World Scientific.
- JAIN, A.K., NANDAKUMAR, K. and NAGAR, A., 2008. Biometric template security. *EURASIP Journal on Advances in Signal Processing,* **2008**, pp. 113.
- JAIN, A.K., ROSS, A. and PANKANTI, S., 2006. Biometrics: a tool for information security. *Information Forensics and Security, IEEE Transactions on,* **1**(2), pp. 125-143.
- JAIN, A.K., ROSS, A. and ULUDAG, U., 2005. Biometric template security: Challenges and solutions, *Proceedings of European Signal Processing Conference* 2005, pp. 1-4.
- JAIN, R. and KANT, C., 2015. Attacks on Biometric Systems: An Overview. *International Journal of Advances in Scientific Research,* **1**(7), pp. 283-288.
- JENSEN, K. and KRISTENSEN, L.M., 2009. *Coloured Petri nets: modelling and validation of concurrent systems.* Springer Science & Business Media.
- JEON, S., KIM, H. and KIM, M., 2011. Enhanced biometrics-based remote user authentication scheme using smart cards. *J.of Security Engineering,* **8**(2), pp. 237-254.
- JIN, A.T.B. and HUI, L.M., 2010. Cancelable biometrics. *Scholarpedia,* **5**(1), pp. 9201.
- JOONSANG BAEK, QUANG HIEU VU, LIU, J.K., XINYI HUANG and YANG XIANG, 2015. A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid.*Cloud Computing, IEEE Transactions on,* **3**(2), pp. 233-244.
- JOYE, M., MUKHOPADHYAY, D. and TUNSTALL, M., 2011. *Security Aspects in Information Technology: First International Conference, InfoSecHiComNet 2011, Haldia, India, October 19-22, 2011. Proceedings.* Springer.
- KAHATE, A., 2013. *Cryptography and network security.* Tata McGraw-Hill Education.

- KATZ, J. and LINDELL, Y., Introduction to Modern Cryptography 2007.
- KELMAN, I., 2006. Warning for the 26 December 2004 tsunamis. *Disaster Prevention and Management,* **15**(1), pp. 178-189.
- KISEL, A., KOCHETKOV, A. and KRANAUSKAS, J., 2008. Fingerprint minutiae matching without global alignment using local structures. *Informatica,* **19**(1), pp. 31-44.
- KODAMA, K., MABUCHI, K. and SHIGEMATSU, I., 1996. A long-term cohort study of the atomic-bomb survivors. *Journal of epidemiology / Japan Epidemiological Association,* **6**(3 Suppl), pp. S95-105.
- KONSTANTINOU, E., NASTOU, P.E., STAMATIOU, Y.C. and ZAROLIAGIS, C., 2013. Securing Embedded Computing Systems through Elliptic Curve Cryptography. *Embedded Computing Systems: Applications, Optimization, and Advanced Design: Applications, Optimization, and Advanced Design,* , pp. 402.
- KRAWCZYK, H., 2001. The order of encryption and authentication for protecting communications (or: How secure is SSL?), *Advances in Cryptology—CRYPTO 2001* 2001, Springer, pp. 310-331.
- KRISHNA, P.V., BABU, M.R. and ARIWA, E., 2012. *Global Trends in Computing and Communication Systems: 4th International Conference, ObCom 2011, Vellore, TN, India, December 9-11, 2011, Part I. Proceedings.* Springer.
- KUMAR, K.P., SHAILAJA, G. and SAXENA, A., 2006. *Secure and efficient threshold key issuing protocol for ID-based cryptosystems*.
- LARMAN, C., 2002. *Applying UML and patterns: an introduction to object-oriented analysis and design and the unified process.* Prentice Hall.
- LAUTER, K., 2004. The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless communications,* **11**(1), pp. 62-67.
- LEE, B., BOYD, C., DAWSON, E., KIM, K., YANG, J. and YOO, S., 2004. Secure key issuing in ID-based cryptography, *Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation-Volume 32* 2004, Australian Computer Society, Inc., pp. 69-74.
- LEE, D. and YANNAKAKIS, M., 1996. Principles and methods of testing finite state machines-a survey. *Proceedings of the IEEE,* **84**(8), pp. 1090-1123.
- LEE, N. and CHIU, Y., 2005. Improved remote authentication scheme with smart card. *Computer Standards & Interfaces,* **27**(2), pp. 177-180.
- LI, C.T. and HWANG, M.S., 2010. An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications,* **33**(1), pp. 1-5.
- LI, J., LI, J., CHEN, X., JIA, C. and LOU, W., 2015. Identity-based encryption with outsourced revocation in cloud computing. *Computers, IEEE Transactions on,* **64**(2), pp. 425-437.
- LI, X., NIU, J., MA, J., WANG, W. and LIU, C., 2011. Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications,* **34**(1), pp. 73-79.
- LIAO, J., XIAO, J., QI, Y., HUANG, P. and RONG, M., 2005. ID-based signature scheme without trusted PKG, *Information Security and Cryptology* 2005, Springer, pp. 53-62.
- LIM, H.W. and PATERSON, K.G., 2011. Identity-based cryptography for grid security. *International Journal of Information Security,* **10**(1), pp. 15-32.
- LIN, C. and LAI, Y., 2004. A flexible biometrics remote user authentication scheme. *Computer Standards & Interfaces,* **27**(1), pp. 19-23.

- LU, J., ZHANG, S. and QIE, S., 2011. Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards. *IACR Cryptology ePrint Archive,* **2011**, pp. 676.
- LUMINI, A. and NANNI, L., 2007. An improved BioHashing for human authentication. *Pattern Recognition,* **40**(3), pp. 1057-1065.
- MALTONI, D., MAIO, D., JAIN, A.K. and PRABHAKAR, S., 2009. *Handbook of fingerprint recognition.* Springer Science & Business Media.
- MAO, W. and BOYD, C., 1993. Towards formal analysis of security protocols, *Computer Security Foundations Workshop VI, 1993. Proceedings* 1993, IEEE, pp. 147-158.
- MAO, W., 2004. *Modern cryptography: theory and practice.* Upper Saddle River, N.J.: Prentice Hall PTR.
- MARCHE, S. and MCNIVEN, J.D., 2003. E-Government and E-Governance: The Future Isn't What It Used To Be. *Canadian Journal of Administrative Sciences/Revue Canadienne des Sciences de l'Administration,* **20**(1), pp. 74-86.
- MARTIN, L., 2008. Identity-based encryption and beyond. *Security & Privacy, IEEE,* **6**(5), pp. 62-64.
- MARTIN, L., 2008. Identity-based encryption comes of age. *Computer,* **41**(8), pp. 93-95.
- MEADOWS, C., 1996. The NRL protocol analyzer: An overview. *The Journal of Logic Programming,* **26**(2), pp. 113-131.
- MEADOWS, C.A., 1995. *Formal verification of cryptographic protocols: A survey.* Springer.
- MENEZES, A.J., VAN OORSCHOT, P.C. and VANSTONE, S.A., 2010. *Handbook of applied cryptography.* CRC press.
- MILLS, D.L., 1991. Internet time synchronization: the network time protocol. *Communications, IEEE Transactions on,* **39**(10), pp. 1482-1493.
- MISHRA, D. and MUKHOPADHYAY, S., 2013. A certificateless authenticated key agreement protocol for digital rights management system. *Quality, Reliability, Security and Robustness in Heterogeneous Networks.* Springer, pp. 568-577.
- MONROSE, F., REITER, M.K., LI, Q. and WETZEL, S., 2001. Cryptographic key generation from voice, *Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on* 2001, IEEE, pp. 202-213.
- NEEDHAM, R.M. and SCHROEDER, M.D., 1978. Using encryption for authentication in large networks of computers. *Communications of the ACM,* **21**(12), pp. 993-999.
- NICANFAR, H., JOKAR, P., BEZNOSOV, K. and LEUNG, V., 2014. Efficient authentication and key management mechanisms for smart grid communications. *Systems Journal, IEEE,* **8**(2), pp. 629-640.
- NIEH, B.B. and TAVARES, S.E., 1993. Modelling and analyzing cryptographic protocols using Petri Nets, *Advances in Cryptology—AUSCRYPT'92* 1993, Springer, pp. 275-295.
- OBAIDAT, M.S., 2007. *Security of e-systems and computer networks.* Cambridge: Cambridge University Press.
- OKOT-UMA, R.W.O. and LONDON, C.S., 2000. Electronic governance: re-inventing good governance. *Commonwealth Secretariat, London,* **5**.
- PACHGHARE, V., 2015. *Cryptography and information security.* 2 edn. PHI Learning Pvt. Ltd.

- PATERSON, K.G. and PRICE, G., 2003. A comparison between traditional public key infrastructures and identity-based cryptography. *Information Security Technical Report,* **8**(3), pp. 57-72.
- PECORA, L.M. and CARROLL, T.L., 1990. Synchronization in chaotic systems. *Physical Review Letters,* **64**(8), pp. 821.
- PERMPOONTANALARP, Y. and SORNKHOM, P., 2009. A new Coloured Petri net methodology for the security analysis of cryptographic protocols, *Proceedings of the 10th Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools, Aarhus, Denmark* 2009.
- PTOLEMAEUS, C., 2014. *System Design, Modeling, and Simulation: Using Ptolemy II.* Ptolemy. org.
- RAMKUMAR, M., 2014. *Symmetric Cryptographic Protocols.* Springer.
- RATHA, N., CONNELL, J., BOLLE, R.M. and CHIKKERUR, S., 2006. Cancelable biometrics: A case study in fingerprints, *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on* 2006, IEEE, pp. 370-373.
- RATHA, N.K., CHIKKERUR, S., CONNELL, J.H. and BOLLE, R.M., 2007. Generating cancelable fingerprint templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* **29**(4), pp. 561-572.
- RATHA, N.K., CONNELL, J.H. and BOLLE, R.M., 2001. An analysis of minutiae matching strength, *Audio-and Video-Based Biometric Person Authentication* 2001, Springer, pp. 223-228.
- RATHA, N.K., CONNELL, J.H. and BOLLE, R.M., 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal,* **40**(3), pp. 614-634.
- RISTIC, I., 2014. *Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications.* Feisty Duck.
- RODRÍGUEZ, H., DÍAZ, W. and AGUIRRE, B.E., 2004. Communicating risk and warnings: an integrated and interdisciplinary research approach.
- ROGERS, D. and TSIRKUNOV, V., Implementing Hazard Early Warning Systems.
- RYAN, P. and SCHNEIDER, S.A., 2001. *The modelling and analysis of security protocols: the csp approach.* Addison-Wesley Professional.
- SAHAI, A. and WATERS, B., 2005. Fuzzy identity-based encryption. *Advances in Cryptology–EUROCRYPT 2005,* , pp. 557-557.
- SAHRAOUI, S., GHARAIBEH, G. and AL-JBOORI, A., 2006. E-Government in Saudi Arabia: Can it overcome its challenges, *e-Government Workshop* 2006.
- SARIER, N.D., 2008. A new biometric identity based encryption scheme, *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for* 2008, IEEE, pp. 2061-2066.
- SCHEIRER, W.J. and BOULT, T.E., 2007. Cracking fuzzy vaults and biometric encryption, *Biometrics Symposium, 2007* 2007, IEEE, pp. 1-6.
- *Security Applications.* Springer, pp. 189-209.
- SEN, J., A Robust Identity-Based Signature Scheme that Avoids Key Escrow Problem.
- SHAMIR, A., 1979. How to share a secret. *Communications of the ACM,* **22**(11), pp. 612-613.
- SHAMIR, A., 1985. Identity-based cryptosystems and signature schemes, *Advances in cryptology* 1985, Springer, pp. 47-53.
- SILVA, M., 2012. 50 years after the PhD thesis of Carl Adam Petri: A perspective⋆.
- SLOAN, R.H. and WARNER, R., 2013. *Unauthorized Access: The Crisis in Online*

Privacy and Security. CRC Press.
- SPEED, T.J., 2012. *Asset Protection through Security Awareness*. CRC Press.
- STAGE, R., GE, S. and GE, R.S., The DISASTER RISK MANAGEMENT CYCLE (DRMC).
- STAPLETON, J.J., 2014. *Security Without Obscurity: A Guide to Confidentiality, Authentication, and Integrity*. CRC Press.
- STEVENS, P., POOLEY, R.J. and POOLEY, R., 2006. *Using UML: software engineering with objects and components*. Addison-Wesley Longman.
- TANENBAUM, A.S., 2003. *Computer networks*. 4th edn. Upper Saddle River, N.J.; London: Prentice Hall PTR; Pearson Education.
- TANENBAUM, A.S., 2011. *Computer networks*. 5th edn. Boston, Mass; London: Pearson Education.
- TAPAAL 2.4.3 Petri nets simulation and verfication of timed-arc Petri nets. Available at: www.tapaal.net.
- TULYAKOV, S., FAROOQ, F., MANSUKHANI, P. and GOVINDARAJU, V., 2007. Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters,* **28**(16), pp. 2427-2436.
- ULUDAG, U., PANKANTI, S., PRABHAKAR, S. and JAIN, A.K., 2004. Biometric cryptosystems: Issues and challenges. *Proceedings of the IEEE,* **92**(6), pp. 948-960.
- UPMANYU, M., NAMBOODIRI, A.M., SRINATHAN, K. and JAWAHAR, C., 2010. Blind authentication: a secure crypto-biometric verification protocol. *Information Forensics and Security, IEEE Transactions on,* **5**(2), pp. 255-268.
- VACCA, J.R., 2007. *Biometric technologies and verification systems*. Oxford: Butterworth-Heinemann.
- VIELHAUER, C., 2005. *Biometric user authentication for IT security: from fundamentals to handwriting*. New York; London: Springer.
- VOLTAGE SECURITY, 2006. *Identity-Based Encryption and PKI Making Security Work*. http://www.voltage.com/pdf/IBE_and_PKI.pdf edn. Voltage Security, Inc.
- WANG, D. and MA, C., 2013. Cryptanalysis of a remote user authentication scheme for mobile client-server environment based on ECC. *Information Fusion*.
- WANG, X., XU, T. and ZHANG, W., Chaos-Based Biometrics Template Protection and Secure Authentication.
- WILLIAM, S. and STALLINGS, W., 2006. *Cryptography and Network Security, 4/E*. Pearson Education India.
- WILSON, S., 2005. The importance of PKI today. *China Communications,* , pp. 15.
- WONG, K., 2002. A fast chaotic cryptographic scheme with dynamic look-up table. *Physics Letters A,* **298**(4), pp. 238-242.
- XU, Y. and XIE, X., 2011. Modelling and analysis of security protocols using coloured petri nets. *Journal of Computers,* **6**(1), pp. 19-27.
- YOKOYAMA, V.T.V., 2000. Elliptic curve cryptosystem. *Fujitsu Sci.Tech.J,* **36**(2), pp. 140-146.
- YUEN, T., SUSILO, W. and MU, Y., 2010. How to construct identity-based signatures without the key escrow problem. *Public Key Infrastructures, Services and Applications,* , pp. 286-301.
- YUSSOFF, Y.M., HASHIM, H. and BABA, M.D., 2012. Identity-based trusted authentication in wireless sensor network. *arXiv preprint arXiv:1207.6185,* .
- ZHANG, L., CHOFFNES, D., LEVIN, D., DUMITRAS, T., MISLOVE, A., SCHULMAN, A. and WILSON, C., 2014. Analysis of SSL certificate reissues and

revocations in the wake of Heartbleed, *Proceedings of the 2014 Conference on Internet Measurement Conference* 2014, ACM, pp. 489-502.

- ZHANG, Z., WONG, D., XU, J. and FENG, D., 2006. Certificateless public-key signature: security model and efficient construction, *Applied Cryptography and Network Security* 2006, Springer, pp. 293-308.
- ZHAO, S., AGGARWAL, A., FROST, R. and BAI, X., 2012. A survey of applications of identity-based cryptography in mobile ad-hoc networks. *Communications Surveys & Tutorials, IEEE,* **14**(2), pp. 380-400.

A

Appendix: Finite State Machine

EFSM Register

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg width="800" height="600" version="1.1"
xmlns="http://www.w3.org/2000/svg">
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="480.5" cy="172.5" rx="30" ry="30"/>
      <text x="468.5" y="178.5" font-family="Times New Roman" font-
size="20">R1</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="480.5" cy="341.5" rx="30" ry="30"/>
```


<text x="468.5" y="347.5" font-family="Times New Roman" font-size="20">R2</text>
<ellipse stroke="black" stroke-width="1" fill="none" cx="198.5" cy="341.5" rx="30" ry="30"/>
<text x="186.5" y="347.5" font-family="Times New Roman" font-size="20">R3</text>
<ellipse stroke="black" stroke-width="1" fill="none" cx="198.5" cy="172.5" rx="30" ry="30"/>
<text x="186.5" y="178.5" font-family="Times New Roman" font-size="20">R0</text>
<ellipse stroke="black" stroke-width="1" fill="none" cx="49.5" cy="172.5" rx="30" ry="30"/>
<polygon stroke="black" stroke-width="1" points="480.5,202.5 480.5,311.5"/>
<polygon fill="black" stroke-width="1" points="480.5,311.5 485.5,303.5 475.5,303.5"/>
<text x="397.5" y="263.5" font-family="Times New Roman" font-size="20">Enter PW</text>
<polygon stroke="black" stroke-width="1" points="450.5,341.5 228.5,341.5"/>
<polygon fill="black" stroke-width="1" points="228.5,341.5 236.5,346.5 236.5,336.5"/>
<text x="293.5" y="362.5" font-family="Times New Roman" font-size="20">Submit Bio</text>
<polygon stroke="black" stroke-width="1" points="198.5,311.5 198.5,202.5"/>
<polygon fill="black" stroke-width="1" points="198.5,202.5 193.5,210.5 203.5,210.5"/>
<text x="203.5" y="263.5" font-family="Times New Roman" font-size="20">Enrolled</text>
<polygon stroke="black" stroke-width="1" points="480.5,142.5 480.5,142.5"/>
<text x="485.5" y="148.5" font-family="Times New Roman" font-size="20">Validate ID</text>
<polygon fill="black" stroke-width="1" points="480.5,142.5 485.5,134.5 475.5,134.5"/>
<path stroke="black" stroke-width="1" fill="none" d="M 506.659,355.945 A 22.5,22.5 0 1 1 484.946,371.05"/>
<text x="524.5" y="417.5" font-family="Times New Roman" font-size="20">Re-enter PW</text>
<polygon fill="black" stroke-width="1" points="484.946,371.05 479.783,378.946 489.781,379.151"/>
<polygon stroke="black" stroke-width="1" points="228.5,172.5 450.5,172.5"/>
<polygon fill="black" stroke-width="1" points="450.5,172.5 442.5,167.5 442.5,177.5"/>
<text x="304.5" y="193.5" font-family="Times New Roman" font-size="20">Enter ID</text>
<path stroke="black" stroke-width="1" fill="none" d="M 186.136,368.705 A 22.5,22.5 0 1 1 169.386,348.234"/>
<text x="-20.5" y="404.5" font-family="Times New Roman" font-size="20">Submit 5 Templates</text>

```
      <polygon fill="black" stroke-width="1" points="169.386,348.234
161.112,343.702 161.686,353.685"/>
      <path stroke="black" stroke-width="1" fill="none" d="M
70.732,151.494 A 92.051,92.051 0 0 1 177.268,151.494"/>
      <polygon fill="black" stroke-width="1" points="70.732,151.494
80.15,150.942 74.363,142.786"/>
      <text x="83.5" y="125.5" font-family="Times New Roman" font-
size="20">Enroll = 1</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
177.272,193.511 A 92.036,92.036 0 0 1 70.728,193.511"/>
      <polygon fill="black" stroke-width="1" points="177.272,193.511
167.855,194.064 173.643,202.219"/>
      <text x="83.5" y="231.5" font-family="Times New Roman" font-
size="20">Enroll = 0</text>
</svg>
```

EFSM Client

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg width="800" height="600" version="1.1"
xmlns="http://www.w3.org/2000/svg">
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="535.5" cy="296.5" rx="30" ry="30"/>
      <text x="523.5" y="302.5" font-family="Times New Roman" font-
size="20">C9</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="535.5" cy="296.5" rx="24" ry="24"/>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="236.5" cy="296.5" rx="30" ry="30"/>
      <text x="224.5" y="302.5" font-family="Times New Roman" font-
size="20">C2</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="195.5" cy="129.5" rx="30" ry="30"/>
      <text x="183.5" y="135.5" font-family="Times New Roman" font-
size="20">C1</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="203.5" cy="57.5" rx="30" ry="30"/>
      <text x="191.5" y="63.5" font-family="Times New Roman" font-
size="20">C0</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="450.5" cy="57.5" rx="30" ry="30"/>
      <text x="438.5" y="63.5" font-family="Times New Roman" font-
size="20">R0</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="105.5" cy="364.5" rx="30" ry="30"/>
      <text x="93.5" y="370.5" font-family="Times New Roman" font-
size="20">C4</text>
```


C3
C5
C6
C7
C8
Re-enter
Re-enter
Validate ID
Registered

```
      <polygon fill="black" stroke-width="1" points="229.354,42.329
238.744,43.237 234.285,34.286"/>
      <text x="258.5" y="10.5" font-family="Times New Roman" font-
size="20">Request to enroll</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
176.212,107.511 A 38.577,38.577 0 0 1 179.855,74.718"/>
      <polygon fill="black" stroke-width="1" points="176.212,107.511
178.338,98.32 168.882,101.572"/>
      <text x="98.5" y="95.5" font-family="Times New Roman" font-
size="20">Enter ID</text>
      <polygon stroke="black" stroke-width="1"
points="202.653,158.635 229.347,267.365"/>
      <polygon fill="black" stroke-width="1" points="229.347,267.365
232.296,258.404 222.584,260.788"/>
      <text x="130.5" y="223.5" font-family="Times New Roman" font-
size="20">Enter PW</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
259.586,277.379 A 216.799,216.799 0 0 1 512.414,277.379"/>
      <polygon fill="black" stroke-width="1" points="512.414,277.379
508.83,268.653 502.999,276.777"/>
      <text x="352.5" y="227.5" font-family="Times New Roman" font-
size="20">Timeout</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
223.628,119.121 A 247.669,247.669 0 0 1 526.52,267.895"/>
      <polygon fill="black" stroke-width="1" points="526.52,267.895
528.338,258.637 518.996,262.204"/>
      <text x="408.5" y="124.5" font-family="Times New Roman" font-
size="20">Timeout</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
327.016,354.496 A 182.746,182.746 0 0 1 506.703,288.212"/>
      <polygon fill="black" stroke-width="1" points="506.703,288.212
499.843,281.735 497.875,291.539"/>
      <text x="337.5" y="285.5" font-family="Times New Roman" font-
size="20">Timeout</text>
      <polygon stroke="black" stroke-width="1"
points="507.616,383.919 526.384,325.081"/>
      <polygon fill="black" stroke-width="1" points="526.384,325.081
519.189,331.184 528.716,334.222"/>
      <text x="524.5" y="367.5" font-family="Times New Roman" font-
size="20">Timeout</text>
      <polygon stroke="black" stroke-width="1"
points="607.194,472.712 546.806,324.288"/>
      <polygon fill="black" stroke-width="1" points="546.806,324.288
545.189,333.583 554.452,329.814"/>
      <text x="584.5" y="395.5" font-family="Times New Roman" font-
size="20">Timeout</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
84.832,342.843 A 133.01,133.01 0 0 1 165.653,131.811"/>
      <polygon fill="black" stroke-width="1" points="84.832,342.843
83.978,333.448 76.013,339.494"/>
      <text x="2.5" y="212.5" font-family="Times New Roman" font-
size="20">Invalid</text>
```

```
      <path stroke="black" stroke-width="1" fill="none" d="M
108.733,334.851 A 80.131,80.131 0 0 1 210.392,282.081"/>
      <polygon fill="black" stroke-width="1" points="108.733,334.851
115.848,328.656 106.283,325.741"/>
      <text x="87.5" y="277.5" font-family="Times New Roman" font-
size="20">Invalid</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
286.443,397.329 A 140.926,140.926 0 0 1 126.706,385.641"/>
      <polygon fill="black" stroke-width="1" points="126.706,385.641
129.805,394.551 136.073,386.759"/>
      <text x="172.5" y="439.5" font-family="Times New Roman" font-
size="20">Invalid</text>
      <polygon stroke="black" stroke-width="1"
points="471.436,425.444 318.564,498.556"/>
      <polygon fill="black" stroke-width="1" points="318.564,498.556
327.938,499.615 323.624,490.594"/>
      <text x="308.5" y="452.5" font-family="Times New Roman" font-
size="20">Terminate</text>
      <polygon stroke="black" stroke-width="1"
points="588.517,501.509 321.483,510.491"/>
      <polygon fill="black" stroke-width="1" points="321.483,510.491
329.647,515.22 329.31,505.225"/>
      <text x="412.5" y="495.5" font-family="Times New Roman" font-
size="20">Terminate</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
596.928,521.331 A 301.388,301.388 0 0 1 113.919,393.281"/>
      <polygon fill="black" stroke-width="1" points="113.919,393.281
111.821,402.479 121.268,399.198"/>
      <text x="267.5" y="608.5" font-family="Times New Roman" font-
size="20">Invalid</text>
      <polygon stroke="black" stroke-width="1"
points="522.692,430.241 594.308,482.759"/>
      <polygon fill="black" stroke-width="1" points="594.308,482.759
590.813,473.996 584.9,482.06"/>
      <text x="465.5" y="477.5" font-family="Times New Roman" font-
size="20">SYN/ACK</text>
      <polygon stroke="black" stroke-width="1"
points="340.048,384.687 468.952,407.313"/>
      <polygon fill="black" stroke-width="1" points="468.952,407.313
461.937,401.006 460.208,410.855"/>
      <text x="299.5" y="423.5" font-family="Times New Roman" font-
size="20">Valid Login Reg.</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
280.969,382.529 A 59.749,59.749 0 0 1 230.117,325.491"/>
      <polygon fill="black" stroke-width="1" points="280.969,382.529
273.799,376.397 272.316,386.287"/>
      <text x="148.5" y="383.5" font-family="Times New Roman" font-
size="20">Submit Bio</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
266.212,297.535 A 64.448,64.448 0 0 1 312.867,349.864"/>
      <polygon fill="black" stroke-width="1" points="266.212,297.535
272.605,304.472 275.249,294.828"/>
```

```
      <text x="302.5" y="308.5" font-family="Times New Roman" font-
size="20">Re-enter</text>
      <polygon stroke="black" stroke-width="1" points="146.5,25.5
177.34,42.814"/>
      <polygon fill="black" stroke-width="1" points="177.34,42.814
172.812,34.538 167.917,43.258"/>
      <polygon stroke="black" stroke-width="1"
points="648.493,499.838 724.507,498.162"/>
      <polygon fill="black" stroke-width="1" points="724.507,498.162
716.399,493.339 716.62,503.337"/>
</svg>
```

EFSM Server

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg width="800" height="600" version="1.1"
xmlns="http://www.w3.org/2000/svg">
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="535.5" cy="296.5" rx="30" ry="30"/>
      <text x="524.5" y="302.5" font-family="Times New Roman" font-
size="20">S9</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="535.5" cy="296.5" rx="24" ry="24"/>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="236.5" cy="296.5" rx="30" ry="30"/>
      <text x="225.5" y="302.5" font-family="Times New Roman" font-
size="20">S2</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="195.5" cy="129.5" rx="30" ry="30"/>
      <text x="184.5" y="135.5" font-family="Times New Roman" font-
size="20">S1</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="203.5" cy="57.5" rx="30" ry="30"/>
      <text x="192.5" y="63.5" font-family="Times New Roman" font-
size="20">S0</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="450.5" cy="57.5" rx="30" ry="30"/>
      <text x="438.5" y="63.5" font-family="Times New Roman" font-
size="20">R0</text>
```

```
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="105.5" cy="364.5" rx="30" ry="30"/>
      <text x="94.5" y="370.5" font-family="Times New Roman" font-
size="20">S4</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="105.5" cy="364.5" rx="24" ry="24"/>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="310.5" cy="379.5" rx="30" ry="30"/>
      <text x="299.5" y="385.5" font-family="Times New Roman" font-
size="20">S3</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="498.5" cy="412.5" rx="30" ry="30"/>
      <text x="487.5" y="418.5" font-family="Times New Roman" font-
size="20">S5</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="618.5" cy="500.5" rx="30" ry="30"/>
      <text x="607.5" y="506.5" font-family="Times New Roman" font-
size="20">S6</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="618.5" cy="500.5" rx="24" ry="24"/>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="291.5" cy="511.5" rx="30" ry="30"/>
      <text x="280.5" y="517.5" font-family="Times New Roman" font-
size="20">S8</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="291.5" cy="511.5" rx="24" ry="24"/>
      <polygon stroke="black" stroke-width="1" points="535.5,266.5
535.5,266.5"/>
      <text x="540.5" y="272.5" font-family="Times New Roman" font-
size="20">Validate ID</text>
      <polygon fill="black" stroke-width="1" points="535.5,266.5
540.5,258.5 530.5,258.5"/>
      <path stroke="black" stroke-width="1" fill="none" d="M
420.61,60.057 A 1273.834,1273.834 0 0 1 233.39,60.057"/>
      <polygon fill="black" stroke-width="1" points="420.61,60.057
412.264,55.658 412.999,65.631"/>
      <text x="284.5" y="84.5" font-family="Times New Roman" font-
size="20">Registered</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
229.354,42.329 A 218.99,218.99 0 0 1 424.646,42.329"/>
```

```
      <polygon fill="black" stroke-width="1" points="229.354,42.329
238.744,43.237 234.285,34.286"/>
      <text x="258.5" y="10.5" font-family="Times New Roman" font-
size="20">Request to enroll</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
176.212,107.511 A 38.577,38.577 0 0 1 179.855,74.718"/>
      <polygon fill="black" stroke-width="1" points="176.212,107.511
178.338,98.32 168.882,101.572"/>
      <text x="98.5" y="95.5" font-family="Times New Roman" font-
size="20">Enter ID</text>
      <polygon stroke="black" stroke-width="1"
points="202.653,158.635 229.347,267.365"/>
      <polygon fill="black" stroke-width="1" points="229.347,267.365
232.296,258.404 222.584,260.788"/>
      <text x="130.5" y="223.5" font-family="Times New Roman" font-
size="20">Enter PW</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
259.586,277.379 A 216.799,216.799 0 0 1 512.414,277.379"/>
      <polygon fill="black" stroke-width="1" points="512.414,277.379
508.83,268.653 502.999,276.777"/>
      <text x="352.5" y="227.5" font-family="Times New Roman" font-
size="20">Timeout</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
223.628,119.121 A 247.669,247.669 0 0 1 526.52,267.895"/>
      <polygon fill="black" stroke-width="1" points="526.52,267.895
528.338,258.637 518.996,262.204"/>
      <text x="408.5" y="124.5" font-family="Times New Roman" font-
size="20">Timeout</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
327.016,354.496 A 182.746,182.746 0 0 1 506.703,288.212"/>
      <polygon fill="black" stroke-width="1" points="506.703,288.212
499.843,281.735 497.875,291.539"/>
      <text x="337.5" y="285.5" font-family="Times New Roman" font-
size="20">Timeout</text>
      <polygon stroke="black" stroke-width="1"
points="507.616,383.919 526.384,325.081"/>
      <polygon fill="black" stroke-width="1" points="526.384,325.081
519.189,331.184 528.716,334.222"/>
      <text x="524.5" y="367.5" font-family="Times New Roman" font-
size="20">Timeout</text>
```

```
      <polygon stroke="black" stroke-width="1"
points="607.194,472.712 546.806,324.288"/>
      <polygon fill="black" stroke-width="1" points="546.806,324.288
545.189,333.583 554.452,329.814"/>
      <text x="584.5" y="395.5" font-family="Times New Roman" font-
size="20">Timeout</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
84.832,342.843 A 133.01,133.01 0 0 1 165.653,131.811"/>
      <polygon fill="black" stroke-width="1" points="84.832,342.843
83.978,333.448 76.013,339.494"/>
      <text x="2.5" y="212.5" font-family="Times New Roman" font-
size="20">Invalid</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
108.733,334.851 A 80.131,80.131 0 0 1 210.392,282.081"/>
      <polygon fill="black" stroke-width="1" points="108.733,334.851
115.848,328.656 106.283,325.741"/>
      <text x="87.5" y="277.5" font-family="Times New Roman" font-
size="20">Invalid</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
286.443,397.329 A 140.926,140.926 0 0 1 126.706,385.641"/>
      <polygon fill="black" stroke-width="1" points="126.706,385.641
129.805,394.551 136.073,386.759"/>
      <text x="172.5" y="439.5" font-family="Times New Roman" font-
size="20">Invalid</text>
      <polygon stroke="black" stroke-width="1"
points="471.436,425.444 318.564,498.556"/>
      <polygon fill="black" stroke-width="1" points="318.564,498.556
327.938,499.615 323.624,490.594"/>
      <text x="308.5" y="452.5" font-family="Times New Roman" font-
size="20">Terminate</text>
      <polygon stroke="black" stroke-width="1"
points="588.517,501.509 321.483,510.491"/>
      <polygon fill="black" stroke-width="1" points="321.483,510.491
329.647,515.22 329.31,505.225"/>
      <text x="412.5" y="495.5" font-family="Times New Roman" font-
size="20">Terminate</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
596.928,521.331 A 301.388,301.388 0 0 1 113.919,393.281"/>
      <polygon fill="black" stroke-width="1" points="113.919,393.281
111.821,402.479 121.268,399.198"/>
```

```
      <text x="267.5" y="608.5" font-family="Times New Roman" font-
size="20">Invalid</text>
      <polygon stroke="black" stroke-width="1"
points="522.692,430.241 594.308,482.759"/>
      <polygon fill="black" stroke-width="1" points="594.308,482.759
590.813,473.996 584.9,482.06"/>
      <text x="511.5" y="477.5" font-family="Times New Roman" font-
size="20">ACK</text>
      <polygon stroke="black" stroke-width="1"
points="340.048,384.687 468.952,407.313"/>
      <polygon fill="black" stroke-width="1" points="468.952,407.313
461.937,401.006 460.208,410.855"/>
      <text x="372.5" y="419.5" font-family="Times New Roman" font-
size="20">SYN</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
280.969,382.529 A 59.749,59.749 0 0 1 230.117,325.491"/>
      <polygon fill="black" stroke-width="1" points="280.969,382.529
273.799,376.397 272.316,386.287"/>
      <text x="148.5" y="383.5" font-family="Times New Roman" font-
size="20">Submit Bio</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
173.62,57.065 A 22.5,22.5 0 1 1 185.67,33.519"/>
      <text x="-5.5" y="21.5" font-family="Times New Roman" font-
size="20">Waiting for client</text>
      <polygon fill="black" stroke-width="1" points="185.67,33.519
186.51,24.122 177.592,28.647"/>
      <path stroke="black" stroke-width="1" fill="none" d="M
225.011,134.197 A 22.5,22.5 0 1 1 209.723,155.781"/>
      <text x="256.5" y="188.5" font-family="Times New Roman" font-
size="20">Re-enter</text>
      <polygon fill="black" stroke-width="1" points="209.723,155.781
207.55,164.962 217.023,161.757"/>
      <path stroke="black" stroke-width="1" fill="none" d="M
250.723,270.219 A 22.5,22.5 0 1 1 266.011,291.803"/>
      <text x="297.5" y="249.5" font-family="Times New Roman" font-
size="20">Re-enter</text>
      <polygon fill="black" stroke-width="1" points="266.011,291.803
273.951,296.899 274.071,286.899"/>
      <path stroke="black" stroke-width="1" fill="none" d="M
328.969,356.007 A 22.5,22.5 0 1 1 340.381,379.869"/>
```

```
      <text x="378.5" y="345.5" font-family="Times New Roman" font-
size="20">Re-enter</text>
      <polygon fill="black" stroke-width="1" points="340.381,379.869
347.342,386.236 349.154,376.402"/>
</svg>
```

EFSM Verifier

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg width="800" height="600" version="1.1"
xmlns="http://www.w3.org/2000/svg">
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="440.5" cy="88.5" rx="30" ry="30"/>
      <text x="428.5" y="94.5" font-family="Times New Roman" font-
size="20">V1</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="537.5" cy="199.5" rx="30" ry="30"/>
      <text x="525.5" y="205.5" font-family="Times New Roman" font-
size="20">V2</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="493.5" cy="348.5" rx="30" ry="30"/>
      <text x="481.5" y="354.5" font-family="Times New Roman" font-
size="20">V3</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="198.5" cy="341.5" rx="30" ry="30"/>
      <text x="186.5" y="347.5" font-family="Times New Roman" font-
size="20">V4</text>
      <ellipse stroke="black" stroke-width="1" fill="none"
cx="198.5" cy="166.5" rx="30" ry="30"/>
      <text x="186.5" y="172.5" font-family="Times New Roman" font-
size="20">V0</text>
      <ellipse stroke="black" stroke-width="1" fill="none" cx="-7.5"
cy="166.5" rx="30" ry="30"/>
      <text x="-12.5" y="172.5" font-family="Times New Roman" font-
size="20">v</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
466.978,102.518 A 167.653,167.653 0 0 1 527.157,171.382"/>
      <polygon fill="black" stroke-width="1" points="527.157,171.382
528.255,162.012 519.216,166.289"/>
      <text x="507.5" y="124.5" font-family="Times New Roman" font-
size="20">Integrity checked</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
544.441,228.619 A 130.815,130.815 0 0 1 515.145,327.823"/>
      <polygon fill="black" stroke-width="1" points="515.145,327.823
524.105,324.868 516.415,318.475"/>
      <text x="547.5" y="293.5" font-family="Times New Roman" font-
size="20">Decrypted done</text>
```

```
      <path stroke="black" stroke-width="1" fill="none" d="M
464.383,355.707 A 505.739,505.739 0 0 1 227.242,350.08"/>
      <polygon fill="black" stroke-width="1" points="227.242,350.08
233.685,356.972 236.26,347.309"/>
      <text x="269.5" y="389.5" font-family="Times New Roman" font-
size="20">Freshness checked</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
180.557,317.545 A 126.861,126.861 0 0 1 180.557,190.455"/>
      <polygon fill="black" stroke-width="1" points="180.557,190.455
172.222,194.875 180.877,199.884"/>
      <text x="92.5" y="259.5" font-family="Times New Roman" font-
size="20">ID valid</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
213.566,140.601 A 174.163,174.163 0 0 1 413.145,76.274"/>
      <polygon fill="black" stroke-width="1" points="413.145,76.274
407.228,68.926 403.948,78.373"/>
      <text x="156.5" y="62.5" font-family="Times New Roman" font-
size="20">Authenticity check</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
225.6,179.368 A 1449.769,1449.769 0 0 1 469.843,330.053"/>
      <polygon fill="black" stroke-width="1" points="225.6,179.368
230.599,187.368 234.982,178.379"/>
      <text x="356.5" y="239.5" font-family="Times New Roman" font-
size="20">Not valid</text>
      <polygon stroke="black" stroke-width="1" points="198.5,311.5
198.5,196.5"/>
      <polygon fill="black" stroke-width="1" points="198.5,196.5
193.5,204.5 203.5,204.5"/>
      <text x="203.5" y="260.5" font-family="Times New Roman" font-
size="20">Not valid</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
418.842,109.235 A 260.716,260.716 0 0 1 228.19,170.685"/>
      <polygon fill="black" stroke-width="1" points="228.19,170.685
235.751,176.327 236.575,166.361"/>
      <text x="329.5" y="181.5" font-family="Times New Roman" font-
size="20">Not valid</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
16.701,148.85 A 154.989,154.989 0 0 1 174.299,148.85"/>
      <polygon fill="black" stroke-width="1" points="174.299,148.85
169.952,140.477 164.868,149.088"/>
      <text x="61.5" y="118.5" font-family="Times New Roman" font-
size="20">Validate</text>
      <path stroke="black" stroke-width="1" fill="none" d="M
170.46,177.116 A 251.749,251.749 0 0 1 20.54,177.116"/>
      <polygon fill="black" stroke-width="1" points="20.54,177.116
26.688,184.271 29.666,174.725"/>
      <text x="69.5" y="209.5" font-family="Times New Roman" font-
size="20">Result</text>
</svg>
```

B

Appendix: Petri Nets

Trust Model with Adversary

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<pnml xmlns="http://www.informatik.hu-berlin.de/top/pnml/ptNetb">
<shared-transition name="T8" urgent="false"/>
<shared-transition name="T20" urgent="false"/>
<shared-transition name="T32" urgent="false"/>
<constant name="periodC" value="7"/>
<constant name="PeriodS" value="5"/>
<constant name="Deadline" value="5"/>
<net active="true" id="TAPN1" type="P/T net">
```

<place id="P1" initialMarking="2" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P1"
nameOffsetX="22.0" nameOffsetY="-4.0" positionX="30.0"
positionY="105.0"/>
<place id="P2" initialMarking="2" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P2"
nameOffsetX="17.0" nameOffsetY="-4.0" positionX="15.0"
positionY="150.0"/>
<place id="P4" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P4"
nameOffsetX="25.0" nameOffsetY="-5.0" positionX="105.0"
positionY="150.0"/>
<place id="P6" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P6"
nameOffsetX="23.0" nameOffsetY="-4.0" positionX="180.0"
positionY="150.0"/>
<place id="P16" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P16"
nameOffsetX="26.0" nameOffsetY="-3.0" positionX="780.0"
positionY="150.0"/>
<place id="P18" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P18"
nameOffsetX="53.0" nameOffsetY="-17.0" positionX="750.0"
positionY="30.0"/>
<place id="P19" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P19"
nameOffsetX="48.0" nameOffsetY="31.0" positionX="795.0"
positionY="240.0"/>
<place id="P20" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P20"
nameOffsetX="2.0" nameOffsetY="22.0" positionX="885.0"
positionY="270.0"/>
<place id="P22" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P22"
nameOffsetX="29.0" nameOffsetY="-3.0" positionX="795.0"
positionY="315.0"/>
<place id="P23" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P23"
nameOffsetX="3.0" nameOffsetY="3.0" positionX="855.0"
positionY="390.0"/>
<place id="P24" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P24"
nameOffsetX="34.0" nameOffsetY="0.0" positionX="735.0"
positionY="390.0"/>
<place id="P33" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P33"
nameOffsetX="27.0" nameOffsetY="-1.0" positionX="90.0"
positionY="390.0"/>
<place id="P34" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P34"
nameOffsetX="63.0" nameOffsetY="36.0" positionX="150.0"
positionY="480.0"/>

<place id="P36" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P36"
nameOffsetX="98.0" nameOffsetY="-18.0" positionX="30.0"
positionY="585.0"/>
<place id="P21" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P21"
nameOffsetX="38.0" nameOffsetY="-2.0" positionX="885.0"
positionY="360.0"/>
<place id="P3" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P3"
nameOffsetX="11.0" nameOffsetY="3.0" positionX="30.0"
positionY="195.0"/>
<place id="P37" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P37"
nameOffsetX="28.0" nameOffsetY="1.0" positionX="135.0"
positionY="585.0"/>
<place id="P38" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P38"
nameOffsetX="24.0" nameOffsetY="-2.0" positionX="90.0"
positionY="645.0"/>
<place id="P46" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P46"
nameOffsetX="34.0" nameOffsetY="-7.0" positionX="720.0"
positionY="645.0"/>
<place id="P49" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P49"
nameOffsetX="69.0" nameOffsetY="-18.0" positionX="660.0"
positionY="735.0"/>
<place id="P50" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P50"
nameOffsetX="54.0" nameOffsetY="30.0" positionX="855.0"
positionY="855.0"/>
<place id="P26" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P26"
nameOffsetX="25.0" nameOffsetY="-5.0" positionX="630.0"
positionY="390.0"/>
<place id="P39" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P39"
nameOffsetX="27.0" nameOffsetY="-7.0" positionX="180.0"
positionY="645.0"/>
<place id="P42" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P42"
nameOffsetX="35.0" nameOffsetY="-4.0" positionX="450.0"
positionY="645.0"/>
<place id="P43" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P43"
nameOffsetX="25.0" nameOffsetY="-1.0" positionX="540.0"
positionY="645.0"/>
<place id="P14" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P14"
nameOffsetX="23.0" nameOffsetY="-4.0" positionX="705.0"
positionY="150.0"/>

<place id="P12" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P12"
nameOffsetX="17.0" nameOffsetY="-7.0" positionX="630.0"
positionY="150.0"/>
<place id="P35" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P35"
nameOffsetX="57.0" nameOffsetY="23.0" positionX="270.0"
positionY="555.0"/>
<place id="P48" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P48"
nameOffsetX="79.0" nameOffsetY="-22.0" positionX="855.0"
positionY="735.0"/>
<place id="P17" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P17"
nameOffsetX="62.0" nameOffsetY="-12.0" positionX="870.0"
positionY="150.0"/>
<place id="P9" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P9"
nameOffsetX="15.0" nameOffsetY="-5.0" positionX="360.0"
positionY="150.0"/>
<place id="P10" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P10"
nameOffsetX="26.0" nameOffsetY="-2.0" positionX="450.0"
positionY="150.0"/>
<place id="P32" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P32"
nameOffsetX="33.0" nameOffsetY="-3.0" positionX="180.0"
positionY="390.0"/>
<place id="P15" initialMarking="3" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P15" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="735.0" positionY="210.0"/>
<place id="P8" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P8"
nameOffsetX="22.0" nameOffsetY="-6.0" positionX="270.0"
positionY="150.0"/>
<place id="P13" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P13"
nameOffsetX="37.0" nameOffsetY="1.0" positionX="705.0"
positionY="90.0"/>
<place id="P25" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P25" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="765.0" positionY="450.0"/>
<place id="P27" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P27"
nameOffsetX="17.0" nameOffsetY="-1.0" positionX="540.0"
positionY="390.0"/>
<place id="P28" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P28"
nameOffsetX="24.0" nameOffsetY="-1.0" positionX="450.0"
positionY="390.0"/>
<place id="P29" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P29"

nameOffsetX="23.0" nameOffsetY="-3.0" positionX="360.0"
positionY="390.0"/>
<place id="P31" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P31"
nameOffsetX="12.0" nameOffsetY="0.0" positionX="165.0"
positionY="315.0"/>
<place id="P40" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P40"
nameOffsetX="24.0" nameOffsetY="1.0" positionX="270.0"
positionY="645.0"/>
<place id="P41" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P41"
nameOffsetX="14.0" nameOffsetY="2.0" positionX="360.0"
positionY="645.0"/>
<place id="P45" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P45"
nameOffsetX="24.0" nameOffsetY="-3.0" positionX="720.0"
positionY="585.0"/>
<place id="P47" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P47"
nameOffsetX="17.0" nameOffsetY="-3.0" positionX="810.0"
positionY="645.0"/>
<place id="P51" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P51" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="660.0" positionY="855.0"/>
<place id="P7" initialMarking="2" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P7" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="180.0" positionY="225.0"/>
<place id="P5" initialMarking="3" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P5" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="120.0" positionY="225.0"/>
<place id="P11" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P11"
nameOffsetX="24.0" nameOffsetY="2.0" positionX="540.0"
positionY="150.0"/>
<place id="P30" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P30"
nameOffsetX="24.0" nameOffsetY="0.0" positionX="270.0"
positionY="390.0"/>
<place id="P44" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P44"
nameOffsetX="28.0" nameOffsetY="-5.0" positionX="630.0"
positionY="645.0"/>
<transition angle="0" id="T1" infiniteServer="false" name="T1"
nameOffsetX="34.0" nameOffsetY="41.0" positionX="60.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T2" infiniteServer="false" name="T2"
nameOffsetX="34.0" nameOffsetY="48.0" positionX="135.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T10" infiniteServer="false" name="T10"
nameOffsetX="26.0" nameOffsetY="51.0" positionX="825.0"
positionY="150.0" priority="0" urgent="false"/>

<transition angle="0" id="T13" infiniteServer="false" name="T13"
nameOffsetX="10.0" nameOffsetY="42.0" positionX="855.0"
positionY="315.0" priority="0" urgent="false"/>
<transition angle="0" id="T21" infiniteServer="false" name="T21"
nameOffsetX="10.0" nameOffsetY="52.0" positionX="135.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T22" infiniteServer="false" name="T22"
nameOffsetX="10.0" nameOffsetY="39.0" positionX="45.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="180" id="T25" infiniteServer="false" name="T25"
nameOffsetX="27.0" nameOffsetY="50.0" positionX="30.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T32" infiniteServer="false" name="T32"
nameOffsetX="41.0" nameOffsetY="43.0" positionX="675.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T34" infiniteServer="false" name="T34"
nameOffsetX="19.0" nameOffsetY="47.0" positionX="855.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="180" id="T3" infiniteServer="false" name="T3"
nameOffsetX="34.0" nameOffsetY="42.0" positionX="225.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T15" infiniteServer="false" name="T15"
nameOffsetX="19.0" nameOffsetY="45.0" positionX="690.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T30" infiniteServer="false" name="T30"
nameOffsetX="18.0" nameOffsetY="46.0" positionX="495.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="270" id="T24" infiniteServer="false" name="T24"
nameOffsetX="40.0" nameOffsetY="38.0" positionX="30.0"
positionY="480.0" priority="0" urgent="false"/>
<transition angle="0" id="T35" infiniteServer="false" name="T35"
nameOffsetX="39.0" nameOffsetY="40.0" positionX="720.0"
positionY="735.0" priority="0" urgent="false"/>
<transition angle="90" id="T36" infiniteServer="false" name="T36"
nameOffsetX="53.0" nameOffsetY="31.0" positionX="855.0"
positionY="795.0" priority="0" urgent="false"/>
<transition angle="0" id="T11" infiniteServer="false" name="T11"
nameOffsetX="23.0" nameOffsetY="40.0" positionX="810.0"
positionY="30.0" priority="0" urgent="false"/>
<transition angle="0" id="T12" infiniteServer="false" name="T12"
nameOffsetX="52.0" nameOffsetY="14.0" positionX="870.0"
positionY="240.0" priority="0" urgent="false"/>
<transition angle="0" id="T5" infiniteServer="false" name="T5"
nameOffsetX="25.0" nameOffsetY="51.0" positionX="405.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T6" infiniteServer="false" name="T6"
nameOffsetX="15.0" nameOffsetY="47.0" positionX="495.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T8" infiniteServer="false" name="T8"
nameOffsetX="32.0" nameOffsetY="50.0" positionX="660.0"
positionY="150.0" priority="0" urgent="false"/>

<transition angle="0" id="T14" infiniteServer="false" name="T14"
nameOffsetX="29.0" nameOffsetY="52.0" positionX="780.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T4" infiniteServer="false" name="T4"
nameOffsetX="20.0" nameOffsetY="48.0" positionX="315.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T20" infiniteServer="false" name="T20"
nameOffsetX="19.0" nameOffsetY="44.0" positionX="225.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T9" infiniteServer="false" name="T9"
nameOffsetX="40.0" nameOffsetY="39.0" positionX="735.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T16" infiniteServer="false" name="T16"
nameOffsetX="39.0" nameOffsetY="46.0" positionX="585.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T18" infiniteServer="false" name="T18"
nameOffsetX="42.0" nameOffsetY="46.0" positionX="405.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T17" infiniteServer="false" name="T17"
nameOffsetX="19.0" nameOffsetY="48.0" positionX="495.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T27" infiniteServer="false" name="T27"
nameOffsetX="43.0" nameOffsetY="41.0" positionX="225.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T28" infiniteServer="false" name="T28"
nameOffsetX="13.0" nameOffsetY="48.0" positionX="315.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T29" infiniteServer="false" name="T29"
nameOffsetX="40.0" nameOffsetY="45.0" positionX="405.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T33" infiniteServer="false" name="T33"
nameOffsetX="23.0" nameOffsetY="47.0" positionX="765.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T26" infiniteServer="false" name="T26"
nameOffsetX="49.0" nameOffsetY="51.0" positionX="135.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T37" infiniteServer="false" name="T37"
nameOffsetX="24.0" nameOffsetY="45.0" positionX="720.0"
positionY="855.0" priority="0" urgent="false"/>
<transition angle="0" id="T7" infiniteServer="false" name="T7"
nameOffsetX="23.0" nameOffsetY="47.0" positionX="585.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T19" infiniteServer="false" name="T19"
nameOffsetX="18.0" nameOffsetY="51.0" positionX="315.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T31" infiniteServer="false" name="T31"
nameOffsetX="41.0" nameOffsetY="45.0" positionX="585.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="90" id="T23" infiniteServer="false" name="T23"
nameOffsetX="46.0" nameOffsetY="39.0" positionX="270.0"
positionY="480.0" priority="0" urgent="false"/>

```
<arc id="Tc to generateLoginRequest" inscription="[0,inf)"
source="P2" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="41" yCoord="164"/>
<arcpath arcPointType="false" id="1" xCoord="66" yCoord="167"/>
</arc>
<arc id="generateLoginRequest to LgoinRqst" inscription="1"
source="T1" target="P4" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="76" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="102" yCoord="162"/>
</arc>
<arc id="LgoinRqst to Encrypt" inscription="[0,inf)" source="P4"
target="T2" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="131" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="141" yCoord="162"/>
</arc>
<arc id="Encrypt to Cipher1" inscription="1" source="T2" target="P6"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="151" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="177" yCoord="162"/>
</arc>
<arc id="MSG1 to T4" inscription="[0,inf)" source="P16" target="T10"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="806" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="831" yCoord="162"/>
</arc>
<arc id="Rs to T6" inscription="[0,inf)" source="P20" target="T13"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="896" yCoord="296"/>
<arcpath arcPointType="false" id="1" xCoord="895" yCoord="326"/>
<arcpath arcPointType="false" id="2" xCoord="872" yCoord="322"/>
</arc>
<arc id="Accept to T6" inscription="[0,inf)" source="P19"
target="T13" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="809" yCoord="266"/>
<arcpath arcPointType="false" id="1" xCoord="812" yCoord="286"/>
<arcpath arcPointType="false" id="2" xCoord="854" yCoord="289"/>
<arcpath arcPointType="false" id="3" xCoord="867" yCoord="312"/>
</arc>
<arc id="T6 to SK_s" inscription="1" source="T13" target="P22"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="861" yCoord="327"/>
<arcpath arcPointType="false" id="1" xCoord="821" yCoord="327"/>
</arc>
<arc id="T6 to SYN_ACK" inscription="1" source="T13" target="P23"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="867" yCoord="342"/>
<arcpath arcPointType="false" id="1" xCoord="867" yCoord="387"/>
</arc>
<arc id="Decrypt_ to MSG2" inscription="1" source="T21" target="P33"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="141" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="116" yCoord="402"/>
```

```
</arc>
<arc id="MSG2 to T9" inscription="[0,inf)" source="P33" target="T22"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="87" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="61" yCoord="402"/>
</arc>
<arc id="T9 to Reject2" inscription="1" source="T22" target="P34"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="57" yCoord="417"/>
<arcpath arcPointType="false" id="1" xCoord="55" yCoord="458"/>
<arcpath arcPointType="false" id="2" xCoord="147" yCoord="487"/>
</arc>
<arc id="Ts to T6" inscription="[0,inf)" source="P21" target="T13"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="896" yCoord="357"/>
<arcpath arcPointType="false" id="1" xCoord="896" yCoord="342"/>
<arcpath arcPointType="false" id="2" xCoord="871" yCoord="332"/>
</arc>
<arc id="Requst to generateLoginRequest" inscription="[0,inf)"
source="P3" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="54" yCoord="198"/>
<arcpath arcPointType="false" id="1" xCoord="68" yCoord="188"/>
<arcpath arcPointType="false" id="2" xCoord="72" yCoord="177"/>
</arc>
<arc id="Tc to T12" inscription="[0,inf)" source="P2" target="T25"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="18" yCoord="174"/>
<arcpath arcPointType="false" id="1" xCoord="21" yCoord="171"/>
<arcpath arcPointType="false" id="2" xCoord="21" yCoord="651"/>
<arcpath arcPointType="false" id="3" xCoord="37" yCoord="651"/>
</arc>
<arc id="T12 to SK_c" inscription="1" source="T25" target="P37"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="47" yCoord="651"/>
<arcpath arcPointType="false" id="1" xCoord="81" yCoord="606"/>
<arcpath arcPointType="false" id="2" xCoord="132" yCoord="599"/>
</arc>
<arc id="T12 to ACK" inscription="1" source="T25" target="P38"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="46" yCoord="661"/>
<arcpath arcPointType="false" id="1" xCoord="87" yCoord="658"/>
</arc>
<arc id="_Decrypt to MSG3" inscription="1" source="T32" target="P46"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="691" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="717" yCoord="657"/>
</arc>
<arc id="Cipher1 to Receive_Cipher1" inscription="[0,inf)"
source="P6" target="T3" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="206" yCoord="160"/>
<arcpath arcPointType="false" id="1" xCoord="232" yCoord="156"/>
</arc>
```

```
<arc id="Cipher2 to T20" inscription="[0,inf)" source="P24"
target="T15" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="732" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="706" yCoord="402"/>
</arc>
<arc id="Intercept_MSG_ to MSG2_A_" inscription="1" source="T15"
target="P26" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="696" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="656" yCoord="402"/>
</arc>
<arc id="Accept2 to T12" inscription="[0,inf)" source="P36"
target="T25" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="41" yCoord="611"/>
<arcpath arcPointType="false" id="1" xCoord="41" yCoord="641"/>
</arc>
<arc id="xMSG3x to SendMSG3_" inscription="[0,inf)" source="P42"
target="T30" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="476" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="501" yCoord="657"/>
</arc>
<arc id="SendMSG3_ to XMSG3X_" inscription="1" source="T30"
target="P43" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="511" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="537" yCoord="657"/>
</arc>
<arc id="P28 to T17" inscription="[0,Deadline]:1" source="P34"
target="T24" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="147" yCoord="491"/>
<arcpath arcPointType="false" id="1" xCoord="57" yCoord="491"/>
</arc>
<arc id="T17 to P30" inscription="[0,Deadline]:1" source="T24"
target="P36" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="42" yCoord="497"/>
<arcpath arcPointType="false" id="1" xCoord="42" yCoord="582"/>
</arc>
<arc id="P37 to T24" inscription="[Deadline,Deadline]" source="P48"
target="T35" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="852" yCoord="747"/>
<arcpath arcPointType="false" id="1" xCoord="736" yCoord="747"/>
</arc>
<arc id="T24 to P38" inscription="1" source="T35" target="P49"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="726" yCoord="747"/>
<arcpath arcPointType="false" id="1" xCoord="686" yCoord="747"/>
</arc>
<arc id="P37 to T25" inscription="[0,Deadline]:1" source="P48"
target="T36" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="866" yCoord="761"/>
<arcpath arcPointType="false" id="1" xCoord="866" yCoord="801"/>
</arc>
<arc id="T25 to P39" inscription="[0,Deadline]:1" source="T36"
target="P50" type="transport" weight="1">
```

```
<arcpath arcPointType="false" id="0" xCoord="866" yCoord="811"/>
<arcpath arcPointType="false" id="1" xCoord="866" yCoord="852"/>
</arc>
<arc id="T23 to P37" inscription="1" source="T34" target="P48"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="867" yCoord="672"/>
<arcpath arcPointType="false" id="1" xCoord="867" yCoord="732"/>
</arc>
<arc id="T7 to P13" inscription="1" source="T10" target="P17"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="841" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="867" yCoord="162"/>
</arc>
<arc id="P13 to T8" inscription="[Deadline,Deadline]" source="P17"
target="T11" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="882" yCoord="147"/>
<arcpath arcPointType="false" id="1" xCoord="884" yCoord="97"/>
<arcpath arcPointType="false" id="2" xCoord="826" yCoord="42"/>
</arc>
<arc id="T8 to P14" inscription="1" source="T11" target="P18"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="816" yCoord="42"/>
<arcpath arcPointType="false" id="1" xCoord="776" yCoord="42"/>
</arc>
<arc id="P13 to T9" inscription="[0,Deadline]:1" source="P17"
target="T12" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="882" yCoord="176"/>
<arcpath arcPointType="false" id="1" xCoord="882" yCoord="237"/>
</arc>
<arc id="T9 to P15" inscription="[0,Deadline]:1" source="T12"
target="P19" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="876" yCoord="252"/>
<arcpath arcPointType="false" id="1" xCoord="821" yCoord="252"/>
</arc>
<arc id="P9 to T5" inscription="[0,inf)" source="P9" target="T5"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="386" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="411" yCoord="162"/>
</arc>
<arc id="T5 to P10" inscription="1" source="T5" target="P10"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="421" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="447" yCoord="162"/>
</arc>
<arc id="P12 to T8" inscription="[0,inf)" source="P12" target="T8"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="656" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="666" yCoord="162"/>
</arc>
<arc id="T8 to P13" inscription="1" source="T8" target="P14"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="676" yCoord="162"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="702" yCoord="162"/>
</arc>
<arc id="T15 to P25" inscription="1" source="T14" target="P24"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="786" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="761" yCoord="402"/>
</arc>
<arc id="P1 to T22__" inscription="[0,inf)" source="P1" target="T25"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="27" yCoord="118"/>
<arcpath arcPointType="false" id="1" xCoord="14" yCoord="119"/>
<arcpath arcPointType="false" id="2" xCoord="14" yCoord="659"/>
<arcpath arcPointType="false" id="3" xCoord="36" yCoord="661"/>
</arc>
<arc id="P1 to T1" inscription="[0,inf)" source="P1" target="T1"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="49" yCoord="129"/>
<arcpath arcPointType="false" id="1" xCoord="67" yCoord="157"/>
</arc>
<arc id="T3 to P8" inscription="1" source="T3" target="P8"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="242" yCoord="161"/>
<arcpath arcPointType="false" id="1" xCoord="267" yCoord="161"/>
</arc>
<arc id="P8 to T4" inscription="[0,inf)" source="P8" target="T4"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="296" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="321" yCoord="162"/>
</arc>
<arc id="T4 to P9" inscription="1" source="T4" target="P9"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="331" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="357" yCoord="162"/>
</arc>
<arc id="T17 to P27" inscription="1" source="T20" target="P32"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="231" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="206" yCoord="402"/>
</arc>
<arc id="P27 to T18" inscription="[0,inf)" source="P32" target="T21"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="177" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="151" yCoord="402"/>
</arc>
<arc id="P10 to T6" inscription="[0,inf)" source="P10" target="T6"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="476" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="501" yCoord="162"/>
</arc>
<arc id="Decrypt to MSG1" inscription="1" source="T9" target="P16"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="751" yCoord="162"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="777" yCoord="162"/>
</arc>
<arc id="P14 to T9" inscription="[0,inf)" source="P15" target="T9"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="747" yCoord="207"/>
<arcpath arcPointType="false" id="1" xCoord="747" yCoord="177"/>
</arc>
<arc id="P13 to T9" inscription="[0,inf)" source="P14" target="T9"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="731" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="741" yCoord="162"/>
</arc>
<arc id="T8 to P13" inscription="1" source="T8" target="P13"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="672" yCoord="147"/>
<arcpath arcPointType="false" id="1" xCoord="673" yCoord="103"/>
<arcpath arcPointType="false" id="2" xCoord="702" yCoord="102"/>
</arc>
<arc id="P15 to T14" inscription="[0,inf)" source="P15" target="T14"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="747" yCoord="237"/>
<arcpath arcPointType="false" id="1" xCoord="747" yCoord="342"/>
<arcpath arcPointType="false" id="2" xCoord="788" yCoord="341"/>
<arcpath arcPointType="false" id="3" xCoord="792" yCoord="387"/>
</arc>
<arc id="P25 to T15" inscription="[0,inf)" source="P25" target="T15"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="762" yCoord="460"/>
<arcpath arcPointType="false" id="1" xCoord="725" yCoord="458"/>
<arcpath arcPointType="false" id="2" xCoord="702" yCoord="417"/>
</arc>
<arc id="P26 to T16" inscription="[0,inf)" source="P26" target="T16"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="627" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="601" yCoord="402"/>
</arc>
<arc id="P28 to T18" inscription="[0,inf)" source="P28" target="T18"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="447" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="421" yCoord="402"/>
</arc>
<arc id="T18 to P29" inscription="1" source="T18" target="P29"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="411" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="386" yCoord="402"/>
</arc>
<arc id="T20 to P31" inscription="1" source="T20" target="P31"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="237" yCoord="387"/>
<arcpath arcPointType="false" id="1" xCoord="228" yCoord="336"/>
<arcpath arcPointType="false" id="2" xCoord="191" yCoord="329"/>
</arc>
```

```
<arc id="T17 to P28" inscription="1" source="T17" target="P28"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="501" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="476" yCoord="402"/>
</arc>
<arc id="P27 to T17" inscription="[0,inf)" source="P27" target="T17"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="537" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="511" yCoord="402"/>
</arc>
<arc id="T27 to P40" inscription="1" source="T27" target="P40"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="241" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="267" yCoord="657"/>
</arc>
<arc id="P40 to T28" inscription="[0,inf)" source="P40" target="T28"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="296" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="321" yCoord="657"/>
</arc>
<arc id="T28 to P41" inscription="1" source="T28" target="P41"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="331" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="357" yCoord="657"/>
</arc>
<arc id="P41 to T29" inscription="[0,inf)" source="P41" target="T29"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="386" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="411" yCoord="657"/>
</arc>
<arc id="T29 to P42" inscription="1" source="T29" target="P42"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="421" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="447" yCoord="657"/>
</arc>
<arc id="T32 to P45" inscription="1" source="T32" target="P45"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="687" yCoord="642"/>
<arcpath arcPointType="false" id="1" xCoord="688" yCoord="613"/>
<arcpath arcPointType="false" id="2" xCoord="717" yCoord="602"/>
</arc>
<arc id="P38 to T26" inscription="[0,inf)" source="P38" target="T26"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="116" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="141" yCoord="657"/>
</arc>
<arc id="T26 to P39" inscription="1" source="T26" target="P39"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="151" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="177" yCoord="657"/>
</arc>
```

```
<arc id="P39 to T27" inscription="[0,inf)" source="P39" target="T27"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="206" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="231" yCoord="657"/>
</arc>
<arc id="P46 to T33" inscription="[0,inf)" source="P46" target="T33"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="746" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="771" yCoord="657"/>
</arc>
<arc id="T33 to P47" inscription="1" source="T33" target="P47"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="781" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="807" yCoord="657"/>
</arc>
<arc id="P47 to T34" inscription="[0,inf)" source="P47" target="T34"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="836" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="861" yCoord="657"/>
</arc>
<arc id="P50 to T37" inscription="[0,inf)" source="P50" target="T37"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="852" yCoord="867"/>
<arcpath arcPointType="false" id="1" xCoord="736" yCoord="867"/>
</arc>
<arc id="T37 to P51" inscription="1" source="T37" target="P51"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="726" yCoord="867"/>
<arcpath arcPointType="false" id="1" xCoord="686" yCoord="867"/>
</arc>
<arc id="P23 to T14" inscription="[0,inf)" source="P23" target="T14"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="852" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="796" yCoord="402"/>
</arc>
<arc id="T6 to P11" inscription="1" source="T6" target="P11"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="511" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="537" yCoord="162"/>
</arc>
<arc id="P11 to T7" inscription="[0,inf)" source="P11" target="T7"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="566" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="591" yCoord="162"/>
</arc>
<arc id="T7 to P12" inscription="1" source="T7" target="P12"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="601" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="627" yCoord="162"/>
</arc>
<arc id="T16 to P27" inscription="1" source="T16" target="P27"
type="normal" weight="1">
```

```
<arcpath arcPointType="false" id="0" xCoord="591" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="566" yCoord="402"/>
</arc>
<arc id="P29 to T19" inscription="[0,inf)" source="P29" target="T19"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="357" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="331" yCoord="402"/>
</arc>
<arc id="T19 to P30" inscription="1" source="T19" target="P30"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="321" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="296" yCoord="402"/>
</arc>
<arc id="P30 to T20" inscription="[0,inf)" source="P30" target="T20"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="267" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="241" yCoord="402"/>
</arc>
<arc id="P43 to T31" inscription="[0,inf)" source="P43" target="T31"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="566" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="591" yCoord="657"/>
</arc>
<arc id="T31 to P44" inscription="1" source="T31" target="P44"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="601" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="627" yCoord="657"/>
</arc>
<arc id="P44 to T32" inscription="[0,inf)" source="P44" target="T32"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="656" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="681" yCoord="657"/>
</arc>
<arc id="T16 to P29" inscription="1" source="T23" target="P35"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="281" yCoord="496"/>
<arcpath arcPointType="false" id="1" xCoord="281" yCoord="552"/>
</arc>
<arc id="P28 to T16" inscription="[Deadline,Deadline]" source="P34"
target="T23" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="176" yCoord="492"/>
<arcpath arcPointType="false" id="1" xCoord="266" yCoord="492"/>
</arc>
<arc id="P15 to T33" inscription="[0,inf)" source="P15" target="T33"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="761" yCoord="222"/>
<arcpath arcPointType="false" id="1" xCoord="928" yCoord="223"/>
<arcpath arcPointType="false" id="2" xCoord="928" yCoord="583"/>
<arcpath arcPointType="false" id="3" xCoord="778" yCoord="583"/>
<arcpath arcPointType="false" id="4" xCoord="777" yCoord="642"/>
</arc>
```

```
<arc id="P5 to T2" inscription="[0,inf)" source="P5" target="T2"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="132" yCoord="222"/>
<arcpath arcPointType="false" id="1" xCoord="133" yCoord="193"/>
<arcpath arcPointType="false" id="2" xCoord="147" yCoord="177"/>
</arc>
<arc id="P7 to T3" inscription="[0,inf)" source="P7" target="T3"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="192" yCoord="222"/>
<arcpath arcPointType="false" id="1" xCoord="193" yCoord="193"/>
<arcpath arcPointType="false" id="2" xCoord="231" yCoord="166"/>
</arc>
<arc id="P5 to T21" inscription="[0,inf)" source="P5" target="T21"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="132" yCoord="251"/>
<arcpath arcPointType="false" id="1" xCoord="133" yCoord="358"/>
<arcpath arcPointType="false" id="2" xCoord="147" yCoord="387"/>
</arc>
<arc id="P5 to T26" inscription="[0,inf)" source="P5" target="T26"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="117" yCoord="237"/>
<arcpath arcPointType="false" id="1" xCoord="13" yCoord="238"/>
<arcpath arcPointType="false" id="2" xCoord="13" yCoord="703"/>
<arcpath arcPointType="false" id="3" xCoord="133" yCoord="703"/>
<arcpath arcPointType="false" id="4" xCoord="147" yCoord="672"/>
</arc>
<arc id="P7 to T27" inscription="[0,inf)" source="P7" target="T27"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="192" yCoord="251"/>
<arcpath arcPointType="false" id="1" xCoord="193" yCoord="283"/>
<arcpath arcPointType="false" id="2" xCoord="13" yCoord="283"/>
<arcpath arcPointType="false" id="3" xCoord="13" yCoord="718"/>
<arcpath arcPointType="false" id="4" xCoord="208" yCoord="718"/>
<arcpath arcPointType="false" id="5" xCoord="237" yCoord="672"/>
</arc>
</net>
<query active="true" approximationDenominator="2" capacity="0"
discreteInclusion="false" enableOverApproximation="false"
enableUnderApproximation="false" extrapolationOption="AUTOMATIC"
gcd="true" hashTableSize="MB_16" inclusionPlaces="*NONE*"
name="Query Comment/Name Here" overApproximation="true" pTrie="true"
query="EF true" reduction="true" reductionOption="VerifyTAPN"
searchOption="HEURISTIC" symmetry="true" timeDarts="true"
traceOption="NONE"/>
<k-bound bound="3"/>
</pnml>
```

Man-in-the-Middle Attack

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<pnml xmlns="http://www.informatik.hu-berlin.de/top/pnml/ptNetb">
<constant name="periodC" value="7"/>
<constant name="PeriodS" value="5"/>
<constant name="Deadline" value="5"/>
<net active="true" id="TAPN1" type="P/T net">
<place id="P1" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P1"
nameOffsetX="22.0" nameOffsetY="-4.0" positionX="45.0"
positionY="105.0"/>
<place id="P2" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P2"
nameOffsetX="17.0" nameOffsetY="-4.0" positionX="45.0"
positionY="150.0"/>
<place id="P4" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P4"
nameOffsetX="25.0" nameOffsetY="-5.0" positionX="150.0"
positionY="150.0"/>
<place id="P5" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P5"
nameOffsetX="23.0" nameOffsetY="-4.0" positionX="270.0"
positionY="150.0"/>
<place id="P11" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P11"
nameOffsetX="26.0" nameOffsetY="-3.0" positionX="675.0"
positionY="120.0"/>
<place id="P14" initialMarking="0" invariant="&lt;= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P14"
nameOffsetX="67.0" nameOffsetY="-20.0" positionX="840.0"
positionY="60.0"/>
<place id="P15" initialMarking="0" invariant="&lt; Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P15"
nameOffsetX="76.0" nameOffsetY="-20.0" positionX="840.0"
positionY="240.0"/>
<place id="P16" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P16"
nameOffsetX="29.0" nameOffsetY="-3.0" positionX="870.0"
positionY="315.0"/>
<place id="P18" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P18"
nameOffsetX="18.0" nameOffsetY="0.0" positionX="735.0"
positionY="270.0"/>
<place id="P20" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P20"
```

```
nameOffsetX="21.0" nameOffsetY="7.0" positionX="675.0"
positionY="360.0"/>
<place id="P22" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P22"
nameOffsetX="34.0" nameOffsetY="0.0" positionX="555.0"
positionY="360.0"/>
<place id="P27" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P27"
nameOffsetX="30.0" nameOffsetY="-1.0" positionX="165.0"
positionY="390.0"/>
<place id="P28" initialMarking="0" invariant="&lt;= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P28"
nameOffsetX="100.0" nameOffsetY="-14.0" positionX="60.0"
positionY="390.0"/>
<place id="P30" initialMarking="0" invariant="&lt; Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P30"
nameOffsetX="114.0" nameOffsetY="5.0" positionX="60.0"
positionY="525.0"/>
<place id="P17" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P17"
nameOffsetX="32.0" nameOffsetY="-4.0" positionX="870.0"
positionY="375.0"/>
<place id="P3" initialMarking="1" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P3"
nameOffsetX="11.0" nameOffsetY="3.0" positionX="45.0"
positionY="195.0"/>
<place id="P31" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P31"
nameOffsetX="28.0" nameOffsetY="1.0" positionX="120.0"
positionY="570.0"/>
<place id="P32" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P32"
nameOffsetX="24.0" nameOffsetY="-2.0" positionX="150.0"
positionY="600.0"/>
<place id="P26" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P26"
nameOffsetX="22.0" nameOffsetY="-6.0" positionX="270.0"
positionY="390.0"/>
<place id="P36" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P36"
nameOffsetX="34.0" nameOffsetY="-7.0" positionX="675.0"
positionY="600.0"/>
<place id="P38" initialMarking="0" invariant="&lt;= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P38"
nameOffsetX="79.0" nameOffsetY="-21.0" positionX="855.0"
positionY="510.0"/>
<place id="P39" initialMarking="0" invariant="&lt; Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P39"
nameOffsetX="63.0" nameOffsetY="-19.0" positionX="870.0"
positionY="690.0"/>
<place id="P6" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P6"
```

nameOffsetX="19.0" nameOffsetY="-6.0" positionX="375.0"
positionY="150.0"/>
<place id="P7" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P7"
nameOffsetX="13.0" nameOffsetY="-4.0" positionX="420.0"
positionY="150.0"/>
<place id="P24" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P24"
nameOffsetX="11.0" nameOffsetY="7.0" positionX="420.0"
positionY="315.0"/>
<place id="P19" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P19"
nameOffsetX="19.0" nameOffsetY="-4.0" positionX="690.0"
positionY="300.0"/>
<place id="P21" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P21"
nameOffsetX="33.0" nameOffsetY="45.0" positionX="675.0"
positionY="420.0"/>
<place id="P23" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P23"
nameOffsetX="25.0" nameOffsetY="50.0" positionX="555.0"
positionY="420.0"/>
<place id="P25" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P25"
nameOffsetX="19.0" nameOffsetY="-4.0" positionX="405.0"
positionY="390.0"/>
<place id="P33" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P33"
nameOffsetX="27.0" nameOffsetY="-7.0" positionX="270.0"
positionY="600.0"/>
<place id="P34" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P34"
nameOffsetX="35.0" nameOffsetY="-4.0" positionX="420.0"
positionY="600.0"/>
<place id="P35" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P35"
nameOffsetX="25.0" nameOffsetY="-1.0" positionX="555.0"
positionY="600.0"/>
<place id="P10" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P10"
nameOffsetX="35.0" nameOffsetY="50.0" positionX="555.0"
positionY="180.0"/>
<place id="P12" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P12"
nameOffsetX="24.0" nameOffsetY="42.0" positionX="675.0"
positionY="180.0"/>
<place id="P8" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P8"
nameOffsetX="34.0" nameOffsetY="43.0" positionX="450.0"
positionY="180.0"/>
<place id="P9" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P9"

nameOffsetX="17.0" nameOffsetY="-7.0" positionX="555.0"
positionY="120.0"/>
<place id="P29" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P29"
nameOffsetX="126.0" nameOffsetY="14.0" positionX="60.0"
positionY="255.0"/>
<place id="P37" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P37"
nameOffsetX="122.0" nameOffsetY="7.0" positionX="795.0"
positionY="600.0"/>
<place id="P13" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P13"
nameOffsetX="114.0" nameOffsetY="4.0" positionX="780.0"
positionY="150.0"/>
<transition angle="0" id="T1" infiniteServer="false" name="T1"
nameOffsetX="30.0" nameOffsetY="51.0" positionX="105.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T2" infiniteServer="false" name="T2"
nameOffsetX="19.0" nameOffsetY="50.0" positionX="210.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T6" infiniteServer="false" name="T6"
nameOffsetX="34.0" nameOffsetY="47.0" positionX="615.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T7" infiniteServer="false" name="T7"
nameOffsetX="15.0" nameOffsetY="52.0" positionX="735.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T10" infiniteServer="false" name="T10"
nameOffsetX="28.0" nameOffsetY="45.0" positionX="765.0"
positionY="360.0" priority="0" urgent="false"/>
<transition angle="0" id="T11" infiniteServer="false" name="T11"
nameOffsetX="45.0" nameOffsetY="46.0" positionX="615.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T14" infiniteServer="false" name="T14"
nameOffsetX="10.0" nameOffsetY="52.0" positionX="210.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T15" infiniteServer="false" name="T15"
nameOffsetX="35.0" nameOffsetY="45.0" positionX="120.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="180" id="T18" infiniteServer="false" name="T18"
nameOffsetX="27.0" nameOffsetY="50.0" positionX="60.0"
positionY="600.0" priority="0" urgent="false"/>
<transition angle="0" id="T19" infiniteServer="false" name="T19"
nameOffsetX="16.0" nameOffsetY="49.0" positionX="210.0"
positionY="600.0" priority="0" urgent="false"/>
<transition angle="0" id="T22" infiniteServer="false" name="T22"
nameOffsetX="41.0" nameOffsetY="43.0" positionX="615.0"
positionY="600.0" priority="0" urgent="false"/>
<transition angle="0" id="T23" infiniteServer="false" name="T23"
nameOffsetX="19.0" nameOffsetY="47.0" positionX="735.0"
positionY="600.0" priority="0" urgent="false"/>

```
<transition angle="180" id="T3" infiniteServer="false" name="T3"
nameOffsetX="34.0" nameOffsetY="47.0" positionX="330.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="180" id="T4" infiniteServer="false" name="T4"
nameOffsetX="37.0" nameOffsetY="44.0" positionX="375.0"
positionY="225.0" priority="0" urgent="false"/>
<transition angle="0" id="T5" infiniteServer="false" name="T5"
nameOffsetX="14.0" nameOffsetY="47.0" positionX="495.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T12" infiniteServer="false" name="T12"
nameOffsetX="16.0" nameOffsetY="45.0" positionX="495.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T13" infiniteServer="false" name="T13"
nameOffsetX="43.0" nameOffsetY="43.0" positionX="330.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T20" infiniteServer="false" name="T20"
nameOffsetX="50.0" nameOffsetY="50.0" positionX="330.0"
positionY="600.0" priority="0" urgent="false"/>
<transition angle="0" id="T21" infiniteServer="false" name="T21"
nameOffsetX="18.0" nameOffsetY="46.0" positionX="495.0"
positionY="600.0" priority="0" urgent="false"/>
<transition angle="90" id="T17" infiniteServer="false" name="T17"
nameOffsetX="54.0" nameOffsetY="28.0" positionX="60.0"
positionY="465.0" priority="0" urgent="false"/>
<transition angle="90" id="T16" infiniteServer="false" name="T16"
nameOffsetX="56.0" nameOffsetY="30.0" positionX="60.0"
positionY="300.0" priority="0" urgent="false"/>
<transition angle="0" id="T24" infiniteServer="false" name="T24"
nameOffsetX="11.0" nameOffsetY="-1.0" positionX="795.0"
positionY="510.0" priority="0" urgent="false"/>
<transition angle="0" id="T25" infiniteServer="false" name="T25"
nameOffsetX="13.0" nameOffsetY="40.0" positionX="795.0"
positionY="690.0" priority="0" urgent="false"/>
<transition angle="0" id="T8" infiniteServer="false" name="T8"
nameOffsetX="11.0" nameOffsetY="2.0" positionX="780.0"
positionY="60.0" priority="0" urgent="false"/>
<transition angle="0" id="T9" infiniteServer="false" name="T9"
nameOffsetX="35.0" nameOffsetY="38.0" positionX="780.0"
positionY="240.0" priority="0" urgent="false"/>
<arc id="Tc to generateLoginRequest" inscription="[0,inf)"
source="P2" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="71" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="111" yCoord="163"/>
</arc>
<arc id="Rc to generateLoginRequest" inscription="[0,inf)"
source="P1" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="69" yCoord="125"/>
<arcpath arcPointType="false" id="1" xCoord="112" yCoord="156"/>
</arc>
<arc id="generateLoginRequest to LgoinRqst" inscription="1"
source="T1" target="P4" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="121" yCoord="162"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="147" yCoord="162"/>
</arc>
<arc id="LgoinRqst to Encrypt" inscription="[0,inf)" source="P4"
target="T2" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="176" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="216" yCoord="162"/>
</arc>
<arc id="Encrypt to Cipher1" inscription="1" source="T2" target="P5"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="226" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="267" yCoord="162"/>
</arc>
<arc id="Decrypt to MSG1" inscription="1" source="T6" target="P11"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="632" yCoord="157"/>
<arcpath arcPointType="false" id="1" xCoord="673" yCoord="138"/>
</arc>
<arc id="MSG1 to T4" inscription="[0,inf)" source="P11" target="T7"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="700" yCoord="138"/>
<arcpath arcPointType="false" id="1" xCoord="742" yCoord="157"/>
</arc>
<arc id="Rs to T6" inscription="[0,inf)" source="P16" target="T10"
type="timed" weight="2">
<arcpath arcPointType="false" id="0" xCoord="870" yCoord="337"/>
<arcpath arcPointType="false" id="1" xCoord="843" yCoord="363"/>
<arcpath arcPointType="false" id="2" xCoord="782" yCoord="371"/>
</arc>
<arc id="Accept to T6" inscription="[0,inf)" source="P15"
target="T10" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="852" yCoord="266"/>
<arcpath arcPointType="false" id="1" xCoord="854" yCoord="324"/>
<arcpath arcPointType="false" id="2" xCoord="782" yCoord="364"/>
</arc>
<arc id="T6 to SK_s" inscription="1" source="T10" target="P18"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="777" yCoord="357"/>
<arcpath arcPointType="false" id="1" xCoord="764" yCoord="339"/>
<arcpath arcPointType="false" id="2" xCoord="751" yCoord="296"/>
</arc>
<arc id="T6 to SYN_ACK" inscription="1" source="T10" target="P20"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="771" yCoord="373"/>
<arcpath arcPointType="false" id="1" xCoord="741" yCoord="388"/>
<arcpath arcPointType="false" id="2" xCoord="701" yCoord="376"/>
</arc>
<arc id="SYN_ACK to Encrypt_" inscription="[0,inf)" source="P20"
target="T11" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="673" yCoord="378"/>
<arcpath arcPointType="false" id="1" xCoord="632" yCoord="397"/>
</arc>
```

<arc id="Decrypt_ to MSG2" inscription="1" source="T14" target="P27"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="216" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="191" yCoord="402"/>
</arc>
<arc id="MSG2 to T9" inscription="[0,inf)" source="P27" target="T15"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="162" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="136" yCoord="402"/>
</arc>
<arc id="T9 to Reject2" inscription="1" source="T15" target="P28"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="126" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="86" yCoord="402"/>
</arc>
<arc id="Ts to T6" inscription="[0,inf)" source="P17" target="T10"
type="timed" weight="2">
<arcpath arcPointType="false" id="0" xCoord="867" yCoord="385"/>
<arcpath arcPointType="false" id="1" xCoord="848" yCoord="384"/>
<arcpath arcPointType="false" id="2" xCoord="781" yCoord="378"/>
</arc>
<arc id="Requst to generateLoginRequest" inscription="[0,inf)"
source="P3" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="71" yCoord="204"/>
<arcpath arcPointType="false" id="1" xCoord="95" yCoord="200"/>
<arcpath arcPointType="false" id="2" xCoord="111" yCoord="170"/>
</arc>
<arc id="Rc to T12" inscription="[0,inf)" source="P1" target="T18"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="42" yCoord="118"/>
<arcpath arcPointType="false" id="1" xCoord="5" yCoord="123"/>
<arcpath arcPointType="false" id="2" xCoord="5" yCoord="618"/>
<arcpath arcPointType="false" id="3" xCoord="66" yCoord="616"/>
</arc>
<arc id="Tc to T12" inscription="[0,inf)" source="P2" target="T18"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="67" yCoord="172"/>
<arcpath arcPointType="false" id="1" xCoord="63" yCoord="168"/>
<arcpath arcPointType="false" id="2" xCoord="18" yCoord="168"/>
<arcpath arcPointType="false" id="3" xCoord="18" yCoord="603"/>
<arcpath arcPointType="false" id="4" xCoord="67" yCoord="606"/>
</arc>
<arc id="T12 to SK_c" inscription="1" source="T18" target="P31"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="77" yCoord="606"/>
<arcpath arcPointType="false" id="1" xCoord="108" yCoord="603"/>
<arcpath arcPointType="false" id="2" xCoord="120" yCoord="591"/>
</arc>
<arc id="T12 to ACK" inscription="1" source="T18" target="P32"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="76" yCoord="616"/>
<arcpath arcPointType="false" id="1" xCoord="147" yCoord="612"/>

```
</arc>
<arc id="ACK to _Encrypt" inscription="[0,inf)" source="P32"
target="T19" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="176" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="216" yCoord="612"/>
</arc>
<arc id="_Decrypt to MSG3" inscription="1" source="T22" target="P36"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="631" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="672" yCoord="612"/>
</arc>
<arc id="MSG3 to T15" inscription="[0,inf)" source="P36"
target="T23" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="701" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="741" yCoord="612"/>
</arc>
<arc id="Cipher1 to Receive_Cipher1" inscription="[0,inf)"
source="P5" target="T3" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="296" yCoord="161"/>
<arcpath arcPointType="false" id="1" xCoord="337" yCoord="161"/>
</arc>
<arc id="Receive_Cipher1 to XCipher1X" inscription="1" source="T3"
target="P6" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="347" yCoord="161"/>
<arcpath arcPointType="false" id="1" xCoord="372" yCoord="161"/>
</arc>
<arc id="FakeMSG to Encrypt__" inscription="[0,inf)" source="P7"
target="T5" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="446" yCoord="161"/>
<arcpath arcPointType="false" id="1" xCoord="502" yCoord="157"/>
</arc>
<arc id="Encrypt_ to Cipher2" inscription="1" source="T11"
target="P22" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="622" yCoord="397"/>
<arcpath arcPointType="false" id="1" xCoord="580" yCoord="378"/>
</arc>
<arc id="Cipher2 to T20" inscription="[0,inf)" source="P22"
target="T12" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="553" yCoord="378"/>
<arcpath arcPointType="false" id="1" xCoord="512" yCoord="397"/>
</arc>
<arc id="T20 to P9" inscription="1" source="T12" target="P24"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="502" yCoord="397"/>
<arcpath arcPointType="false" id="1" xCoord="434" yCoord="374"/>
<arcpath arcPointType="false" id="2" xCoord="432" yCoord="341"/>
</arc>
<arc id="Compute to A_SK" inscription="1" source="T10" target="P19"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="772" yCoord="366"/>
<arcpath arcPointType="false" id="1" xCoord="741" yCoord="358"/>
<arcpath arcPointType="false" id="2" xCoord="711" yCoord="323"/>
```

```
</arc>
<arc id="Compute to SYNACK_A" inscription="1" source="T10"
target="P21" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="771" yCoord="380"/>
<arcpath arcPointType="false" id="1" xCoord="742" yCoord="432"/>
<arcpath arcPointType="false" id="2" xCoord="702" yCoord="432"/>
</arc>
<arc id="SYNACK_A to SendMSG_" inscription="[0,inf)" source="P21"
target="T11" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="673" yCoord="425"/>
<arcpath arcPointType="false" id="1" xCoord="631" yCoord="407"/>
</arc>
<arc id="SendMSG_ to MSG2_A" inscription="1" source="T11"
target="P23" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="621" yCoord="407"/>
<arcpath arcPointType="false" id="1" xCoord="580" yCoord="425"/>
</arc>
<arc id="MSG2_A to Intercept_MSG_" inscription="[0,inf)"
source="P23" target="T12" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="553" yCoord="425"/>
<arcpath arcPointType="false" id="1" xCoord="511" yCoord="407"/>
</arc>
<arc id="Intercept_MSG_ to MSG2_A_" inscription="1" source="T12"
target="P25" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="501" yCoord="407"/>
<arcpath arcPointType="false" id="1" xCoord="431" yCoord="403"/>
</arc>
<arc id="MSG2_A_ to _SendMSG_" inscription="[0,inf)" source="P25"
target="T13" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="402" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="346" yCoord="402"/>
</arc>
<arc id="_SendMSG_ to SYN_ACK" inscription="1" source="T13"
target="P26" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="336" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="296" yCoord="402"/>
</arc>
<arc id="Accept2 to T12" inscription="[0,inf)" source="P30"
target="T18" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="71" yCoord="551"/>
<arcpath arcPointType="false" id="1" xCoord="71" yCoord="596"/>
</arc>
<arc id="SYN_ACK to RecieveMSG2" inscription="[0,inf)" source="P26"
target="T14" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="267" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="226" yCoord="402"/>
</arc>
<arc id="SendMSG3 to MSG3_" inscription="1" source="T19"
target="P33" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="226" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="267" yCoord="612"/>
</arc>
```

<arc id="MSG3_ to Intercept_MSG3" inscription="[0,inf)" source="P33"
target="T20" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="296" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="336" yCoord="612"/>
</arc>
<arc id="Intercept_MSG3 to xMSG3x" inscription="1" source="T20"
target="P34" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="346" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="417" yCoord="612"/>
</arc>
<arc id="xMSG3x to SendMSG3_" inscription="[0,inf)" source="P34"
target="T21" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="446" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="501" yCoord="612"/>
</arc>
<arc id="SendMSG3_ to XMSG3X_" inscription="1" source="T21"
target="P35" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="511" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="552" yCoord="612"/>
</arc>
<arc id="XMSG3X_ to _ReceiveMSG3" inscription="[0,inf)" source="P35"
target="T22" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="581" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="621" yCoord="612"/>
</arc>
<arc id="MSG1_C to ReceiveMSG" inscription="[0,inf)" source="P10"
target="T6" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="580" yCoord="185"/>
<arcpath arcPointType="false" id="1" xCoord="621" yCoord="167"/>
</arc>
<arc id="ReceiveMSG to MSG1_C_" inscription="1" source="T6"
target="P12" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="631" yCoord="167"/>
<arcpath arcPointType="false" id="1" xCoord="673" yCoord="185"/>
</arc>
<arc id="MSG1_C_ to Verify_" inscription="[0,inf)" source="P12"
target="T7" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="700" yCoord="185"/>
<arcpath arcPointType="false" id="1" xCoord="741" yCoord="167"/>
</arc>
<arc id="XMSG1X to DuplicateMSG" inscription="[0,inf)" source="P6"
target="T4" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="386" yCoord="176"/>
<arcpath arcPointType="false" id="1" xCoord="386" yCoord="221"/>
</arc>
<arc id="DuplicateMSG to xMSG1_A" inscription="1" source="T4"
target="P7" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="392" yCoord="231"/>
<arcpath arcPointType="false" id="1" xCoord="421" yCoord="226"/>
<arcpath arcPointType="false" id="2" xCoord="429" yCoord="176"/>
</arc>

```
<arc id="DuplicateMSG to xMSG1_C" inscription="1" source="T4"
target="P8" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="391" yCoord="241"/>
<arcpath arcPointType="false" id="1" xCoord="436" yCoord="241"/>
<arcpath arcPointType="false" id="2" xCoord="454" yCoord="205"/>
</arc>
<arc id="xMSG1_C to Send_MSG" inscription="[0,inf)" source="P8"
target="T5" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="474" yCoord="184"/>
<arcpath arcPointType="false" id="1" xCoord="501" yCoord="167"/>
</arc>
<arc id="Cipher1_i to Decrypt" inscription="[0,inf)" source="P9"
target="T6" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="580" yCoord="138"/>
<arcpath arcPointType="false" id="1" xCoord="622" yCoord="157"/>
</arc>
<arc id="Encrypt__ to Cipher1_i" inscription="1" source="T5"
target="P9" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="512" yCoord="157"/>
<arcpath arcPointType="false" id="1" xCoord="553" yCoord="138"/>
</arc>
<arc id="P28 to T16" inscription="[Deadline,Deadline]" source="P28"
target="T16" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="71" yCoord="387"/>
<arcpath arcPointType="false" id="1" xCoord="71" yCoord="316"/>
</arc>
<arc id="T16 to P29" inscription="1" source="T16" target="P29"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="71" yCoord="306"/>
<arcpath arcPointType="false" id="1" xCoord="71" yCoord="281"/>
</arc>
<arc id="P28 to T17" inscription="[0,Deadline]:1" source="P28"
target="T17" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="71" yCoord="416"/>
<arcpath arcPointType="false" id="1" xCoord="71" yCoord="471"/>
</arc>
<arc id="T17 to P30" inscription="[0,Deadline]:1" source="T17"
target="P30" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="71" yCoord="481"/>
<arcpath arcPointType="false" id="1" xCoord="71" yCoord="522"/>
</arc>
<arc id="P37 to T24" inscription="[Deadline,Deadline]" source="P37"
target="T24" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="807" yCoord="597"/>
<arcpath arcPointType="false" id="1" xCoord="807" yCoord="529"/>
<arcpath arcPointType="false" id="2" xCoord="807" yCoord="537"/>
</arc>
<arc id="T24 to P38" inscription="1" source="T24" target="P38"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="811" yCoord="522"/>
<arcpath arcPointType="false" id="1" xCoord="852" yCoord="522"/>
</arc>
```

<arc id="P37 to T25" inscription="[0,Deadline]:1" source="P37"
target="T25" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="807" yCoord="626"/>
<arcpath arcPointType="false" id="1" xCoord="807" yCoord="687"/>
</arc>
<arc id="T25 to P39" inscription="[0,Deadline]:1" source="T25"
target="P39" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="811" yCoord="702"/>
<arcpath arcPointType="false" id="1" xCoord="867" yCoord="702"/>
</arc>
<arc id="T23 to P37" inscription="1" source="T23" target="P37"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="751" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="792" yCoord="612"/>
</arc>
<arc id="T7 to P13" inscription="1" source="T7" target="P13"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="751" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="777" yCoord="162"/>
</arc>
<arc id="P13 to T8" inscription="[Deadline,Deadline]" source="P13"
target="T8" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="792" yCoord="147"/>
<arcpath arcPointType="false" id="1" xCoord="792" yCoord="87"/>
</arc>
<arc id="T8 to P14" inscription="1" source="T8" target="P14"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="796" yCoord="72"/>
<arcpath arcPointType="false" id="1" xCoord="837" yCoord="72"/>
</arc>
<arc id="P13 to T9" inscription="[0,Deadline]:1" source="P13"
target="T9" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="792" yCoord="176"/>
<arcpath arcPointType="false" id="1" xCoord="792" yCoord="237"/>
</arc>
<arc id="T9 to P15" inscription="[0,Deadline]:1" source="T9"
target="P15" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="796" yCoord="252"/>
<arcpath arcPointType="false" id="1" xCoord="837" yCoord="252"/>
</arc>
<arc id="Send_MSG to MSG1_C" inscription="1" source="T5"
target="P10" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="511" yCoord="167"/>
<arcpath arcPointType="false" id="1" xCoord="553" yCoord="185"/>
</arc>
</net>
<query active="true" approximationDenominator="2" capacity="0"
discreteInclusion="false" enableOverApproximation="false"
enableUnderApproximation="false" extrapolationOption="AUTOMATIC"
gcd="true" hashTableSize="MB_16" inclusionPlaces="*NONE*"
name="Query Comment/Name Here" overApproximation="true" pTrie="true"
query="EF true" reduction="true" reductionOption="VerifyTAPN"

```
searchOption="HEURISTIC" symmetry="true" timeDarts="true"
traceOption="NONE"/>
<k-bound bound="3"/>
</pnml>
```

Reflection Attack

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<pnml xmlns="http://www.informatik.hu-berlin.de/top/pnml/ptNetb">
<constant name="periodC" value="7"/>
<constant name="PeriodS" value="5"/>
<constant name="Deadline" value="5"/>
<net active="true" id="TAPN1" type="P/T net">
<labels border="false" height="20" positionX="125" positionY="24"
width="77">Client-Side</labels>
<labels border="false" height="35" positionX="801" positionY="55"
width="77">Server-Side</labels>
<labels border="false" height="17" positionX="368" positionY="28"
width="134">          Intruder</labels>
<place id="P1" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P1"
nameOffsetX="22.0" nameOffsetY="-4.0" positionX="45.0"
positionY="105.0"/>
<place id="P2" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P2"
nameOffsetX="17.0" nameOffsetY="-4.0" positionX="45.0"
positionY="150.0"/>
<place id="P4" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P4"
nameOffsetX="25.0" nameOffsetY="-6.0" positionX="225.0"
positionY="150.0"/>
<place id="P5" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P5"
nameOffsetX="29.0" nameOffsetY="2.0" positionX="375.0"
positionY="150.0"/>
<place id="P13" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P13"
nameOffsetX="41.0" nameOffsetY="-6.0" positionX="255.0"
positionY="435.0"/>
<place id="P3" initialMarking="1" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P3"
nameOffsetX="11.0" nameOffsetY="3.0" positionX="45.0"
positionY="210.0"/>
<place id="P14" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P14"
nameOffsetX="27.0" nameOffsetY="-5.0" positionX="255.0"
positionY="510.0"/>
<place id="P6" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P6"
nameOffsetX="36.0" nameOffsetY="-1.0" positionX="510.0"
positionY="150.0"/>
```

<place id="P9" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P9"
nameOffsetX="26.0" nameOffsetY="-6.0" positionX="255.0"
positionY="255.0"/>
<place id="P7" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P7"
nameOffsetX="32.0" nameOffsetY="4.0" positionX="510.0"
positionY="255.0"/>
<place id="P8" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P8"
nameOffsetX="26.0" nameOffsetY="-1.0" positionX="375.0"
positionY="255.0"/>
<place id="P10" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P10"
nameOffsetX="127.0" nameOffsetY="5.0" positionX="195.0"
positionY="345.0"/>
<place id="P16" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P16"
nameOffsetX="26.0" nameOffsetY="2.0" positionX="510.0"
positionY="510.0"/>
<place id="P15" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P15"
nameOffsetX="31.0" nameOffsetY="-5.0" positionX="375.0"
positionY="510.0"/>
<place id="P11" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P11"
nameOffsetX="118.0" nameOffsetY="-2.0" positionX="45.0"
positionY="270.0"/>
<place id="P12" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P12"
nameOffsetX="75.0" nameOffsetY="-15.0" positionX="60.0"
positionY="435.0"/>
<transition angle="0" id="T1" infiniteServer="false" name="T1"
nameOffsetX="26.0" nameOffsetY="49.0" positionX="135.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T2" infiniteServer="false" name="T2"
nameOffsetX="18.0" nameOffsetY="49.0" positionX="315.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="90" id="T7" infiniteServer="false" name="T7"
nameOffsetX="-7.0" nameOffsetY="20.0" positionX="195.0"
positionY="285.0" priority="0" urgent="false"/>
<transition angle="0" id="T6" infiniteServer="false" name="T6"
nameOffsetX="10.0" nameOffsetY="50.0" positionX="315.0"
positionY="255.0" priority="0" urgent="false"/>
<transition angle="0" id="T3" infiniteServer="false" name="T3"
nameOffsetX="30.0" nameOffsetY="46.0" positionX="435.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T5" infiniteServer="false" name="T5"
nameOffsetX="32.0" nameOffsetY="44.0" positionX="435.0"
positionY="255.0" priority="0" urgent="false"/>

```
<transition angle="0" id="T10" infiniteServer="false" name="T10"
nameOffsetX="26.0" nameOffsetY="46.0" positionX="60.0"
positionY="510.0" priority="0" urgent="false"/>
<transition angle="0" id="T11" infiniteServer="false" name="T11"
nameOffsetX="14.0" nameOffsetY="51.0" positionX="315.0"
positionY="510.0" priority="0" urgent="false"/>
<transition angle="0" id="T12" infiniteServer="false" name="T12"
nameOffsetX="50.0" nameOffsetY="42.0" positionX="435.0"
positionY="510.0" priority="0" urgent="false"/>
<transition angle="0" id="T8" infiniteServer="false" name="T8"
nameOffsetX="32.0" nameOffsetY="51.0" positionX="45.0"
positionY="345.0" priority="0" urgent="false"/>
<transition angle="0" id="T9" infiniteServer="false" name="T9"
nameOffsetX="23.0" nameOffsetY="48.0" positionX="195.0"
positionY="435.0" priority="0" urgent="false"/>
<transition angle="90" id="T4" infiniteServer="false" name="T4"
nameOffsetX="40.0" nameOffsetY="36.0" positionX="570.0"
positionY="210.0" priority="0" urgent="false"/>
<arc id="Tc to generateLoginRequest" inscription="[0,inf)"
source="P2" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="71" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="141" yCoord="163"/>
</arc>
<arc id="Rc to generateLoginRequest" inscription="[0,inf)"
source="P1" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="70" yCoord="123"/>
<arcpath arcPointType="false" id="1" xCoord="142" yCoord="156"/>
</arc>
<arc id="generateLoginRequest to LgoinRqst" inscription="1"
source="T1" target="P4" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="151" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="222" yCoord="162"/>
</arc>
<arc id="LgoinRqst to Encrypt" inscription="[0,inf)" source="P4"
target="T2" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="251" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="321" yCoord="162"/>
</arc>
<arc id="Encrypt to Cipher1" inscription="1" source="T2" target="P5"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="331" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="372" yCoord="162"/>
</arc>
<arc id="Requst to generateLoginRequest" inscription="[0,inf)"
source="P3" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="68" yCoord="211"/>
<arcpath arcPointType="false" id="1" xCoord="96" yCoord="186"/>
<arcpath arcPointType="false" id="2" xCoord="141" yCoord="170"/>
</arc>
<arc id="xMSG2x to SendMSG2" inscription="[0,inf)" source="P7"
target="T5" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="507" yCoord="267"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="451" yCoord="267"/>
</arc>
<arc id="SendMSG2 to Fake_SYNACK" inscription="1" source="T5"
target="P8" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="441" yCoord="267"/>
<arcpath arcPointType="false" id="1" xCoord="401" yCoord="267"/>
</arc>
<arc id="Login_MSG to Intercept_MSG" inscription="[0,inf)"
source="P5" target="T3" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="401" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="441" yCoord="162"/>
</arc>
<arc id="Intercept_MSG to LoginMSG_" inscription="1" source="T3"
target="P6" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="451" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="507" yCoord="162"/>
</arc>
<arc id="Verify_ to Accept" inscription="1" source="T7" target="P10"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="206" yCoord="301"/>
<arcpath arcPointType="false" id="1" xCoord="206" yCoord="342"/>
</arc>
<arc id="ReceiveMSG to _MSG2" inscription="1" source="T6"
target="P9" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="321" yCoord="267"/>
<arcpath arcPointType="false" id="1" xCoord="281" yCoord="267"/>
</arc>
<arc id="_MSG2 to Verify_" inscription="[0,inf)" source="P9"
target="T7" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="252" yCoord="267"/>
<arcpath arcPointType="false" id="1" xCoord="210" yCoord="270"/>
<arcpath arcPointType="false" id="2" xCoord="206" yCoord="291"/>
</arc>
<arc id="Rc to T20" inscription="[0,inf)" source="P1" target="T10"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="42" yCoord="118"/>
<arcpath arcPointType="false" id="1" xCoord="15" yCoord="120"/>
<arcpath arcPointType="false" id="2" xCoord="15" yCoord="525"/>
<arcpath arcPointType="false" id="3" xCoord="66" yCoord="527"/>
</arc>
<arc id="Tc to T20" inscription="[0,inf)" source="P2" target="T10"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="42" yCoord="163"/>
<arcpath arcPointType="false" id="1" xCoord="30" yCoord="165"/>
<arcpath arcPointType="false" id="2" xCoord="30" yCoord="510"/>
<arcpath arcPointType="false" id="3" xCoord="67" yCoord="517"/>
</arc>
<arc id="T20 to ACK" inscription="1" source="T10" target="P14"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="76" yCoord="527"/>
<arcpath arcPointType="false" id="1" xCoord="252" yCoord="522"/>
</arc>
```

```
<arc id="T20 to C_SK" inscription="1" source="T10" target="P13"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="77" yCoord="517"/>
<arcpath arcPointType="false" id="1" xCoord="195" yCoord="510"/>
<arcpath arcPointType="false" id="2" xCoord="255" yCoord="456"/>
</arc>
<arc id="ACK to SendACk" inscription="[0,inf)" source="P14"
target="T11" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="281" yCoord="522"/>
<arcpath arcPointType="false" id="1" xCoord="321" yCoord="522"/>
</arc>
<arc id="ReceiveACK to _ACK" inscription="1" source="T12"
target="P16" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="451" yCoord="522"/>
<arcpath arcPointType="false" id="1" xCoord="507" yCoord="522"/>
</arc>
<arc id="SendACk to ACK_" inscription="1" source="T11" target="P15"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="331" yCoord="522"/>
<arcpath arcPointType="false" id="1" xCoord="372" yCoord="522"/>
</arc>
<arc id="ACK_ to ReceiveACK" inscription="[0,inf)" source="P15"
target="T12" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="401" yCoord="522"/>
<arcpath arcPointType="false" id="1" xCoord="441" yCoord="522"/>
</arc>
<arc id="P12 to T8" inscription="[Deadline,Deadline]" source="P10"
target="T8" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="192" yCoord="357"/>
<arcpath arcPointType="false" id="1" xCoord="61" yCoord="357"/>
</arc>
<arc id="T8 to P13" inscription="1" source="T8" target="P11"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="57" yCoord="342"/>
<arcpath arcPointType="false" id="1" xCoord="57" yCoord="296"/>
</arc>
<arc id="P12 to T9" inscription="[0,Deadline]:1" source="P10"
target="T9" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="207" yCoord="371"/>
<arcpath arcPointType="false" id="1" xCoord="207" yCoord="432"/>
</arc>
<arc id="T9 to P14" inscription="[0,Deadline]:1" source="T9"
target="P12" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="201" yCoord="447"/>
<arcpath arcPointType="false" id="1" xCoord="86" yCoord="447"/>
</arc>
<arc id="P14 to T10" inscription="[0,inf)" source="P12" target="T10"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="72" yCoord="461"/>
<arcpath arcPointType="false" id="1" xCoord="72" yCoord="507"/>
</arc>
```

```
<arc id="P10 to T6" inscription="[0,inf)" source="P8" target="T6"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="372" yCoord="267"/>
<arcpath arcPointType="false" id="1" xCoord="331" yCoord="267"/>
</arc>
<arc id="P6 to T4" inscription="[0,inf)" source="P6" target="T4"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="536" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="584" yCoord="164"/>
<arcpath arcPointType="false" id="2" xCoord="581" yCoord="216"/>
</arc>
<arc id="T4 to P9" inscription="1" source="T4" target="P7"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="581" yCoord="226"/>
<arcpath arcPointType="false" id="1" xCoord="584" yCoord="269"/>
<arcpath arcPointType="false" id="2" xCoord="536" yCoord="267"/>
</arc>
</net>
<query active="true" approximationDenominator="2" capacity="0"
discreteInclusion="false" enableOverApproximation="false"
enableUnderApproximation="false" extrapolationOption="AUTOMATIC"
gcd="true" hashTableSize="MB_16" inclusionPlaces="*NONE*"
name="Query Comment/Name Here" overApproximation="true" pTrie="true"
query="EF true" reduction="true" reductionOption="VerifyTAPN"
searchOption="HEURISTIC" symmetry="true" timeDarts="true"
traceOption="NONE"/>
<k-bound bound="3"/>
</pnml>
```

Parallel Session Attack

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<pnml xmlns="http://www.informatik.hu-berlin.de/top/pnml/ptNetb">
<constant name="periodC" value="7"/>
<constant name="PeriodS" value="5"/>
<constant name="Deadline" value="5"/>
<net active="true" id="TAPN1" type="P/T net">
<labels border="false" height="18" positionX="93" positionY="0"
width="75">Client-Side</labels>
<labels border="false" height="18" positionX="739" positionY="0"
width="75">Server-Side</labels>
<labels border="false" height="15" positionX="381" positionY="0"
width="132">          Intruder</labels>
<place id="P1" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P1"
nameOffsetX="9.0" nameOffsetY="0.0" positionX="13.0"
positionY="70.0"/>
<place id="P2" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P2"
nameOffsetX="17.0" nameOffsetY="-4.0" positionX="5.0"
positionY="121.0"/>
<place id="P4" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P4"
nameOffsetX="29.0" nameOffsetY="-4.0" positionX="97.0"
positionY="121.0"/>
<place id="P5" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P5"
nameOffsetX="34.0" nameOffsetY="-2.0" positionX="181.0"
positionY="121.0"/>
<place id="P8" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P8"
nameOffsetX="25.0" nameOffsetY="-4.0" positionX="481.0"
positionY="121.0"/>
<place id="P10" initialMarking="0" invariant="&lt;= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P10"
nameOffsetX="65.0" nameOffsetY="-18.0" positionX="715.0"
positionY="73.0"/>
<place id="P9" initialMarking="0" invariant="&lt;= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P9"
nameOffsetX="69.0" nameOffsetY="-18.0" positionX="565.0"
positionY="121.0"/>
<place id="P12" initialMarking="1" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P12"
```

nameOffsetX="47.0" nameOffsetY="13.0" positionX="637.0"
positionY="265.0"/>
<place id="P14" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P14"
nameOffsetX="24.0" nameOffsetY="1.0" positionX="481.0"
positionY="253.0"/>
<place id="P13" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P13"
nameOffsetX="26.0" nameOffsetY="-4.0" positionX="628.0"
positionY="316.0"/>
<place id="P3" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P3"
nameOffsetX="9.0" nameOffsetY="5.0" positionX="13.0"
positionY="170.0"/>
<place id="P15" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P15"
nameOffsetX="31.0" nameOffsetY="4.0" positionX="481.0"
positionY="301.0"/>
<place id="P16" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P16"
nameOffsetX="26.0" nameOffsetY="2.0" positionX="385.0"
positionY="301.0"/>
<place id="P17" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P17"
nameOffsetX="26.0" nameOffsetY="-6.0" positionX="290.0"
positionY="301.0"/>
<place id="P18" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P18"
nameOffsetX="34.0" nameOffsetY="-4.0" positionX="290.0"
positionY="373.0"/>
<place id="P19" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P19"
nameOffsetX="25.0" nameOffsetY="-4.0" positionX="385.0"
positionY="373.0"/>
<place id="P20" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P20"
nameOffsetX="29.0" nameOffsetY="-3.0" positionX="470.0"
positionY="373.0"/>
<place id="P27" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P27"
nameOffsetX="17.0" nameOffsetY="1.0" positionX="487.0"
positionY="545.0"/>
<place id="P28" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P28"
nameOffsetX="13.0" nameOffsetY="-2.0" positionX="385.0"
positionY="545.0"/>
<place id="P22" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P22"
nameOffsetX="66.0" nameOffsetY="-17.0" positionX="715.0"
positionY="325.0"/>
<place id="P23" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P23"

nameOffsetX="83.0" nameOffsetY="-15.0" positionX="613.0"
positionY="460.0"/>
<place id="P24" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P24"
nameOffsetX="27.0" nameOffsetY="-5.0" positionX="661.0"
positionY="496.0"/>
<place id="P25" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P25"
nameOffsetX="26.0" nameOffsetY="-1.0" positionX="673.0"
positionY="545.0"/>
<place id="P26" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P26"
nameOffsetX="9.0" nameOffsetY="2.0" positionX="526.0"
positionY="508.0"/>
<place id="P6" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P6"
nameOffsetX="27.0" nameOffsetY="3.0" positionX="277.0"
positionY="121.0"/>
<place id="P7" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P7"
nameOffsetX="22.0" nameOffsetY="-5.0" positionX="385.0"
positionY="121.0"/>
<place id="P11" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P11"
nameOffsetX="112.0" nameOffsetY="0.0" positionX="565.0"
positionY="241.0"/>
<place id="P21" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P21"
nameOffsetX="59.0" nameOffsetY="-15.0" positionX="565.0"
positionY="373.0"/>
<place id="P29" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P29"
nameOffsetX="30.0" nameOffsetY="2.0" positionX="290.0"
positionY="545.0"/>
<transition angle="180" id="T1" infiniteServer="false" name="T1"
nameOffsetX="26.0" nameOffsetY="49.0" positionX="61.0"
positionY="121.0" priority="0" urgent="false"/>
<transition angle="0" id="T2" infiniteServer="false" name="T2"
nameOffsetX="19.0" nameOffsetY="51.0" positionX="133.0"
positionY="121.0" priority="0" urgent="false"/>
<transition angle="0" id="T5" infiniteServer="false" name="T5"
nameOffsetX="34.0" nameOffsetY="41.0" positionX="433.0"
positionY="121.0" priority="0" urgent="false"/>
<transition angle="0" id="T6" infiniteServer="false" name="T6"
nameOffsetX="24.0" nameOffsetY="48.0" positionX="517.0"
positionY="121.0" priority="0" urgent="false"/>
<transition angle="0" id="T9" infiniteServer="false" name="T9"
nameOffsetX="23.0" nameOffsetY="40.0" positionX="565.0"
positionY="301.0" priority="0" urgent="false"/>
<transition angle="0" id="T10" infiniteServer="false" name="T10"
nameOffsetX="37.0" nameOffsetY="48.0" positionX="433.0"
positionY="301.0" priority="0" urgent="false"/>

```
<transition angle="0" id="T11" infiniteServer="false" name="T11"
nameOffsetX="15.0" nameOffsetY="46.0" positionX="337.0"
positionY="301.0" priority="0" urgent="false"/>
<transition angle="0" id="T12" infiniteServer="false" name="T12"
nameOffsetX="36.0" nameOffsetY="43.0" positionX="241.0"
positionY="301.0" priority="0" urgent="false"/>
<transition angle="0" id="T13" infiniteServer="false" name="T13"
nameOffsetX="7.0" nameOffsetY="41.0" positionX="337.0"
positionY="373.0" priority="0" urgent="false"/>
<transition angle="0" id="T14" infiniteServer="false" name="T14"
nameOffsetX="36.0" nameOffsetY="43.0" positionX="433.0"
positionY="373.0" priority="0" urgent="false"/>
<transition angle="0" id="T19" infiniteServer="false" name="T19"
nameOffsetX="42.0" nameOffsetY="47.0" positionX="433.0"
positionY="545.0" priority="0" urgent="false"/>
<transition angle="0" id="T15" infiniteServer="false" name="T15"
nameOffsetX="25.0" nameOffsetY="52.0" positionX="517.0"
positionY="373.0" priority="0" urgent="false"/>
<transition angle="180" id="T18" infiniteServer="false" name="T18"
nameOffsetX="44.0" nameOffsetY="44.0" positionX="613.0"
positionY="545.0" priority="0" urgent="false"/>
<transition angle="0" id="T3" infiniteServer="false" name="T3"
nameOffsetX="31.0" nameOffsetY="48.0" positionX="217.0"
positionY="121.0" priority="0" urgent="false"/>
<transition angle="0" id="T4" infiniteServer="false" name="T4"
nameOffsetX="14.0" nameOffsetY="45.0" positionX="337.0"
positionY="121.0" priority="0" urgent="false"/>
<transition angle="90" id="T8" infiniteServer="false" name="T8"
nameOffsetX="-7.0" nameOffsetY="26.0" positionX="565.0"
positionY="181.0" priority="0" urgent="false"/>
<transition angle="0" id="T7" infiniteServer="false" name="T7"
nameOffsetX="18.0" nameOffsetY="39.0" positionX="715.0"
positionY="121.0" priority="0" urgent="false"/>
<transition angle="0" id="T16" infiniteServer="false" name="T16"
nameOffsetX="17.0" nameOffsetY="40.0" positionX="715.0"
positionY="373.0" priority="0" urgent="false"/>
<transition angle="0" id="T17" infiniteServer="false" name="T17"
nameOffsetX="42.0" nameOffsetY="44.0" positionX="565.0"
positionY="460.0" priority="0" urgent="false"/>
<transition angle="0" id="T20" infiniteServer="false" name="T20"
nameOffsetX="11.0" nameOffsetY="46.0" positionX="337.0"
positionY="545.0" priority="0" urgent="false"/>
<arc id="Tc to generateLoginRequest" inscription="[0,inf)"
source="P2" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="31" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="67" yCoord="133"/>
</arc>
<arc id="Rc to generateLoginRequest" inscription="[0,inf)"
source="P1" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="35" yCoord="92"/>
<arcpath arcPointType="false" id="1" xCoord="68" yCoord="126"/>
</arc>
```

```
<arc id="generateLoginRequest to LgoinRqst" inscription="1"
source="T1" target="P4" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="78" yCoord="132"/>
<arcpath arcPointType="false" id="1" xCoord="94" yCoord="132"/>
</arc>
<arc id="LgoinRqst to Encrypt" inscription="[0,inf)" source="P4"
target="T2" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="123" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="139" yCoord="133"/>
</arc>
<arc id="Encrypt to Cipher1" inscription="1" source="T2" target="P5"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="149" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="178" yCoord="133"/>
</arc>
<arc id="Decrypt to MSG1" inscription="1" source="T5" target="P8"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="449" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="478" yCoord="133"/>
</arc>
<arc id="MSG1 to T4" inscription="[0,inf)" source="P8" target="T6"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="507" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="523" yCoord="133"/>
</arc>
<arc id="Rs to T6" inscription="[0,inf)" source="P12" target="T9"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="634" yCoord="278"/>
<arcpath arcPointType="false" id="1" xCoord="600" yCoord="281"/>
<arcpath arcPointType="false" id="2" xCoord="582" yCoord="308"/>
</arc>
<arc id="T6 to SK_s" inscription="1" source="T9" target="P14"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="572" yCoord="308"/>
<arcpath arcPointType="false" id="1" xCoord="549" yCoord="274"/>
<arcpath arcPointType="false" id="2" xCoord="507" yCoord="267"/>
</arc>
<arc id="Ts to T6" inscription="[0,inf)" source="P13" target="T9"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="625" yCoord="325"/>
<arcpath arcPointType="false" id="1" xCoord="581" yCoord="318"/>
</arc>
<arc id="Requst to generateLoginRequest" inscription="[0,inf)"
source="P3" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="30" yCoord="167"/>
<arcpath arcPointType="false" id="1" xCoord="38" yCoord="146"/>
<arcpath arcPointType="false" id="2" xCoord="67" yCoord="140"/>
</arc>
<arc id="SYNACK_A to SendMSG_" inscription="[0,inf)" source="P15"
target="T10" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="478" yCoord="313"/>
<arcpath arcPointType="false" id="1" xCoord="449" yCoord="313"/>
```

```
</arc>
<arc id="SendMSG_ to MSG2_A" inscription="1" source="T10"
target="P16" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="439" yCoord="313"/>
<arcpath arcPointType="false" id="1" xCoord="411" yCoord="313"/>
</arc>
<arc id="MSG2_A to Intercept_MSG_" inscription="[0,inf)"
source="P16" target="T11" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="382" yCoord="313"/>
<arcpath arcPointType="false" id="1" xCoord="353" yCoord="313"/>
</arc>
<arc id="Intercept_MSG_ to MSG2_A_" inscription="1" source="T11"
target="P17" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="343" yCoord="313"/>
<arcpath arcPointType="false" id="1" xCoord="316" yCoord="313"/>
</arc>
<arc id="_MSG2 to FabricateMSG2" inscription="[0,inf)" source="P17"
target="T12" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="287" yCoord="313"/>
<arcpath arcPointType="false" id="1" xCoord="257" yCoord="313"/>
</arc>
<arc id="FabricateMSG2 to xMSG2x" inscription="1" source="T12"
target="P18" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="247" yCoord="313"/>
<arcpath arcPointType="false" id="1" xCoord="237" yCoord="309"/>
<arcpath arcPointType="false" id="2" xCoord="237" yCoord="381"/>
<arcpath arcPointType="false" id="3" xCoord="287" yCoord="384"/>
</arc>
<arc id="xMSG2x to SendMSG2" inscription="[0,inf)" source="P18"
target="T13" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="316" yCoord="385"/>
<arcpath arcPointType="false" id="1" xCoord="343" yCoord="385"/>
</arc>
<arc id="SendMSG2 to LoginReq2" inscription="1" source="T13"
target="P19" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="353" yCoord="385"/>
<arcpath arcPointType="false" id="1" xCoord="382" yCoord="385"/>
</arc>
<arc id="LoginReq2 to RecieveMSG2_" inscription="[0,inf)"
source="P19" target="T14" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="411" yCoord="385"/>
<arcpath arcPointType="false" id="1" xCoord="439" yCoord="385"/>
</arc>
<arc id="RecieveMSG2_ to SYN_A" inscription="1" source="T14"
target="P20" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="449" yCoord="385"/>
<arcpath arcPointType="false" id="1" xCoord="467" yCoord="385"/>
</arc>
<arc id="SYNACK_A to Recieve3" inscription="[0,inf)" source="P27"
target="T19" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="484" yCoord="557"/>
<arcpath arcPointType="false" id="1" xCoord="449" yCoord="557"/>
```

```
</arc>
<arc id="Recieve3 to SYN_ACK_" inscription="1" source="T19"
target="P28" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="439" yCoord="557"/>
<arcpath arcPointType="false" id="1" xCoord="411" yCoord="557"/>
</arc>
<arc id="Compute to SYNACK_C" inscription="1" source="T9"
target="P15" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="571" yCoord="318"/>
<arcpath arcPointType="false" id="1" xCoord="507" yCoord="314"/>
</arc>
<arc id="Verify_ to Accept" inscription="1" source="T6" target="P9"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="533" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="562" yCoord="133"/>
</arc>
<arc id="SYN_A to _Verify" inscription="[0,inf)" source="P20"
target="T15" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="496" yCoord="385"/>
<arcpath arcPointType="false" id="1" xCoord="523" yCoord="385"/>
</arc>
<arc id="Accept_ to T19" inscription="[0,inf)" source="P23"
target="T18" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="624" yCoord="486"/>
<arcpath arcPointType="false" id="1" xCoord="624" yCoord="541"/>
</arc>
<arc id="Rc_ to T19" inscription="[0,inf)" source="P24" target="T18"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="670" yCoord="522"/>
<arcpath arcPointType="false" id="1" xCoord="667" yCoord="538"/>
<arcpath arcPointType="false" id="2" xCoord="630" yCoord="551"/>
</arc>
<arc id="Ts_ to T19" inscription="[0,inf)" source="P25" target="T18"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="670" yCoord="558"/>
<arcpath arcPointType="false" id="1" xCoord="629" yCoord="561"/>
</arc>
<arc id="T19 to SK_A" inscription="1" source="T18" target="P26"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="620" yCoord="551"/>
<arcpath arcPointType="false" id="1" xCoord="591" yCoord="518"/>
<arcpath arcPointType="false" id="2" xCoord="552" yCoord="519"/>
</arc>
<arc id="T19 to SYNACK_A" inscription="1" source="T18" target="P27"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="619" yCoord="561"/>
<arcpath arcPointType="false" id="1" xCoord="513" yCoord="557"/>
</arc>
<arc id="P5 to T3" inscription="[0,inf)" source="P5" target="T3"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="207" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="223" yCoord="133"/>
```

```
</arc>
<arc id="T3 to P6" inscription="1" source="T3" target="P6"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="233" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="274" yCoord="133"/>
</arc>
<arc id="P6 to T4" inscription="[0,inf)" source="P6" target="T4"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="303" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="343" yCoord="133"/>
</arc>
<arc id="T4 to P7" inscription="1" source="T4" target="P7"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="353" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="382" yCoord="133"/>
</arc>
<arc id="P7 to T5" inscription="[0,inf)" source="P7" target="T5"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="411" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="439" yCoord="133"/>
</arc>
<arc id="P9 to T7" inscription="[Deadline,Deadline]" source="P9"
target="T7" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="591" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="721" yCoord="133"/>
</arc>
<arc id="T7 to P10" inscription="1" source="T7" target="P10"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="727" yCoord="118"/>
<arcpath arcPointType="false" id="1" xCoord="727" yCoord="99"/>
</arc>
<arc id="P9 to T8" inscription="[0,Deadline]:1" source="P9"
target="T8" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="576" yCoord="147"/>
<arcpath arcPointType="false" id="1" xCoord="576" yCoord="187"/>
</arc>
<arc id="T8 to P11" inscription="[0,Deadline]:1" source="T8"
target="P11" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="576" yCoord="197"/>
<arcpath arcPointType="false" id="1" xCoord="576" yCoord="238"/>
</arc>
<arc id="P11 to T9" inscription="[0,inf)" source="P11" target="T9"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="577" yCoord="267"/>
<arcpath arcPointType="false" id="1" xCoord="577" yCoord="298"/>
</arc>
<arc id="T15 to P21" inscription="1" source="T15" target="P21"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="533" yCoord="385"/>
<arcpath arcPointType="false" id="1" xCoord="562" yCoord="385"/>
</arc>
```

<arc id="P21 to T16" inscription="[Deadline,Deadline]" source="P21"
target="T16" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="591" yCoord="385"/>
<arcpath arcPointType="false" id="1" xCoord="721" yCoord="385"/>
</arc>
<arc id="T16 to P22" inscription="1" source="T16" target="P22"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="727" yCoord="370"/>
<arcpath arcPointType="false" id="1" xCoord="727" yCoord="351"/>
</arc>
<arc id="P21 to T17" inscription="[0,Deadline]:1" source="P21"
target="T17" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="577" yCoord="399"/>
<arcpath arcPointType="false" id="1" xCoord="577" yCoord="457"/>
</arc>
<arc id="T17 to P23" inscription="[0,Deadline]:1" source="T17"
target="P23" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="581" yCoord="472"/>
<arcpath arcPointType="false" id="1" xCoord="610" yCoord="472"/>
</arc>
<arc id="P28 to T20" inscription="[0,inf)" source="P28" target="T20"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="382" yCoord="557"/>
<arcpath arcPointType="false" id="1" xCoord="353" yCoord="557"/>
</arc>
<arc id="T20 to P29" inscription="1" source="T20" target="P29"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="343" yCoord="557"/>
<arcpath arcPointType="false" id="1" xCoord="316" yCoord="557"/>
</arc>
</net>
<query active="true" approximationDenominator="2" capacity="0"
discreteInclusion="false" enableOverApproximation="false"
enableUnderApproximation="false" extrapolationOption="AUTOMATIC"
gcd="true" hashTableSize="MB_16" inclusionPlaces="*NONE*"
name="Query Comment/Name Here" overApproximation="true" pTrie="true"
query="EF true" reduction="true" reductionOption="VerifyTAPN"
searchOption="HEURISTIC" symmetry="true" timeDarts="true"
traceOption="NONE"/>
<k-bound bound="3"/>
</pnml>

Ciphertext Attack

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<pnml xmlns="http://www.informatik.hu-berlin.de/top/pnml/ptNetb">
<constant name="periodC" value="7"/>
<constant name="PeriodS" value="5"/>
<constant name="Deadline" value="5"/>
<net active="true" id="TAPN1" type="P/T net">
<place id="P1" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P1"
nameOffsetX="22.0" nameOffsetY="-4.0" positionX="30.0"
positionY="105.0"/>
<place id="P2" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P2"
nameOffsetX="17.0" nameOffsetY="-4.0" positionX="26.0"
positionY="150.0"/>
<place id="P4" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P4"
nameOffsetX="25.0" nameOffsetY="-5.0" positionX="105.0"
positionY="150.0"/>
<place id="P6" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P6"
nameOffsetX="23.0" nameOffsetY="-4.0" positionX="195.0"
positionY="150.0"/>
<place id="P15" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P15"
nameOffsetX="26.0" nameOffsetY="-3.0" positionX="765.0"
positionY="150.0"/>
<place id="P17" initialMarking="0" invariant="&lt;= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P17"
nameOffsetX="83.0" nameOffsetY="-19.0" positionX="795.0"
positionY="60.0"/>
<place id="P18_" initialMarking="0" invariant="&lt; Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P18_"
nameOffsetX="59.0" nameOffsetY="-20.0" positionX="795.0"
positionY="240.0"/>
<place id="P19" initialMarking="1" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P19"
nameOffsetX="29.0" nameOffsetY="-3.0" positionX="900.0"
positionY="270.0"/>
<place id="P21" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P21"
nameOffsetX="29.0" nameOffsetY="-3.0" positionX="810.0"
positionY="315.0"/>
<place id="P22" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P22"
```

nameOffsetX="3.0" nameOffsetY="3.0" positionX="855.0"
positionY="375.0"/>
<place id="P25" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P25"
nameOffsetX="34.0" nameOffsetY="0.0" positionX="675.0"
positionY="390.0"/>
<place id="P28" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P28"
nameOffsetX="40.0" nameOffsetY="-1.0" positionX="180.0"
positionY="390.0"/>
<place id="P29" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P29"
nameOffsetX="99.0" nameOffsetY="-20.0" positionX="45.0"
positionY="390.0"/>
<place id="P31" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P31"
nameOffsetX="114.0" nameOffsetY="5.0" positionX="45.0"
positionY="540.0"/>
<place id="P20" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P20"
nameOffsetX="36.0" nameOffsetY="0.0" positionX="900.0"
positionY="375.0"/>
<place id="P3" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P3"
nameOffsetX="11.0" nameOffsetY="3.0" positionX="30.0"
positionY="195.0"/>
<place id="P32" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P32"
nameOffsetX="28.0" nameOffsetY="1.0" positionX="120.0"
positionY="615.0"/>
<place id="P33_" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P33_"
nameOffsetX="24.0" nameOffsetY="-2.0" positionX="150.0"
positionY="645.0"/>
<place id="P36" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P36"
nameOffsetX="34.0" nameOffsetY="-7.0" positionX="735.0"
positionY="645.0"/>
<place id="P38" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P38"
nameOffsetX="102.0" nameOffsetY="-13.0" positionX="945.0"
positionY="600.0"/>
<place id="P39" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P39"
nameOffsetX="63.0" nameOffsetY="-19.0" positionX="960.0"
positionY="735.0"/>
<place id="P11" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P11"
nameOffsetX="25.0" nameOffsetY="-6.0" positionX="495.0"
positionY="165.0"/>
<place id="P23" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P23"

nameOffsetX="25.0" nameOffsetY="-1.0" positionX="855.0"
positionY="420.0"/>
<place id="P26" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P26"
nameOffsetX="25.0" nameOffsetY="-5.0" positionX="480.0"
positionY="390.0"/>
<place id="P34_" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P34_"
nameOffsetX="27.0" nameOffsetY="-7.0" positionX="270.0"
positionY="645.0"/>
<place id="P35_" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P35_"
nameOffsetX="35.0" nameOffsetY="-4.0" positionX="480.0"
positionY="645.0"/>
<place id="P35" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P35"
nameOffsetX="25.0" nameOffsetY="-1.0" positionX="615.0"
positionY="645.0"/>
<place id="P13" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P13"
nameOffsetX="23.0" nameOffsetY="-4.0" positionX="675.0"
positionY="150.0"/>
<place id="P12" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P12"
nameOffsetX="17.0" nameOffsetY="-7.0" positionX="585.0"
positionY="150.0"/>
<place id="P30" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P30"
nameOffsetX="126.0" nameOffsetY="14.0" positionX="45.0"
positionY="255.0"/>
<place id="P37" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P37"
nameOffsetX="122.0" nameOffsetY="7.0" positionX="855.0"
positionY="645.0"/>
<place id="P16" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P16"
nameOffsetX="79.0" nameOffsetY="-11.0" positionX="855.0"
positionY="150.0"/>
<place id="P5" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P5" nameOffsetX="-
1.0" nameOffsetY="10.0" positionX="105.0" positionY="210.0"/>
<place id="P7" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P7" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="240.0" positionY="270.0"/>
<place id="P9" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P9"
nameOffsetX="15.0" nameOffsetY="-5.0" positionX="375.0"
positionY="150.0"/>
<place id="P10" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P10"
nameOffsetX="26.0" nameOffsetY="-2.0" positionX="465.0"
positionY="150.0"/>

<place id="P27" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P27"
nameOffsetX="33.0" nameOffsetY="-3.0" positionX="285.0"
positionY="390.0"/>
<place id="P14" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P14" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="720.0" positionY="270.0"/>
<place id="P24" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P24"
nameOffsetX="28.0" nameOffsetY="-7.0" positionX="765.0"
positionY="390.0"/>
<place id="P8" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P8"
nameOffsetX="22.0" nameOffsetY="-6.0" positionX="285.0"
positionY="150.0"/>
<transition angle="0" id="T1" infiniteServer="false" name="T1"
nameOffsetX="34.0" nameOffsetY="41.0" positionX="60.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T2" infiniteServer="false" name="T2"
nameOffsetX="19.0" nameOffsetY="50.0" positionX="150.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T9" infiniteServer="false" name="T9"
nameOffsetX="6.0" nameOffsetY="40.0" positionX="720.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T10" infiniteServer="false" name="T10"
nameOffsetX="15.0" nameOffsetY="52.0" positionX="810.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T13" infiniteServer="false" name="T13"
nameOffsetX="25.0" nameOffsetY="47.0" positionX="870.0"
positionY="315.0" priority="0" urgent="false"/>
<transition angle="0" id="T14" infiniteServer="false" name="T14"
nameOffsetX="33.0" nameOffsetY="45.0" positionX="810.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T18" infiniteServer="false" name="T18"
nameOffsetX="10.0" nameOffsetY="52.0" positionX="240.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T19" infiniteServer="false" name="T19"
nameOffsetX="35.0" nameOffsetY="45.0" positionX="105.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="180" id="T22__" infiniteServer="false"
name="T22__" nameOffsetX="27.0" nameOffsetY="50.0" positionX="75.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T199" infiniteServer="false" name="T199"
nameOffsetX="16.0" nameOffsetY="49.0" positionX="210.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T22_" infiniteServer="false" name="T22_"
nameOffsetX="41.0" nameOffsetY="43.0" positionX="675.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T23_" infiniteServer="false" name="T23_"
nameOffsetX="19.0" nameOffsetY="47.0" positionX="795.0"
positionY="645.0" priority="0" urgent="false"/>

<transition angle="180" id="T3" infiniteServer="false" name="T3"
nameOffsetX="38.0" nameOffsetY="39.0" positionX="240.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="180" id="T6" infiniteServer="false" name="T6"
nameOffsetX="37.0" nameOffsetY="44.0" positionX="465.0"
positionY="240.0" priority="0" urgent="false"/>
<transition angle="0" id="T16" infiniteServer="false" name="T16"
nameOffsetX="40.0" nameOffsetY="44.0" positionX="630.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T20__" infiniteServer="false" name="T20__"
nameOffsetX="50.0" nameOffsetY="50.0" positionX="330.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="0" id="T21_" infiniteServer="false" name="T21_"
nameOffsetX="18.0" nameOffsetY="46.0" positionX="555.0"
positionY="645.0" priority="0" urgent="false"/>
<transition angle="270" id="T21" infiniteServer="false" name="T21"
nameOffsetX="54.0" nameOffsetY="28.0" positionX="45.0"
positionY="480.0" priority="0" urgent="false"/>
<transition angle="90" id="T20" infiniteServer="false" name="T20"
nameOffsetX="56.0" nameOffsetY="30.0" positionX="45.0"
positionY="300.0" priority="0" urgent="false"/>
<transition angle="0" id="T24_" infiniteServer="false" name="T24_"
nameOffsetX="11.0" nameOffsetY="-1.0" positionX="855.0"
positionY="600.0" priority="0" urgent="false"/>
<transition angle="0" id="T25_" infiniteServer="false" name="T25_"
nameOffsetX="13.0" nameOffsetY="40.0" positionX="855.0"
positionY="735.0" priority="0" urgent="false"/>
<transition angle="0" id="T11" infiniteServer="false" name="T11"
nameOffsetX="51.0" nameOffsetY="18.0" positionX="855.0"
positionY="60.0" priority="0" urgent="false"/>
<transition angle="0" id="T12" infiniteServer="false" name="T12"
nameOffsetX="35.0" nameOffsetY="38.0" positionX="855.0"
positionY="240.0" priority="0" urgent="false"/>
<transition angle="0" id="T5" infiniteServer="false" name="T5"
nameOffsetX="25.0" nameOffsetY="51.0" positionX="420.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T7" infiniteServer="false" name="T7"
nameOffsetX="14.0" nameOffsetY="47.0" positionX="540.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T8" infiniteServer="false" name="T8"
nameOffsetX="32.0" nameOffsetY="50.0" positionX="630.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T15" infiniteServer="false" name="T15"
nameOffsetX="29.0" nameOffsetY="52.0" positionX="720.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="0" id="T4" infiniteServer="false" name="T4"
nameOffsetX="20.0" nameOffsetY="48.0" positionX="330.0"
positionY="150.0" priority="0" urgent="false"/>
<transition angle="0" id="T17" infiniteServer="false" name="T17"
nameOffsetX="19.0" nameOffsetY="44.0" positionX="330.0"
positionY="390.0" priority="0" urgent="false"/>

<arc id="Tc to generateLoginRequest" inscription="[0,inf)"
source="P2" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="52" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="66" yCoord="162"/>
</arc>
<arc id="generateLoginRequest to LgoinRqst" inscription="1"
source="T1" target="P4" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="76" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="102" yCoord="162"/>
</arc>
<arc id="LgoinRqst to Encrypt" inscription="[0,inf)" source="P4"
target="T2" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="131" yCoord="160"/>
<arcpath arcPointType="false" id="1" xCoord="157" yCoord="157"/>
</arc>
<arc id="Encrypt to Cipher1" inscription="1" source="T2" target="P6"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="166" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="192" yCoord="162"/>
</arc>
<arc id="Decrypt to MSG1" inscription="1" source="T9" target="P15"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="736" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="762" yCoord="162"/>
</arc>
<arc id="MSG1 to T4" inscription="[0,inf)" source="P15" target="T10"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="791" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="816" yCoord="162"/>
</arc>
<arc id="Rs to T6" inscription="[0,inf)" source="P19" target="T13"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="910" yCoord="296"/>
<arcpath arcPointType="false" id="1" xCoord="908" yCoord="324"/>
<arcpath arcPointType="false" id="2" xCoord="887" yCoord="322"/>
</arc>
<arc id="Accept to T6" inscription="[0,inf)" source="P18_"
target="T13" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="808" yCoord="266"/>
<arcpath arcPointType="false" id="1" xCoord="810" yCoord="284"/>
<arcpath arcPointType="false" id="2" xCoord="882" yCoord="287"/>
<arcpath arcPointType="false" id="3" xCoord="882" yCoord="312"/>
</arc>
<arc id="T6 to SK_s" inscription="1" source="T13" target="P21"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="877" yCoord="322"/>
<arcpath arcPointType="false" id="1" xCoord="836" yCoord="325"/>
</arc>
<arc id="T6 to SYN_ACK" inscription="1" source="T13" target="P22"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="876" yCoord="332"/>
<arcpath arcPointType="false" id="1" xCoord="862" yCoord="344"/>

<arcpath arcPointType="false" id="2" xCoord="865" yCoord="372"/>
</arc>
<arc id="SYN_ACK to Encrypt_" inscription="[0,inf)" source="P22"
target="T14" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="852" yCoord="390"/>
<arcpath arcPointType="false" id="1" xCoord="827" yCoord="397"/>
</arc>
<arc id="Decrypt_ to MSG2" inscription="1" source="T18" target="P28"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="246" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="206" yCoord="402"/>
</arc>
<arc id="MSG2 to T9" inscription="[0,inf)" source="P28" target="T19"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="177" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="121" yCoord="402"/>
</arc>
<arc id="T9 to Reject2" inscription="1" source="T19" target="P29"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="111" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="71" yCoord="402"/>
</arc>
<arc id="Ts to T6" inscription="[0,inf)" source="P20" target="T13"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="906" yCoord="372"/>
<arcpath arcPointType="false" id="1" xCoord="894" yCoord="340"/>
<arcpath arcPointType="false" id="2" xCoord="886" yCoord="332"/>
</arc>
<arc id="Requst to generateLoginRequest" inscription="[0,inf)"
source="P3" target="T1" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="53" yCoord="197"/>
<arcpath arcPointType="false" id="1" xCoord="66" yCoord="186"/>
<arcpath arcPointType="false" id="2" xCoord="72" yCoord="177"/>
</arc>
<arc id="Tc to T12" inscription="[0,inf)" source="P2" target="T22__"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="23" yCoord="167"/>
<arcpath arcPointType="false" id="1" xCoord="19" yCoord="169"/>
<arcpath arcPointType="false" id="2" xCoord="19" yCoord="649"/>
<arcpath arcPointType="false" id="3" xCoord="82" yCoord="651"/>
</arc>
<arc id="T12 to SK_c" inscription="1" source="T22__" target="P32"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="92" yCoord="651"/>
<arcpath arcPointType="false" id="1" xCoord="109" yCoord="649"/>
<arcpath arcPointType="false" id="2" xCoord="121" yCoord="637"/>
</arc>
<arc id="T12 to ACK" inscription="1" source="T22__" target="P33_"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="91" yCoord="661"/>
<arcpath arcPointType="false" id="1" xCoord="147" yCoord="657"/>
</arc>

<arc id="ACK to _Encrypt" inscription="[0,inf)" source="P33_"
target="T199" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="176" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="216" yCoord="657"/>
</arc>
<arc id="_Decrypt to MSG3" inscription="1" source="T22_"
target="P36" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="691" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="732" yCoord="657"/>
</arc>
<arc id="MSG3 to T15" inscription="[0,inf)" source="P36"
target="T23_" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="761" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="801" yCoord="657"/>
</arc>
<arc id="Cipher1 to Receive_Cipher1" inscription="[0,inf)"
source="P6" target="T3" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="221" yCoord="161"/>
<arcpath arcPointType="false" id="1" xCoord="247" yCoord="161"/>
</arc>
<arc id="Cipher2 to T20" inscription="[0,inf)" source="P25"
target="T16" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="672" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="646" yCoord="402"/>
</arc>
<arc id="SYNACK_A to SendMSG_" inscription="[0,inf)" source="P23"
target="T14" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="854" yCoord="424"/>
<arcpath arcPointType="false" id="1" xCoord="826" yCoord="407"/>
</arc>
<arc id="Intercept_MSG_ to MSG2_A_" inscription="1" source="T16"
target="P26" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="636" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="506" yCoord="402"/>
</arc>
<arc id="Accept2 to T12" inscription="[0,inf)" source="P31"
target="T22__" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="61" yCoord="566"/>
<arcpath arcPointType="false" id="1" xCoord="86" yCoord="641"/>
</arc>
<arc id="SendMSG3 to MSG3_" inscription="1" source="T199"
target="P34_" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="226" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="267" yCoord="657"/>
</arc>
<arc id="MSG3_ to Intercept_MSG3" inscription="[0,inf)"
source="P34_" target="T20__" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="296" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="336" yCoord="657"/>
</arc>
<arc id="Intercept_MSG3 to xMSG3x" inscription="1" source="T20__"
target="P35_" type="normal" weight="1">

```
<arcpath arcPointType="false" id="0" xCoord="346" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="477" yCoord="657"/>
</arc>
<arc id="xMSG3x to SendMSG3_" inscription="[0,inf)" source="P35_"
target="T21_" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="506" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="561" yCoord="657"/>
</arc>
<arc id="SendMSG3_ to XMSG3X_" inscription="1" source="T21_"
target="P35" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="571" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="612" yCoord="657"/>
</arc>
<arc id="XMSG3X_ to _ReceiveMSG3" inscription="[0,inf)" source="P35"
target="T22_" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="641" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="681" yCoord="657"/>
</arc>
<arc id="DuplicateMSG to xMSG1_A" inscription="1" source="T6"
target="P11" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="482" yCoord="251"/>
<arcpath arcPointType="false" id="1" xCoord="497" yCoord="242"/>
<arcpath arcPointType="false" id="2" xCoord="504" yCoord="191"/>
</arc>
<arc id="P28 to T16" inscription="[Deadline,Deadline]" source="P29"
target="T20" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="56" yCoord="387"/>
<arcpath arcPointType="false" id="1" xCoord="56" yCoord="316"/>
</arc>
<arc id="T16 to P29" inscription="1" source="T20" target="P30"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="56" yCoord="306"/>
<arcpath arcPointType="false" id="1" xCoord="56" yCoord="281"/>
</arc>
<arc id="P28 to T17" inscription="[0,Deadline]:1" source="P29"
target="T21" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="57" yCoord="416"/>
<arcpath arcPointType="false" id="1" xCoord="57" yCoord="487"/>
</arc>
<arc id="T17 to P30" inscription="[0,Deadline]:1" source="T21"
target="P31" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="57" yCoord="497"/>
<arcpath arcPointType="false" id="1" xCoord="57" yCoord="537"/>
</arc>
<arc id="P37 to T24" inscription="[Deadline,Deadline]" source="P37"
target="T24_" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="869" yCoord="642"/>
<arcpath arcPointType="false" id="1" xCoord="868" yCoord="650"/>
<arcpath arcPointType="false" id="2" xCoord="867" yCoord="627"/>
</arc>
<arc id="T24 to P38" inscription="1" source="T24_" target="P38"
type="normal" weight="1">
```

```
<arcpath arcPointType="false" id="0" xCoord="871" yCoord="612"/>
<arcpath arcPointType="false" id="1" xCoord="942" yCoord="612"/>
</arc>
<arc id="P37 to T25" inscription="[0,Deadline]:1" source="P37"
target="T25_" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="867" yCoord="671"/>
<arcpath arcPointType="false" id="1" xCoord="867" yCoord="732"/>
</arc>
<arc id="T25 to P39" inscription="[0,Deadline]:1" source="T25_"
target="P39" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="871" yCoord="747"/>
<arcpath arcPointType="false" id="1" xCoord="957" yCoord="747"/>
</arc>
<arc id="T23 to P37" inscription="1" source="T23_" target="P37"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="811" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="852" yCoord="657"/>
</arc>
<arc id="T7 to P13" inscription="1" source="T10" target="P16"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="826" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="852" yCoord="162"/>
</arc>
<arc id="P13 to T8" inscription="[Deadline,Deadline]" source="P16"
target="T11" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="867" yCoord="147"/>
<arcpath arcPointType="false" id="1" xCoord="867" yCoord="87"/>
</arc>
<arc id="T8 to P14" inscription="1" source="T11" target="P17"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="861" yCoord="72"/>
<arcpath arcPointType="false" id="1" xCoord="821" yCoord="72"/>
</arc>
<arc id="P13 to T9" inscription="[0,Deadline]:1" source="P16"
target="T12" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="867" yCoord="176"/>
<arcpath arcPointType="false" id="1" xCoord="867" yCoord="237"/>
</arc>
<arc id="T9 to P15" inscription="[0,Deadline]:1" source="T12"
target="P18_" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="861" yCoord="252"/>
<arcpath arcPointType="false" id="1" xCoord="821" yCoord="252"/>
</arc>
<arc id="P5 to T2" inscription="[0,inf)" source="P5" target="T2"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="117" yCoord="207"/>
<arcpath arcPointType="false" id="1" xCoord="117" yCoord="192"/>
<arcpath arcPointType="false" id="2" xCoord="156" yCoord="167"/>
</arc>
<arc id="P9 to T5" inscription="[0,inf)" source="P9" target="T5"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="401" yCoord="162"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="426" yCoord="162"/>
</arc>
<arc id="T5 to P10" inscription="1" source="T5" target="P10"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="436" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="462" yCoord="162"/>
</arc>
<arc id="P10 to T6" inscription="[0,inf)" source="P10" target="T6"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="476" yCoord="176"/>
<arcpath arcPointType="false" id="1" xCoord="476" yCoord="236"/>
</arc>
<arc id="Encrypt__ to Cipher1_i" inscription="1" source="T7"
target="P12" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="556" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="582" yCoord="162"/>
</arc>
<arc id="FakeMSG to Encrypt__" inscription="[0,inf)" source="P11"
target="T7" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="518" yCoord="167"/>
<arcpath arcPointType="false" id="1" xCoord="524" yCoord="162"/>
<arcpath arcPointType="false" id="2" xCoord="546" yCoord="162"/>
</arc>
<arc id="P12 to T8" inscription="[0,inf)" source="P12" target="T8"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="611" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="636" yCoord="162"/>
</arc>
<arc id="T8 to P13" inscription="1" source="T8" target="P13"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="646" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="672" yCoord="162"/>
</arc>
<arc id="P13 to T9" inscription="[0,inf)" source="P13" target="T9"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="701" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="726" yCoord="162"/>
</arc>
<arc id="P14 to T15" inscription="[0,inf)" source="P14" target="T15"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="732" yCoord="297"/>
<arcpath arcPointType="false" id="1" xCoord="732" yCoord="342"/>
<arcpath arcPointType="false" id="2" xCoord="732" yCoord="387"/>
</arc>
<arc id="T14 to P24" inscription="1" source="T14" target="P24"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="816" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="791" yCoord="402"/>
</arc>
<arc id="P24 to T15" inscription="[0,inf)" source="P24" target="T15"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="762" yCoord="402"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="736" yCoord="402"/>
</arc>
<arc id="T15 to P25" inscription="1" source="T15" target="P25"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="726" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="701" yCoord="402"/>
</arc>
<arc id="P7 to T3" inscription="[0,inf)" source="P7" target="T3"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="252" yCoord="267"/>
<arcpath arcPointType="false" id="1" xCoord="252" yCoord="192"/>
<arcpath arcPointType="false" id="2" xCoord="251" yCoord="176"/>
</arc>
<arc id="T3 to P7" inscription="1" source="T3" target="P7"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="251" yCoord="176"/>
<arcpath arcPointType="false" id="1" xCoord="252" yCoord="192"/>
<arcpath arcPointType="false" id="2" xCoord="252" yCoord="267"/>
</arc>
<arc id="P7 to T18" inscription="[0,inf)" source="P7" target="T18"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="252" yCoord="297"/>
<arcpath arcPointType="false" id="1" xCoord="252" yCoord="357"/>
<arcpath arcPointType="false" id="2" xCoord="252" yCoord="387"/>
</arc>
<arc id="T18 to P7" inscription="1" source="T18" target="P7"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="252" yCoord="387"/>
<arcpath arcPointType="false" id="1" xCoord="252" yCoord="357"/>
<arcpath arcPointType="false" id="2" xCoord="252" yCoord="297"/>
</arc>
<arc id="P1 to T22__" inscription="[0,inf)" source="P1"
target="T22__" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="27" yCoord="117"/>
<arcpath arcPointType="false" id="1" xCoord="12" yCoord="117"/>
<arcpath arcPointType="false" id="2" xCoord="12" yCoord="657"/>
<arcpath arcPointType="false" id="3" xCoord="81" yCoord="661"/>
</arc>
<arc id="P1 to T1" inscription="[0,inf)" source="P1" target="T1"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="52" yCoord="127"/>
<arcpath arcPointType="false" id="1" xCoord="72" yCoord="147"/>
</arc>
<arc id="T15 to P14" inscription="1" source="T15" target="P14"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="732" yCoord="387"/>
<arcpath arcPointType="false" id="1" xCoord="732" yCoord="342"/>
<arcpath arcPointType="false" id="2" xCoord="732" yCoord="297"/>
</arc>
<arc id="P14 to T9" inscription="[0,inf)" source="P14" target="T9"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="732" yCoord="267"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="732" yCoord="192"/>
<arcpath arcPointType="false" id="2" xCoord="732" yCoord="177"/>
</arc>
<arc id="T9 to P14" inscription="1" source="T9" target="P14"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="732" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="732" yCoord="207"/>
<arcpath arcPointType="false" id="2" xCoord="732" yCoord="267"/>
</arc>
<arc id="T3 to P8" inscription="1" source="T3" target="P8"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="257" yCoord="161"/>
<arcpath arcPointType="false" id="1" xCoord="282" yCoord="161"/>
</arc>
<arc id="P8 to T4" inscription="[0,inf)" source="P8" target="T4"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="311" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="336" yCoord="162"/>
</arc>
<arc id="T4 to P9" inscription="1" source="T4" target="P9"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="346" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="372" yCoord="162"/>
</arc>
<arc id="T17 to P27" inscription="1" source="T17" target="P27"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="336" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="311" yCoord="402"/>
</arc>
<arc id="MSG2_A_ to _SendMSG_" inscription="[0,inf)" source="P26"
target="T17" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="477" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="346" yCoord="402"/>
</arc>
<arc id="P27 to T18" inscription="[0,inf)" source="P27" target="T18"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="282" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="256" yCoord="402"/>
</arc>
</net>
<query active="true" approximationDenominator="2" capacity="0"
discreteInclusion="false" enableOverApproximation="false"
enableUnderApproximation="false" extrapolationOption="AUTOMATIC"
gcd="true" hashTableSize="MB_16" inclusionPlaces="*NONE*"
name="Query Comment/Name Here" overApproximation="true" pTrie="true"
query="EF true" reduction="true" reductionOption="VerifyTAPN"
searchOption="HEURISTIC" symmetry="true" timeDarts="true"
traceOption="NONE"/>
<k-bound bound="3"/>
</pnml>
```

Modified Trust Model (Complex)

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<pnml xmlns="http://www.informatik.hu-berlin.de/top/pnml/ptNetb">
<shared-place initialMarking="0" invariant="&lt; inf"
name="SecretKey"/>
<shared-transition name="T9" urgent="false"/>
<shared-transition name="T26" urgent="false"/>
<shared-transition name="T41" urgent="false"/>
<constant name="Deadline" value="30"/>
<constant name="Period" value="20"/>
<constant name="Reject" value="30"/>
<constant name="Accept" value="98"/>
<net active="true" id="TAPN1" type="P/T net">
<place id="P1" initialMarking="1" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P1" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="60.0" positionY="45.0"/>
<place id="P7" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P7"
nameOffsetX="18.0" nameOffsetY="45.0" positionX="165.0"
positionY="45.0"/>
<place id="P2" initialMarking="4" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P2" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="60.0" positionY="90.0"/>
<place id="P3" initialMarking="1" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P3" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="60.0" positionY="135.0"/>
<place id="P8" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P8"
nameOffsetX="34.0" nameOffsetY="43.0" positionX="165.0"
positionY="105.0"/>
<place id="P4" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P4" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="60.0" positionY="180.0"/>
<place id="P9" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P9"
nameOffsetX="34.0" nameOffsetY="40.0" positionX="165.0"
positionY="165.0"/>
<place id="P5" initialMarking="3" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P5" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="60.0" positionY="225.0"/>
<place id="P6" initialMarking="2" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P6" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="60.0" positionY="270.0"/>
<place id="P10" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P10"
nameOffsetX="37.0" nameOffsetY="46.0" positionX="255.0"
positionY="165.0"/>
```

<place id="P11" initialMarking="3" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P11" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="225.0" positionY="405.0"/>
<place id="P12" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P12" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="300.0" positionY="225.0"/>
<place id="P13" initialMarking="2" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P13"
nameOffsetX="26.0" nameOffsetY="41.0" positionX="330.0"
positionY="345.0"/>
<place id="P14" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P14"
nameOffsetX="21.0" nameOffsetY="-7.0" positionX="345.0"
positionY="165.0"/>
<place id="P15" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P15"
nameOffsetX="19.0" nameOffsetY="-1.0" positionX="435.0"
positionY="165.0"/>
<place id="P16" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P16"
nameOffsetX="18.0" nameOffsetY="-1.0" positionX="510.0"
positionY="165.0"/>
<place id="P17" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P17" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="585.0" positionY="90.0"/>
<place id="P18" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P18"
nameOffsetX="18.0" nameOffsetY="44.0" positionX="585.0"
positionY="180.0"/>
<place id="P19" initialMarking="2" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P19" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="615.0" positionY="225.0"/>
<place id="P20" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P20"
nameOffsetX="23.0" nameOffsetY="-3.0" positionX="660.0"
positionY="165.0"/>
<place id="P21" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P21"
nameOffsetX="53.0" nameOffsetY="-18.0" positionX="750.0"
positionY="165.0"/>
<place id="P22" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P22"
nameOffsetX="50.0" nameOffsetY="-19.0" positionX="870.0"
positionY="90.0"/>
<place id="P23" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P23"
nameOffsetX="112.0" nameOffsetY="5.0" positionX="750.0"
positionY="285.0"/>
<place id="P31" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P31"
nameOffsetX="26.0" nameOffsetY="0.0" positionX="810.0"
positionY="450.0"/>

<place id="P30" initialMarking="3" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P30"
nameOffsetX="28.0" nameOffsetY="-4.0" positionX="810.0"
positionY="405.0"/>
<place id="P28" initialMarking="2" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P28"
nameOffsetX="25.0" nameOffsetY="0.0" positionX="600.0"
positionY="330.0"/>
<place id="P33" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P33"
nameOffsetX="32.0" nameOffsetY="-3.0" positionX="690.0"
positionY="450.0"/>
<place id="P32" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P32"
nameOffsetX="17.0" nameOffsetY="-5.0" positionX="675.0"
positionY="405.0"/>
<place id="P29" initialMarking="2" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P29"
nameOffsetX="20.0" nameOffsetY="2.0" positionX="585.0"
positionY="375.0"/>
<place id="P24" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P24"
nameOffsetX="40.0" nameOffsetY="0.0" positionX="840.0"
positionY="360.0"/>
<place id="P26" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P26"
nameOffsetX="7.0" nameOffsetY="4.0" positionX="690.0"
positionY="255.0"/>
<place id="P27" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P27"
nameOffsetX="36.0" nameOffsetY="4.0" positionX="630.0"
positionY="285.0"/>
<place id="P25" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P25"
nameOffsetX="31.0" nameOffsetY="45.0" positionX="765.0"
positionY="360.0"/>
<place id="P34" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P34"
nameOffsetX="15.0" nameOffsetY="0.0" positionX="585.0"
positionY="450.0"/>
<place id="P35" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P35"
nameOffsetX="36.0" nameOffsetY="2.0" positionX="825.0"
positionY="510.0"/>
<place id="P36" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P36"
nameOffsetX="27.0" nameOffsetY="2.0" positionX="720.0"
positionY="495.0"/>
<place id="P38" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P38"
nameOffsetX="26.0" nameOffsetY="-2.0" positionX="720.0"
positionY="555.0"/>

<place id="P37" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P37"
nameOffsetX="41.0" nameOffsetY="3.0" positionX="615.0"
positionY="495.0"/>
<place id="P39" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P39"
nameOffsetX="34.0" nameOffsetY="44.0" positionX="555.0"
positionY="540.0"/>
<place id="P40" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P40" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="525.0" positionY="585.0"/>
<place id="P41" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P41" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="585.0" positionY="585.0"/>
<place id="P42" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P42"
nameOffsetX="17.0" nameOffsetY="-7.0" positionX="525.0"
positionY="660.0"/>
<place id="P43" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P43"
nameOffsetX="25.0" nameOffsetY="-3.0" positionX="420.0"
positionY="660.0"/>
<place id="P44" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P44"
nameOffsetX="30.0" nameOffsetY="-3.0" positionX="345.0"
positionY="660.0"/>
<place id="P46" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P46"
nameOffsetX="13.0" nameOffsetY="-5.0" positionX="270.0"
positionY="660.0"/>
<place id="P45" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P45"
nameOffsetX="34.0" nameOffsetY="0.0" positionX="270.0"
positionY="570.0"/>
<place id="P48" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P48" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="75.0" positionY="660.0"/>
<place id="P49" initialMarking="0" invariant="<= Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P49"
nameOffsetX="76.0" nameOffsetY="-22.0" positionX="75.0"
positionY="495.0"/>
<place id="P50" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P50" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="75.0" positionY="810.0"/>
<place id="P47" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P47"
nameOffsetX="23.0" nameOffsetY="4.0" positionX="180.0"
positionY="660.0"/>
<place id="P52" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P52"
nameOffsetX="30.0" nameOffsetY="-3.0" positionX="150.0"
positionY="900.0"/>

<place id="P51" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P51" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="150.0" positionY="855.0"/>
<place id="P53" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P53"
nameOffsetX="34.0" nameOffsetY="-2.0" positionX="120.0"
positionY="930.0"/>
<place id="P54" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P54" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="75.0" positionY="1065.0"/>
<place id="P55" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P55" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="195.0" positionY="960.0"/>
<place id="P56" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P56"
nameOffsetX="31.0" nameOffsetY="-5.0" positionX="300.0"
positionY="945.0"/>
<place id="P57" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P57"
nameOffsetX="18.0" nameOffsetY="-5.0" positionX="180.0"
positionY="1035.0"/>
<place id="P58" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P58"
nameOffsetX="31.0" nameOffsetY="2.0" positionX="285.0"
positionY="1035.0"/>
<place id="P59" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P59"
nameOffsetX="39.0" nameOffsetY="2.0" positionX="270.0"
positionY="1140.0"/>
<place id="P60" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P60" nameOffsetX="-
4.0" nameOffsetY="17.0" positionX="135.0" positionY="1140.0"/>
<place id="P61" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P61" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="315.0" positionY="1200.0"/>
<place id="P62" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P62"
nameOffsetX="26.0" nameOffsetY="-6.0" positionX="435.0"
positionY="1200.0"/>
<place id="P63" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P63"
nameOffsetX="29.0" nameOffsetY="0.0" positionX="510.0"
positionY="1200.0"/>
<place id="P65" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P65"
nameOffsetX="27.0" nameOffsetY="5.0" positionX="600.0"
positionY="1125.0"/>
<place id="P66" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P66"
nameOffsetX="28.0" nameOffsetY="1.0" positionX="705.0"
positionY="1125.0"/>

<place id="P67" initialMarking="0" invariant="< Deadline"
markingOffsetX="0.0" markingOffsetY="0.0" name="P67"
nameOffsetX="100.0" nameOffsetY="-12.0" positionX="795.0"
positionY="1125.0"/>
<place id="P68" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P68"
nameOffsetX="15.0" nameOffsetY="5.0" positionX="795.0"
positionY="990.0"/>
<place id="P69" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P69" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="795.0" positionY="1260.0"/>
<place id="P70" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P70" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="660.0" positionY="1260.0"/>
<place id="P64" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P64"
nameOffsetX="17.0" nameOffsetY="-2.0" positionX="555.0"
positionY="1125.0"/>
<transition angle="0" id="T1" infiniteServer="false" name="T1"
nameOffsetX="25.0" nameOffsetY="46.0" positionX="120.0"
positionY="45.0" priority="0" urgent="false"/>
<transition angle="0" id="T2" infiniteServer="false" name="T2"
nameOffsetX="23.0" nameOffsetY="45.0" positionX="120.0"
positionY="105.0" priority="0" urgent="false"/>
<transition angle="0" id="T3" infiniteServer="false" name="T3"
nameOffsetX="24.0" nameOffsetY="44.0" positionX="120.0"
positionY="165.0" priority="0" urgent="false"/>
<transition angle="0" id="T4" infiniteServer="false" name="T4"
nameOffsetX="39.0" nameOffsetY="40.0" positionX="210.0"
positionY="165.0" priority="0" urgent="false"/>
<transition angle="0" id="T5" infiniteServer="false" name="T5"
nameOffsetX="32.0" nameOffsetY="3.0" positionX="300.0"
positionY="165.0" priority="0" urgent="false"/>
<transition angle="0" id="T6" infiniteServer="false" name="T6"
nameOffsetX="26.0" nameOffsetY="52.0" positionX="330.0"
positionY="255.0" priority="0" urgent="false"/>
<transition angle="0" id="T7" infiniteServer="false" name="T7"
nameOffsetX="9.0" nameOffsetY="45.0" positionX="390.0"
positionY="165.0" priority="0" urgent="false"/>
<transition angle="0" id="T8" infiniteServer="false" name="T8"
nameOffsetX="26.0" nameOffsetY="41.0" positionX="465.0"
positionY="165.0" priority="0" urgent="false"/>
<transition angle="0" id="T9" infiniteServer="false" name="T9"
nameOffsetX="26.0" nameOffsetY="49.0" positionX="540.0"
positionY="165.0" priority="0" urgent="false"/>
<transition angle="0" id="T10" infiniteServer="false" name="T10"
nameOffsetX="39.0" nameOffsetY="50.0" positionX="615.0"
positionY="165.0" priority="0" urgent="false"/>
<transition angle="0" id="T11" infiniteServer="false" name="T11"
nameOffsetX="20.0" nameOffsetY="46.0" positionX="705.0"
positionY="165.0" priority="0" urgent="false"/>

```
<transition angle="0" id="T12" infiniteServer="false" name="T12"
nameOffsetX="34.0" nameOffsetY="41.0" positionX="870.0"
positionY="165.0" priority="0" urgent="false"/>
<transition angle="90" id="T13" infiniteServer="false" name="T13"
nameOffsetX="-5.0" nameOffsetY="35.0" positionX="750.0"
positionY="225.0" priority="0" urgent="false"/>
<transition angle="0" id="T16" infiniteServer="false" name="T16"
nameOffsetX="26.0" nameOffsetY="50.0" positionX="765.0"
positionY="435.0" priority="0" urgent="false"/>
<transition angle="0" id="T15" infiniteServer="false" name="T15"
nameOffsetX="23.0" nameOffsetY="46.0" positionX="720.0"
positionY="390.0" priority="0" urgent="false"/>
<transition angle="135" id="T17" infiniteServer="false" name="T17"
nameOffsetX="36.0" nameOffsetY="48.0" positionX="630.0"
positionY="420.0" priority="0" urgent="false"/>
<transition angle="225" id="T14" infiniteServer="false" name="T14"
nameOffsetX="9.0" nameOffsetY="39.0" positionX="720.0"
positionY="330.0" priority="0" urgent="false"/>
<transition angle="0" id="T18" infiniteServer="false" name="T18"
nameOffsetX="28.0" nameOffsetY="43.0" positionX="780.0"
positionY="495.0" priority="0" urgent="false"/>
<transition angle="0" id="T19" infiniteServer="false" name="T19"
nameOffsetX="38.0" nameOffsetY="50.0" positionX="780.0"
positionY="555.0" priority="0" urgent="false"/>
<transition angle="0" id="T20" infiniteServer="false" name="T20"
nameOffsetX="28.0" nameOffsetY="48.0" positionX="660.0"
positionY="495.0" priority="0" urgent="false"/>
<transition angle="135" id="T21" infiniteServer="false" name="T21"
nameOffsetX="6.0" nameOffsetY="1.0" positionX="555.0"
positionY="495.0" priority="0" urgent="false"/>
<transition angle="135" id="T23" infiniteServer="false" name="T23"
nameOffsetX="41.0" nameOffsetY="41.0" positionX="555.0"
positionY="630.0" priority="0" urgent="false"/>
<transition angle="0" id="T22" infiniteServer="false" name="T22"
nameOffsetX="9.0" nameOffsetY="41.0" positionX="510.0"
positionY="540.0" priority="0" urgent="false"/>
<transition angle="180" id="T24" infiniteServer="false" name="T24"
nameOffsetX="24.0" nameOffsetY="49.0" positionX="465.0"
positionY="660.0" priority="0" urgent="false"/>
<transition angle="0" id="T25" infiniteServer="false" name="T25"
nameOffsetX="14.0" nameOffsetY="50.0" positionX="390.0"
positionY="660.0" priority="0" urgent="false"/>
<transition angle="0" id="T26" infiniteServer="false" name="T26"
nameOffsetX="22.0" nameOffsetY="49.0" positionX="315.0"
positionY="660.0" priority="0" urgent="false"/>
<transition angle="0" id="T27" infiniteServer="false" name="T27"
nameOffsetX="27.0" nameOffsetY="48.0" positionX="225.0"
positionY="660.0" priority="0" urgent="false"/>
<transition angle="0" id="T29" infiniteServer="false" name="T29"
nameOffsetX="39.0" nameOffsetY="34.0" positionX="75.0"
positionY="555.0" priority="0" urgent="false"/>
```

<transition angle="0" id="T30" infiniteServer="false" name="T30"
nameOffsetX="43.0" nameOffsetY="35.0" positionX="75.0"
positionY="735.0" priority="0" urgent="false"/>
<transition angle="0" id="T28" infiniteServer="false" name="T28"
nameOffsetX="26.0" nameOffsetY="44.0" positionX="150.0"
positionY="660.0" priority="0" urgent="false"/>
<transition angle="0" id="T31" infiniteServer="false" name="T31"
nameOffsetX="8.0" nameOffsetY="44.0" positionX="75.0"
positionY="870.0" priority="0" urgent="false"/>
<transition angle="0" id="T32" infiniteServer="false" name="T32"
nameOffsetX="35.0" nameOffsetY="45.0" positionX="150.0"
positionY="960.0" priority="0" urgent="false"/>
<transition angle="0" id="T33" infiniteServer="false" name="T33"
nameOffsetX="31.0" nameOffsetY="-4.0" positionX="250.0"
positionY="945.0" priority="0" urgent="false"/>
<transition angle="0" id="T34" infiniteServer="false" name="T34"
nameOffsetX="26.0" nameOffsetY="51.0" positionX="135.0"
positionY="1035.0" priority="0" urgent="false"/>
<transition angle="0" id="T35" infiniteServer="false" name="T35"
nameOffsetX="41.0" nameOffsetY="37.0" positionX="225.0"
positionY="1035.0" priority="0" urgent="false"/>
<transition angle="0" id="T36" infiniteServer="false" name="T36"
nameOffsetX="51.0" nameOffsetY="-3.0" positionX="330.0"
positionY="1035.0" priority="0" urgent="false"/>
<transition angle="0" id="T38" infiniteServer="false" name="T38"
nameOffsetX="29.0" nameOffsetY="45.0" positionX="135.0"
positionY="1200.0" priority="0" urgent="false"/>
<transition angle="0" id="T39" infiniteServer="false" name="T39"
nameOffsetX="-5.0" nameOffsetY="35.0" positionX="390.0"
positionY="1200.0" priority="0" urgent="false"/>
<transition angle="0" id="T40" infiniteServer="false" name="T40"
nameOffsetX="40.0" nameOffsetY="50.0" positionX="465.0"
positionY="1200.0" priority="0" urgent="false"/>
<transition angle="0" id="T41" infiniteServer="false" name="T41"
nameOffsetX="33.0" nameOffsetY="41.0" positionX="555.0"
positionY="1200.0" priority="0" urgent="false"/>
<transition angle="0" id="T42" infiniteServer="false" name="T42"
nameOffsetX="34.0" nameOffsetY="46.0" positionX="645.0"
positionY="1125.0" priority="0" urgent="false"/>
<transition angle="0" id="T43" infiniteServer="false" name="T43"
nameOffsetX="26.0" nameOffsetY="49.0" positionX="750.0"
positionY="1125.0" priority="0" urgent="false"/>
<transition angle="0" id="T44" infiniteServer="false" name="T44"
nameOffsetX="-5.0" nameOffsetY="35.0" positionX="795.0"
positionY="1035.0" priority="0" urgent="false"/>
<transition angle="0" id="T45" infiniteServer="false" name="T45"
nameOffsetX="41.0" nameOffsetY="35.0" positionX="795.0"
positionY="1200.0" priority="0" urgent="false"/>
<transition angle="0" id="T46" infiniteServer="false" name="T46"
nameOffsetX="19.0" nameOffsetY="51.0" positionX="735.0"
positionY="1260.0" priority="0" urgent="false"/>

```
<transition angle="0" id="T37" infiniteServer="false" name="T37"
nameOffsetX="27.0" nameOffsetY="47.0" positionX="195.0"
positionY="1140.0" priority="0" urgent="false"/>
<arc id="Pc to T0" inscription="[0,inf)" source="P1" target="T1"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="86" yCoord="55"/>
<arcpath arcPointType="false" id="1" xCoord="127" yCoord="52"/>
</arc>
<arc id="T0 to w1" inscription="1" source="T1" target="P7"
type="normal" weight="2">
<arcpath arcPointType="false" id="0" xCoord="136" yCoord="57"/>
<arcpath arcPointType="false" id="1" xCoord="162" yCoord="57"/>
</arc>
<arc id="Rc to T0" inscription="[0,inf)" source="P2" target="T1"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="86" yCoord="102"/>
<arcpath arcPointType="false" id="1" xCoord="118" yCoord="103"/>
<arcpath arcPointType="false" id="2" xCoord="118" yCoord="73"/>
<arcpath arcPointType="false" id="3" xCoord="126" yCoord="62"/>
</arc>
<arc id="Rc to T2" inscription="[0,inf)" source="P2" target="T2"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="86" yCoord="104"/>
<arcpath arcPointType="false" id="1" xCoord="127" yCoord="112"/>
</arc>
<arc id="Prv_C to T2" inscription="[0,inf)" source="P3" target="T2"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="86" yCoord="147"/>
<arcpath arcPointType="false" id="1" xCoord="118" yCoord="148"/>
<arcpath arcPointType="false" id="2" xCoord="118" yCoord="133"/>
<arcpath arcPointType="false" id="3" xCoord="126" yCoord="122"/>
</arc>
<arc id="T2 to M2" inscription="1" source="T2" target="P8"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="136" yCoord="117"/>
<arcpath arcPointType="false" id="1" xCoord="162" yCoord="117"/>
</arc>
<arc id="Rc to T3" inscription="[0,inf)" source="P2" target="T3"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="85" yCoord="108"/>
<arcpath arcPointType="false" id="1" xCoord="103" yCoord="118"/>
<arcpath arcPointType="false" id="2" xCoord="103" yCoord="163"/>
<arcpath arcPointType="false" id="3" xCoord="127" yCoord="172"/>
</arc>
<arc id="M1 to T3" inscription="[0,inf)" source="P4" target="T3"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="86" yCoord="189"/>
<arcpath arcPointType="false" id="1" xCoord="126" yCoord="182"/>
</arc>
<arc id="T3 to M3" inscription="1" source="T3" target="P9"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="136" yCoord="177"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="162" yCoord="177"/>
</arc>
<arc id="w1 to T4" inscription="[0,inf)" source="P7" target="T4"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="191" yCoord="57"/>
<arcpath arcPointType="false" id="1" xCoord="223" yCoord="58"/>
<arcpath arcPointType="false" id="2" xCoord="222" yCoord="162"/>
</arc>
<arc id="M2 to T4" inscription="[0,inf)" source="P8" target="T4"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="191" yCoord="117"/>
<arcpath arcPointType="false" id="1" xCoord="208" yCoord="118"/>
<arcpath arcPointType="false" id="2" xCoord="208" yCoord="163"/>
<arcpath arcPointType="false" id="3" xCoord="217" yCoord="171"/>
</arc>
<arc id="M3 to T4" inscription="[0,inf)" source="P9" target="T4"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="191" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="216" yCoord="178"/>
</arc>
<arc id="ID to T4" inscription="[0,inf)" source="P5" target="T4"
type="timed" weight="2">
<arcpath arcPointType="false" id="0" xCoord="86" yCoord="237"/>
<arcpath arcPointType="false" id="1" xCoord="193" yCoord="238"/>
<arcpath arcPointType="false" id="2" xCoord="193" yCoord="208"/>
<arcpath arcPointType="false" id="3" xCoord="216" yCoord="185"/>
</arc>
<arc id="Tc to T4" inscription="[0,inf)" source="P6" target="T4"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="86" yCoord="282"/>
<arcpath arcPointType="false" id="1" xCoord="223" yCoord="283"/>
<arcpath arcPointType="false" id="2" xCoord="222" yCoord="192"/>
</arc>
<arc id="T4 to MSG" inscription="1" source="T4" target="P10"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="226" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="252" yCoord="177"/>
</arc>
<arc id="MSG to T5" inscription="[0,inf)" source="P10" target="T5"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="281" yCoord="175"/>
<arcpath arcPointType="false" id="1" xCoord="307" yCoord="172"/>
</arc>
<arc id="ScrtK to T5" inscription="[0,inf)" source="P11" target="T5"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="237" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="238" yCoord="298"/>
<arcpath arcPointType="false" id="2" xCoord="306" yCoord="182"/>
</arc>
<arc id="T5 to C1" inscription="1" source="T5" target="P12"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="312" yCoord="192"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="312" yCoord="222"/>
</arc>
<arc id="MACkey to T6" inscription="[0,inf)" source="P13"
target="T6" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="342" yCoord="342"/>
<arcpath arcPointType="false" id="1" xCoord="342" yCoord="282"/>
</arc>
<arc id="C1 to T6" inscription="[0,inf)" source="P12" target="T6"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="318" yCoord="250"/>
<arcpath arcPointType="false" id="1" xCoord="318" yCoord="250"/>
<arcpath arcPointType="false" id="2" xCoord="336" yCoord="267"/>
</arc>
<arc id="T6 to A1" inscription="1" source="T6" target="P14"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="346" yCoord="267"/>
<arcpath arcPointType="false" id="1" xCoord="358" yCoord="268"/>
<arcpath arcPointType="false" id="2" xCoord="357" yCoord="191"/>
</arc>
<arc id="A1 to T7" inscription="[0,inf)" source="P14" target="T7"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="371" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="396" yCoord="177"/>
</arc>
<arc id="T7 to P15" inscription="1" source="T7" target="P15"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="406" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="432" yCoord="177"/>
</arc>
<arc id="P15 to T8" inscription="[0,inf)" source="P15" target="T8"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="461" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="471" yCoord="177"/>
</arc>
<arc id="T8 to P16" inscription="1" source="T8" target="P16"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="481" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="507" yCoord="177"/>
</arc>
<arc id="P16 to IntegrityCheck" inscription="[0,inf)" source="P16"
target="T9" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="536" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="546" yCoord="177"/>
</arc>
<arc id="IntegrityCheck to P21" inscription="1" source="T9"
target="P18" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="556" yCoord="182"/>
<arcpath arcPointType="false" id="1" xCoord="582" yCoord="188"/>
</arc>
<arc id="IntegrityCheck to P20" inscription="1" source="T9"
target="P17" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="557" yCoord="172"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="598" yCoord="163"/>
<arcpath arcPointType="false" id="2" xCoord="597" yCoord="116"/>
</arc>
<arc id="P21 to T10" inscription="[0,inf)" source="P18" target="T10"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="610" yCoord="184"/>
<arcpath arcPointType="false" id="1" xCoord="621" yCoord="177"/>
</arc>
<arc id="P22 to T10" inscription="[0,inf)" source="P19" target="T10"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="627" yCoord="222"/>
<arcpath arcPointType="false" id="1" xCoord="627" yCoord="192"/>
</arc>
<arc id="T10 to P23" inscription="1" source="T10" target="P20"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="631" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="657" yCoord="177"/>
</arc>
<arc id="P23 to T11" inscription="[0,inf)" source="P20" target="T11"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="686" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="711" yCoord="177"/>
</arc>
<arc id="T11 to P24" inscription="1" source="T11" target="P21"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="721" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="747" yCoord="177"/>
</arc>
<arc id="P24 to T12" inscription="[Deadline,Deadline]" source="P21"
target="T12" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="776" yCoord="177"/>
<arcpath arcPointType="false" id="1" xCoord="876" yCoord="177"/>
</arc>
<arc id="T12 to P25" inscription="1" source="T12" target="P22"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="882" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="882" yCoord="116"/>
</arc>
<arc id="P24 to T13" inscription="[0,Period]:1" source="P21"
target="T13" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="761" yCoord="191"/>
<arcpath arcPointType="false" id="1" xCoord="761" yCoord="231"/>
</arc>
<arc id="T13 to P26" inscription="[0,Period]:1" source="T13"
target="P23" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="761" yCoord="241"/>
<arcpath arcPointType="false" id="1" xCoord="761" yCoord="282"/>
</arc>
<arc id="Ps to T14" inscription="[0,inf)" source="P31" target="T16"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="807" yCoord="458"/>
<arcpath arcPointType="false" id="1" xCoord="781" yCoord="452"/>
```

```
</arc>
<arc id="Rs to T14" inscription="[0,inf)" source="P30" target="T16"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="809" yCoord="425"/>
<arcpath arcPointType="false" id="1" xCoord="782" yCoord="442"/>
</arc>
<arc id="T14 to W2" inscription="1" source="T16" target="P33"
type="normal" weight="2">
<arcpath arcPointType="false" id="0" xCoord="771" yCoord="447"/>
<arcpath arcPointType="false" id="1" xCoord="716" yCoord="459"/>
</arc>
<arc id="Rs to T15" inscription="[0,inf)" source="P30" target="T15"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="807" yCoord="415"/>
<arcpath arcPointType="false" id="1" xCoord="736" yCoord="407"/>
</arc>
<arc id="T15 to Ks" inscription="1" source="T15" target="P32"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="726" yCoord="402"/>
<arcpath arcPointType="false" id="1" xCoord="701" yCoord="411"/>
</arc>
<arc id="P26 to T17" inscription="[0,inf)" source="P23" target="T14"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="754" yCoord="310"/>
<arcpath arcPointType="false" id="1" xCoord="742" yCoord="331"/>
</arc>
<arc id="T17 to Tc_" inscription="1" source="T14" target="P26"
type="normal" weight="2">
<arcpath arcPointType="false" id="0" xCoord="732" yCoord="334"/>
<arcpath arcPointType="false" id="1" xCoord="708" yCoord="280"/>
</arc>
<arc id="T17 to IDc_" inscription="1" source="T14" target="P27"
type="normal" weight="2">
<arcpath arcPointType="false" id="0" xCoord="724" yCoord="341"/>
<arcpath arcPointType="false" id="1" xCoord="655" yCoord="304"/>
</arc>
<arc id="T17 to M3_" inscription="1" source="T14" target="P24"
type="normal" weight="3">
<arcpath arcPointType="false" id="0" xCoord="739" yCoord="341"/>
<arcpath arcPointType="false" id="1" xCoord="837" yCoord="368"/>
</arc>
<arc id="T17 to W1_" inscription="1" source="T14" target="P25"
type="normal" weight="2">
<arcpath arcPointType="false" id="0" xCoord="732" yCoord="348"/>
<arcpath arcPointType="false" id="1" xCoord="763" yCoord="364"/>
</arc>
<arc id="W1_ to T15" inscription="[0,inf)" source="P25" target="T15"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="764" yCoord="380"/>
<arcpath arcPointType="false" id="1" xCoord="737" yCoord="397"/>
</arc>
```

```
<arc id="T18 to M5" inscription="1" source="T18" target="P36"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="786" yCoord="507"/>
<arcpath arcPointType="false" id="1" xCoord="746" yCoord="507"/>
</arc>
<arc id="M4 to T19" inscription="[0,inf)" source="P35" target="T19"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="827" yCoord="533"/>
<arcpath arcPointType="false" id="1" xCoord="823" yCoord="538"/>
<arcpath arcPointType="false" id="2" xCoord="797" yCoord="559"/>
</arc>
<arc id="T19 to M6" inscription="1" source="T19" target="P38"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="786" yCoord="567"/>
<arcpath arcPointType="false" id="1" xCoord="746" yCoord="567"/>
</arc>
<arc id="M5 to T20" inscription="[0,inf)" source="P36" target="T20"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="717" yCoord="505"/>
<arcpath arcPointType="false" id="1" xCoord="677" yCoord="502"/>
</arc>
<arc id="M6 to T21" inscription="[0,inf)" source="P38" target="T21"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="717" yCoord="564"/>
<arcpath arcPointType="false" id="1" xCoord="628" yCoord="553"/>
<arcpath arcPointType="false" id="2" xCoord="577" yCoord="518"/>
</arc>
<arc id="M7 to T21" inscription="[0,inf)" source="P37" target="T21"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="612" yCoord="507"/>
<arcpath arcPointType="false" id="1" xCoord="576" yCoord="509"/>
</arc>
<arc id="T21 to P42" inscription="1" source="T21" target="P39"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="563" yCoord="510"/>
<arcpath arcPointType="false" id="1" xCoord="565" yCoord="537"/>
</arc>
<arc id="P22 to T23" inscription="[0,inf)" source="P19" target="T22"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="612" yCoord="237"/>
<arcpath arcPointType="false" id="1" xCoord="523" yCoord="238"/>
<arcpath arcPointType="false" id="2" xCoord="522" yCoord="537"/>
</arc>
<arc id="P42 to T23" inscription="[0,inf)" source="P39" target="T22"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="552" yCoord="552"/>
<arcpath arcPointType="false" id="1" xCoord="526" yCoord="552"/>
</arc>
<arc id="T23 to P43" inscription="1" source="T22" target="P40"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="522" yCoord="567"/>
<arcpath arcPointType="false" id="1" xCoord="530" yCoord="583"/>
```

```
</arc>
<arc id="P43 to T22" inscription="[0,inf)" source="P40" target="T23"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="544" yCoord="610"/>
<arcpath arcPointType="false" id="1" xCoord="556" yCoord="631"/>
</arc>
<arc id="P44 to T22" inscription="[0,inf)" source="P41" target="T23"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="588" yCoord="609"/>
<arcpath arcPointType="false" id="1" xCoord="570" yCoord="637"/>
</arc>
<arc id="T22 to P45" inscription="1" source="T23" target="P42"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="563" yCoord="645"/>
<arcpath arcPointType="false" id="1" xCoord="547" yCoord="661"/>
</arc>
<arc id="P45 to T24" inscription="[0,inf)" source="P42" target="T24"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="522" yCoord="671"/>
<arcpath arcPointType="false" id="1" xCoord="482" yCoord="671"/>
</arc>
<arc id="T24 to P46" inscription="1" source="T24" target="P43"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="472" yCoord="671"/>
<arcpath arcPointType="false" id="1" xCoord="446" yCoord="671"/>
</arc>
<arc id="P46 to T25" inscription="[0,inf)" source="P43" target="T25"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="417" yCoord="672"/>
<arcpath arcPointType="false" id="1" xCoord="406" yCoord="672"/>
</arc>
<arc id="T25 to P47" inscription="1" source="T25" target="P44"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="396" yCoord="672"/>
<arcpath arcPointType="false" id="1" xCoord="371" yCoord="672"/>
</arc>
<arc id="P47 to Integrity_C" inscription="[0,inf)" source="P44"
target="T26" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="342" yCoord="672"/>
<arcpath arcPointType="false" id="1" xCoord="331" yCoord="672"/>
</arc>
<arc id="Integrity_C to P48" inscription="1" source="T26"
target="P46" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="321" yCoord="677"/>
<arcpath arcPointType="false" id="1" xCoord="296" yCoord="674"/>
</arc>
<arc id="Integrity_C to P49" inscription="1" source="T26"
target="P45" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="322" yCoord="667"/>
<arcpath arcPointType="false" id="1" xCoord="283" yCoord="628"/>
<arcpath arcPointType="false" id="2" xCoord="282" yCoord="596"/>
</arc>
```

```
<arc id="P48 to T27" inscription="[0,inf)" source="P46" target="T27"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="267" yCoord="672"/>
<arcpath arcPointType="false" id="1" xCoord="241" yCoord="672"/>
</arc>
<arc id="T16 to SK_s" inscription="1" source="T17" target="P34"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="638" yCoord="435"/>
<arcpath arcPointType="false" id="1" xCoord="609" yCoord="453"/>
</arc>
<arc id="M3_ to T18" inscription="[0,inf)" source="P24" target="T18"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="850" yCoord="386"/>
<arcpath arcPointType="false" id="1" xCoord="838" yCoord="478"/>
<arcpath arcPointType="false" id="2" xCoord="797" yCoord="502"/>
</arc>
<arc id="T20 to M7" inscription="1" source="T20" target="P37"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="666" yCoord="507"/>
<arcpath arcPointType="false" id="1" xCoord="641" yCoord="507"/>
</arc>
<arc id="W2 to T21" inscription="[0,inf)" source="P33" target="T21"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="687" yCoord="465"/>
<arcpath arcPointType="false" id="1" xCoord="643" yCoord="478"/>
<arcpath arcPointType="false" id="2" xCoord="573" yCoord="506"/>
</arc>
<arc id="IDS to T21" inscription="[0,inf)" source="P29" target="T21"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="582" yCoord="387"/>
<arcpath arcPointType="false" id="1" xCoord="553" yCoord="388"/>
<arcpath arcPointType="false" id="2" xCoord="562" yCoord="494"/>
</arc>
<arc id="Ts to T21" inscription="[0,inf)" source="P28" target="T21"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="597" yCoord="345"/>
<arcpath arcPointType="false" id="1" xCoord="553" yCoord="358"/>
<arcpath arcPointType="false" id="2" xCoord="565" yCoord="497"/>
</arc>
<arc id="IDc_ to T21" inscription="[0,inf)" source="P27"
target="T21" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="627" yCoord="301"/>
<arcpath arcPointType="false" id="1" xCoord="553" yCoord="328"/>
<arcpath arcPointType="false" id="2" xCoord="568" yCoord="500"/>
</arc>
<arc id="P50 to T28" inscription="[Deadline,Deadline]" source="P48"
target="T29" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="87" yCoord="657"/>
<arcpath arcPointType="false" id="1" xCoord="87" yCoord="582"/>
</arc>
<arc id="T28 to P51" inscription="1" source="T29" target="P49"
type="normal" weight="1">
```

```
<arcpath arcPointType="false" id="0" xCoord="87" yCoord="552"/>
<arcpath arcPointType="false" id="1" xCoord="87" yCoord="521"/>
</arc>
<arc id="T27 to P53" inscription="1" source="T27" target="P47"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="231" yCoord="672"/>
<arcpath arcPointType="false" id="1" xCoord="206" yCoord="672"/>
</arc>
<arc id="P53 to T30" inscription="[0,inf)" source="P47" target="T28"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="177" yCoord="672"/>
<arcpath arcPointType="false" id="1" xCoord="166" yCoord="672"/>
</arc>
<arc id="P50 to T29" inscription="[0,Period]:1" source="P48"
target="T30" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="87" yCoord="686"/>
<arcpath arcPointType="false" id="1" xCoord="87" yCoord="732"/>
</arc>
<arc id="T29 to P52" inscription="[0,Period]:1" source="T30"
target="P50" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="87" yCoord="762"/>
<arcpath arcPointType="false" id="1" xCoord="87" yCoord="807"/>
</arc>
<arc id="P52 to T31" inscription="[0,inf)" source="P50" target="T31"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="87" yCoord="836"/>
<arcpath arcPointType="false" id="1" xCoord="87" yCoord="867"/>
</arc>
<arc id="T31 to W2_" inscription="1" source="T31" target="P53"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="91" yCoord="888"/>
<arcpath arcPointType="false" id="1" xCoord="122" yCoord="930"/>
</arc>
<arc id="W2_ to T32" inscription="[0,inf)" source="P53" target="T32"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="142" yCoord="952"/>
<arcpath arcPointType="false" id="1" xCoord="157" yCoord="967"/>
</arc>
<arc id="Rc to T32" inscription="[0,inf)" source="P2" target="T32"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="57" yCoord="102"/>
<arcpath arcPointType="false" id="1" xCoord="13" yCoord="103"/>
<arcpath arcPointType="false" id="2" xCoord="28" yCoord="973"/>
<arcpath arcPointType="false" id="3" xCoord="133" yCoord="973"/>
<arcpath arcPointType="false" id="4" xCoord="156" yCoord="977"/>
</arc>
<arc id="T32 to Kc" inscription="1" source="T32" target="P55"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="166" yCoord="972"/>
<arcpath arcPointType="false" id="1" xCoord="192" yCoord="972"/>
</arc>
```

```
<arc id="Kc to T33" inscription="[0,inf)" source="P55" target="T33"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="221" yCoord="970"/>
<arcpath arcPointType="false" id="1" xCoord="256" yCoord="965"/>
</arc>
<arc id="Tc to T33" inscription="[0,inf)" source="P6" target="T33"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="57" yCoord="282"/>
<arcpath arcPointType="false" id="1" xCoord="28" yCoord="283"/>
<arcpath arcPointType="false" id="2" xCoord="28" yCoord="1018"/>
<arcpath arcPointType="false" id="3" xCoord="253" yCoord="1018"/>
<arcpath arcPointType="false" id="4" xCoord="262" yCoord="972"/>
</arc>
<arc id="T31 to Ts_" inscription="1" source="T31" target="P52"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="92" yCoord="881"/>
<arcpath arcPointType="false" id="1" xCoord="148" yCoord="905"/>
</arc>
<arc id="T31 to IDs_" inscription="1" source="T31" target="P51"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="92" yCoord="874"/>
<arcpath arcPointType="false" id="1" xCoord="147" yCoord="868"/>
</arc>
<arc id="Ts_ to T33" inscription="[0,inf)" source="P52" target="T33"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="175" yCoord="918"/>
<arcpath arcPointType="false" id="1" xCoord="256" yCoord="958"/>
</arc>
<arc id="IDs_ to T33" inscription="[0,inf)" source="P51"
target="T33" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="173" yCoord="876"/>
<arcpath arcPointType="false" id="1" xCoord="257" yCoord="951"/>
</arc>
<arc id="w1 to T33" inscription="[0,inf)" source="P7" target="T33"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="177" yCoord="42"/>
<arcpath arcPointType="false" id="1" xCoord="178" yCoord="28"/>
<arcpath arcPointType="false" id="2" xCoord="13" yCoord="28"/>
<arcpath arcPointType="false" id="3" xCoord="28" yCoord="1018"/>
<arcpath arcPointType="false" id="4" xCoord="253" yCoord="1018"/>
<arcpath arcPointType="false" id="5" xCoord="262" yCoord="972"/>
</arc>
<arc id="T33 to SK_" inscription="1" source="T33" target="P56"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="266" yCoord="957"/>
<arcpath arcPointType="false" id="1" xCoord="297" yCoord="957"/>
</arc>
<arc id="M6_ to T34" inscription="[0,inf)" source="P54" target="T34"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="100" yCoord="1070"/>
<arcpath arcPointType="false" id="1" xCoord="141" yCoord="1052"/>
</arc>
```

```
<arc id="T34 to M8" inscription="1" source="T34" target="P57"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="151" yCoord="1047"/>
<arcpath arcPointType="false" id="1" xCoord="177" yCoord="1047"/>
</arc>
<arc id="M8 to T35" inscription="[0,inf)" source="P57" target="T35"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="206" yCoord="1047"/>
<arcpath arcPointType="false" id="1" xCoord="231" yCoord="1047"/>
</arc>
<arc id="M6_ to T35" inscription="[0,inf)" source="P54" target="T35"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="101" yCoord="1077"/>
<arcpath arcPointType="false" id="1" xCoord="118" yCoord="1078"/>
<arcpath arcPointType="false" id="2" xCoord="238" yCoord="1078"/>
<arcpath arcPointType="false" id="3" xCoord="237" yCoord="1062"/>
</arc>
<arc id="T35 to M9" inscription="1" source="T35" target="P58"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="241" yCoord="1047"/>
<arcpath arcPointType="false" id="1" xCoord="282" yCoord="1047"/>
</arc>
<arc id="T31 to M6_" inscription="1" source="T31" target="P54"
type="normal" weight="2">
<arcpath arcPointType="false" id="0" xCoord="87" yCoord="897"/>
<arcpath arcPointType="false" id="1" xCoord="87" yCoord="1062"/>
</arc>
<arc id="ID to T36" inscription="[0,inf)" source="P5" target="T36"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="57" yCoord="237"/>
<arcpath arcPointType="false" id="1" xCoord="28" yCoord="238"/>
<arcpath arcPointType="false" id="2" xCoord="28" yCoord="1108"/>
<arcpath arcPointType="false" id="3" xCoord="328" yCoord="1093"/>
<arcpath arcPointType="false" id="4" xCoord="342" yCoord="1062"/>
</arc>
<arc id="Tc to T36" inscription="[0,inf)" source="P6" target="T36"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="57" yCoord="282"/>
<arcpath arcPointType="false" id="1" xCoord="28" yCoord="283"/>
<arcpath arcPointType="false" id="2" xCoord="28" yCoord="1108"/>
<arcpath arcPointType="false" id="3" xCoord="328" yCoord="1093"/>
<arcpath arcPointType="false" id="4" xCoord="342" yCoord="1062"/>
</arc>
<arc id="IDs_ to T36" inscription="[0,inf)" source="P51"
target="T36" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="176" yCoord="869"/>
<arcpath arcPointType="false" id="1" xCoord="343" yCoord="898"/>
<arcpath arcPointType="false" id="2" xCoord="342" yCoord="1032"/>
</arc>
<arc id="M9 to T36" inscription="[0,inf)" source="P58" target="T36"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="311" yCoord="1047"/>
```

```
<arcpath arcPointType="false" id="1" xCoord="336" yCoord="1047"/>
</arc>
<arc id="T36 to P65" inscription="1" source="T36" target="P59"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="342" yCoord="1062"/>
<arcpath arcPointType="false" id="1" xCoord="331" yCoord="1146"/>
<arcpath arcPointType="false" id="2" xCoord="296" yCoord="1150"/>
</arc>
<arc id="P68 to T38" inscription="[0,inf)" source="P60" target="T38"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="147" yCoord="1166"/>
<arcpath arcPointType="false" id="1" xCoord="147" yCoord="1197"/>
</arc>
<arc id="T38 to P69" inscription="1" source="T38" target="P61"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="151" yCoord="1212"/>
<arcpath arcPointType="false" id="1" xCoord="312" yCoord="1212"/>
</arc>
<arc id="P69 to T39" inscription="[0,inf)" source="P61" target="T39"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="341" yCoord="1212"/>
<arcpath arcPointType="false" id="1" xCoord="396" yCoord="1212"/>
</arc>
<arc id="T39 to P62" inscription="1" source="T39" target="P62"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="406" yCoord="1212"/>
<arcpath arcPointType="false" id="1" xCoord="432" yCoord="1212"/>
</arc>
<arc id="P62 to T40" inscription="[0,inf)" source="P62" target="T40"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="461" yCoord="1212"/>
<arcpath arcPointType="false" id="1" xCoord="471" yCoord="1212"/>
</arc>
<arc id="T40 to P63" inscription="1" source="T40" target="P63"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="481" yCoord="1212"/>
<arcpath arcPointType="false" id="1" xCoord="492" yCoord="1212"/>
<arcpath arcPointType="false" id="2" xCoord="507" yCoord="1212"/>
</arc>
<arc id="P63 to T41" inscription="[0,inf)" source="P63" target="T41"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="536" yCoord="1212"/>
<arcpath arcPointType="false" id="1" xCoord="561" yCoord="1212"/>
</arc>
<arc id="T41 to P65" inscription="1" source="T41" target="P65"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="571" yCoord="1212"/>
<arcpath arcPointType="false" id="1" xCoord="612" yCoord="1212"/>
<arcpath arcPointType="false" id="2" xCoord="612" yCoord="1152"/>
</arc>
<arc id="P65 to T42" inscription="[0,inf)" source="P65" target="T42"
type="timed" weight="1">
```

```
<arcpath arcPointType="false" id="0" xCoord="626" yCoord="1137"/>
<arcpath arcPointType="false" id="1" xCoord="651" yCoord="1137"/>
</arc>
<arc id="T42 to P66" inscription="1" source="T42" target="P66"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="661" yCoord="1137"/>
<arcpath arcPointType="false" id="1" xCoord="702" yCoord="1137"/>
</arc>
<arc id="P66 to T43" inscription="[0,inf)" source="P66" target="T43"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="731" yCoord="1137"/>
<arcpath arcPointType="false" id="1" xCoord="756" yCoord="1137"/>
</arc>
<arc id="T43 to P67" inscription="1" source="T43" target="P67"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="766" yCoord="1137"/>
<arcpath arcPointType="false" id="1" xCoord="792" yCoord="1137"/>
</arc>
<arc id="P67 to T44" inscription="[Deadline,Deadline]" source="P67"
target="T44" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="807" yCoord="1122"/>
<arcpath arcPointType="false" id="1" xCoord="807" yCoord="1062"/>
</arc>
<arc id="T44 to P68" inscription="1" source="T44" target="P68"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="807" yCoord="1032"/>
<arcpath arcPointType="false" id="1" xCoord="807" yCoord="1016"/>
</arc>
<arc id="P67 to T45" inscription="[0,Period]:1" source="P67"
target="T45" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="807" yCoord="1151"/>
<arcpath arcPointType="false" id="1" xCoord="807" yCoord="1197"/>
</arc>
<arc id="T45 to P69" inscription="[0,Period]:1" source="T45"
target="P69" type="transport" weight="1">
<arcpath arcPointType="false" id="0" xCoord="807" yCoord="1227"/>
<arcpath arcPointType="false" id="1" xCoord="807" yCoord="1257"/>
</arc>
<arc id="P69 to T46" inscription="[0,inf)" source="P69" target="T46"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="792" yCoord="1272"/>
<arcpath arcPointType="false" id="1" xCoord="751" yCoord="1272"/>
</arc>
<arc id="T46 to P70" inscription="1" source="T46" target="P70"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="741" yCoord="1272"/>
<arcpath arcPointType="false" id="1" xCoord="686" yCoord="1272"/>
</arc>
<arc id="P35 to T18" inscription="[0,inf)" source="P35" target="T18"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="822" yCoord="518"/>
<arcpath arcPointType="false" id="1" xCoord="796" yCoord="512"/>
```

```
</arc>
<arc id="P32 to T17" inscription="[0,inf)" source="P32" target="T17"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="673" yCoord="423"/>
<arcpath arcPointType="false" id="1" xCoord="651" yCoord="434"/>
</arc>
<arc id="P26 to T17" inscription="[0,inf)" source="P26" target="T17"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="696" yCoord="281"/>
<arcpath arcPointType="false" id="1" xCoord="643" yCoord="425"/>
</arc>
<arc id="P27 to T17" inscription="[0,inf)" source="P27" target="T17"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="641" yCoord="311"/>
<arcpath arcPointType="false" id="1" xCoord="639" yCoord="421"/>
</arc>
<arc id="P28 to T17" inscription="[0,inf)" source="P28" target="T17"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="615" yCoord="356"/>
<arcpath arcPointType="false" id="1" xCoord="631" yCoord="421"/>
</arc>
<arc id="P29 to T17" inscription="[0,inf)" source="P29" target="T17"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="607" yCoord="397"/>
<arcpath arcPointType="false" id="1" xCoord="631" yCoord="421"/>
</arc>
<arc id="P26 to T21" inscription="[0,inf)" source="P26" target="T21"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="687" yCoord="267"/>
<arcpath arcPointType="false" id="1" xCoord="552" yCoord="267"/>
<arcpath arcPointType="false" id="2" xCoord="570" yCoord="503"/>
</arc>
<arc id="T28 to P48" inscription="1" source="T28" target="P48"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="156" yCoord="672"/>
<arcpath arcPointType="false" id="1" xCoord="101" yCoord="672"/>
</arc>
<arc id="M1 to T34" inscription="[0,inf)" source="P4" target="T34"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="57" yCoord="192"/>
<arcpath arcPointType="false" id="1" xCoord="28" yCoord="193"/>
<arcpath arcPointType="false" id="2" xCoord="28" yCoord="898"/>
<arcpath arcPointType="false" id="3" xCoord="28" yCoord="1048"/>
<arcpath arcPointType="false" id="4" xCoord="142" yCoord="1042"/>
</arc>
<arc id="P11 to T27" inscription="[0,inf)" source="P11" target="T27"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="237" yCoord="431"/>
<arcpath arcPointType="false" id="1" xCoord="237" yCoord="657"/>
</arc>
<arc id="P59 to T37" inscription="[0,inf)" source="P59" target="T37"
type="timed" weight="1">
```

```
<arcpath arcPointType="false" id="0" xCoord="267" yCoord="1152"/>
<arcpath arcPointType="false" id="1" xCoord="211" yCoord="1152"/>
</arc>
<arc id="T37 to P60" inscription="1" source="T37" target="P60"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="201" yCoord="1152"/>
<arcpath arcPointType="false" id="1" xCoord="161" yCoord="1152"/>
</arc>
<arc id="P11 to T37" inscription="[0,inf)" source="P11" target="T37"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="222" yCoord="417"/>
<arcpath arcPointType="false" id="1" xCoord="12" yCoord="417"/>
<arcpath arcPointType="false" id="2" xCoord="12" yCoord="1122"/>
<arcpath arcPointType="false" id="3" xCoord="207" yCoord="1122"/>
<arcpath arcPointType="false" id="4" xCoord="207" yCoord="1137"/>
</arc>
<arc id="P25 to T17" inscription="[0,inf)" source="P25" target="T17"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="762" yCoord="372"/>
<arcpath arcPointType="false" id="1" xCoord="687" yCoord="372"/>
<arcpath arcPointType="false" id="2" xCoord="647" yCoord="430"/>
</arc>
<arc id="P33 to T17" inscription="[0,inf)" source="P33" target="T17"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="687" yCoord="456"/>
<arcpath arcPointType="false" id="1" xCoord="652" yCoord="443"/>
</arc>
<arc id="P24 to T20" inscription="[0,inf)" source="P24" target="T20"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="865" yCoord="378"/>
<arcpath arcPointType="false" id="1" xCoord="882" yCoord="387"/>
<arcpath arcPointType="false" id="2" xCoord="882" yCoord="597"/>
<arcpath arcPointType="false" id="3" xCoord="702" yCoord="597"/>
<arcpath arcPointType="false" id="4" xCoord="702" yCoord="522"/>
<arcpath arcPointType="false" id="5" xCoord="676" yCoord="512"/>
</arc>
<arc id="P13 to T38" inscription="[0,inf)" source="P13" target="T38"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="327" yCoord="357"/>
<arcpath arcPointType="false" id="1" xCoord="12" yCoord="357"/>
<arcpath arcPointType="false" id="2" xCoord="15" yCoord="1212"/>
<arcpath arcPointType="false" id="3" xCoord="141" yCoord="1212"/>
</arc>
<arc id="P19 to T42" inscription="[0,inf)" source="P19" target="T42"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="642" yCoord="237"/>
<arcpath arcPointType="false" id="1" xCoord="897" yCoord="237"/>
<arcpath arcPointType="false" id="2" xCoord="897" yCoord="942"/>
<arcpath arcPointType="false" id="3" xCoord="657" yCoord="942"/>
<arcpath arcPointType="false" id="4" xCoord="657" yCoord="1122"/>
</arc>
```

<arc id="T41 to P64" inscription="1" source="T41" target="P64"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="567" yCoord="1197"/>
<arcpath arcPointType="false" id="1" xCoord="567" yCoord="1151"/>
</arc>
<arc id="P30 to T19" inscription="[0,inf)" source="P30" target="T19"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="837" yCoord="417"/>
<arcpath arcPointType="false" id="1" xCoord="867" yCoord="417"/>
<arcpath arcPointType="false" id="2" xCoord="867" yCoord="567"/>
<arcpath arcPointType="false" id="3" xCoord="797" yCoord="566"/>
</arc>
</net>
<net active="true" id="Integrity1" type="P/T net">
<place id="Authenticated_msg" initialMarking="0" invariant="<
inf" markingOffsetX="0.0" markingOffsetY="0.0"
name="Authenticated_msg" nameOffsetX="65.0" nameOffsetY="2.0"
positionX="105.0" positionY="120.0"/>
<place id="Recieved_MAC_Value" initialMarking="0" invariant="<
inf" markingOffsetX="0.0" markingOffsetY="0.0"
name="Recieved_MAC_Value" nameOffsetX="69.0" nameOffsetY="-4.0"
positionX="300.0" positionY="60.0"/>
<place id="Cipher" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="Cipher"
nameOffsetX="30.0" nameOffsetY="44.0" positionX="240.0"
positionY="120.0"/>
<place id="MAC_Key" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="MAC_Key"
nameOffsetX="-5.0" nameOffsetY="35.0" positionX="300.0"
positionY="195.0"/>
<place id="Computed_MAC_Value" initialMarking="0" invariant="<
inf" markingOffsetX="0.0" markingOffsetY="0.0"
name="Computed_MAC_Value" nameOffsetX="76.0" nameOffsetY="39.0"
positionX="375.0" positionY="120.0"/>
<place id="Result" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="Result"
nameOffsetX="37.0" nameOffsetY="45.0" positionX="495.0"
positionY="120.0"/>
<transition angle="0" id="T9" infiniteServer="false" name="T9"
nameOffsetX="-18.0" nameOffsetY="188.0" positionX="30.0"
positionY="120.0" priority="0" urgent="false"/>
<transition angle="0" id="Split" infiniteServer="false" name="Split"
nameOffsetX="27.0" nameOffsetY="2.0" positionX="180.0"
positionY="120.0" priority="0" urgent="false"/>
<transition angle="0" id="Compute" infiniteServer="false"
name="Compute" nameOffsetX="35.0" nameOffsetY="-1.0"
positionX="300.0" positionY="120.0" priority="0" urgent="false"/>
<transition angle="0" id="Compare" infiniteServer="false"
name="Compare" nameOffsetX="36.0" nameOffsetY="-5.0"
positionX="450.0" positionY="120.0" priority="0" urgent="false"/>
<arc id="IntegrityCheck to A1" inscription="1" source="T9"
target="Authenticated_msg" type="normal" weight="1">

<arcpath arcPointType="false" id="0" xCoord="46" yCoord="132"/>
<arcpath arcPointType="false" id="1" xCoord="102" yCoord="132"/>
</arc>
<arc id="A1 to T3" inscription="[0,inf)" source="Authenticated_msg"
target="Split" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="131" yCoord="132"/>
<arcpath arcPointType="false" id="1" xCoord="186" yCoord="132"/>
</arc>
<arc id="T3 to MACValue" inscription="1" source="Split"
target="Recieved_MAC_Value" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="197" yCoord="127"/>
<arcpath arcPointType="false" id="1" xCoord="298" yCoord="78"/>
</arc>
<arc id="T3 to Cipher" inscription="1" source="Split"
target="Cipher" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="196" yCoord="137"/>
<arcpath arcPointType="false" id="1" xCoord="237" yCoord="133"/>
</arc>
<arc id="Cipher to T4" inscription="[0,inf)" source="Cipher"
target="Compute" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="266" yCoord="132"/>
<arcpath arcPointType="false" id="1" xCoord="306" yCoord="132"/>
</arc>
<arc id="Macscrt to T4" inscription="[0,inf)" source="MAC_Key"
target="Compute" type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="312" yCoord="192"/>
<arcpath arcPointType="false" id="1" xCoord="312" yCoord="147"/>
</arc>
<arc id="T4 to MacValue2" inscription="1" source="Compute"
target="Computed_MAC_Value" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="316" yCoord="132"/>
<arcpath arcPointType="false" id="1" xCoord="372" yCoord="132"/>
</arc>
<arc id="MACValue to T5" inscription="[0,inf)"
source="Recieved_MAC_Value" target="Compare" type="timed"
weight="1">
<arcpath arcPointType="false" id="0" xCoord="326" yCoord="77"/>
<arcpath arcPointType="false" id="1" xCoord="457" yCoord="127"/>
</arc>
<arc id="MacValue2 to T5" inscription="[0,inf)"
source="Computed_MAC_Value" target="Compare" type="timed"
weight="1">
<arcpath arcPointType="false" id="0" xCoord="401" yCoord="133"/>
<arcpath arcPointType="false" id="1" xCoord="456" yCoord="137"/>
</arc>
<arc id="T5 to P11" inscription="1" source="Compare" target="Result"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="466" yCoord="132"/>
<arcpath arcPointType="false" id="1" xCoord="492" yCoord="132"/>
</arc>
</net>
<net active="true" id="Integrity2" type="P/T net">

<place id="P19" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P19"
nameOffsetX="22.0" nameOffsetY="-2.0" positionX="105.0"
positionY="75.0"/>
<place id="P20" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P20"
nameOffsetX="38.0" nameOffsetY="7.0" positionX="180.0"
positionY="75.0"/>
<place id="P21" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P21"
nameOffsetX="4.0" nameOffsetY="10.0" positionX="255.0"
positionY="15.0"/>
<place id="P22" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P22"
nameOffsetX="12.0" nameOffsetY="3.0" positionX="300.0"
positionY="75.0"/>
<place id="P23" initialMarking="0" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P23"
nameOffsetX="29.0" nameOffsetY="-4.0" positionX="435.0"
positionY="75.0"/>
<place id="P24" initialMarking="1" invariant="< inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P24" nameOffsetX="-
5.0" nameOffsetY="35.0" positionX="240.0" positionY="165.0"/>
<transition angle="0" id="T26" infiniteServer="false" name="T26"
nameOffsetX="-5.0" nameOffsetY="35.0" positionX="60.0"
positionY="75.0" priority="0" urgent="false"/>
<transition angle="0" id="T1" infiniteServer="false" name="T1"
nameOffsetX="21.0" nameOffsetY="47.0" positionX="135.0"
positionY="75.0" priority="0" urgent="false"/>
<transition angle="0" id="T2" infiniteServer="false" name="T2"
nameOffsetX="8.0" nameOffsetY="40.0" positionX="240.0"
positionY="75.0" priority="0" urgent="false"/>
<transition angle="0" id="T3" infiniteServer="false" name="T3"
nameOffsetX="35.0" nameOffsetY="43.0" positionX="360.0"
positionY="75.0" priority="0" urgent="false"/>
<arc id="Integrity_C to P19" inscription="1" source="T26"
target="P19" type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="76" yCoord="87"/>
<arcpath arcPointType="false" id="1" xCoord="102" yCoord="87"/>
</arc>
<arc id="P19 to T1" inscription="[0,inf)" source="P19" target="T1"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="131" yCoord="87"/>
<arcpath arcPointType="false" id="1" xCoord="141" yCoord="87"/>
</arc>
<arc id="T1 to P20" inscription="1" source="T1" target="P20"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="151" yCoord="92"/>
<arcpath arcPointType="false" id="1" xCoord="177" yCoord="88"/>
</arc>
<arc id="T1 to P21" inscription="1" source="T1" target="P21"
type="normal" weight="1">

```
<arcpath arcPointType="false" id="0" xCoord="152" yCoord="82"/>
<arcpath arcPointType="false" id="1" xCoord="253" yCoord="33"/>
</arc>
<arc id="P21 to T3" inscription="[0,inf)" source="P21" target="T3"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="277" yCoord="37"/>
<arcpath arcPointType="false" id="1" xCoord="268" yCoord="28"/>
<arcpath arcPointType="false" id="2" xCoord="367" yCoord="82"/>
</arc>
<arc id="P20 to T2" inscription="[0,inf)" source="P20" target="T2"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="206" yCoord="87"/>
<arcpath arcPointType="false" id="1" xCoord="246" yCoord="87"/>
</arc>
<arc id="P24 to T2" inscription="[0,inf)" source="P24" target="T2"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="252" yCoord="162"/>
<arcpath arcPointType="false" id="1" xCoord="252" yCoord="102"/>
</arc>
<arc id="T2 to P22" inscription="1" source="T2" target="P22"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="256" yCoord="87"/>
<arcpath arcPointType="false" id="1" xCoord="297" yCoord="87"/>
</arc>
<arc id="P22 to T3" inscription="[0,inf)" source="P22" target="T3"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="326" yCoord="88"/>
<arcpath arcPointType="false" id="1" xCoord="366" yCoord="92"/>
</arc>
<arc id="T3 to P23" inscription="1" source="T3" target="P23"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="376" yCoord="87"/>
<arcpath arcPointType="false" id="1" xCoord="432" yCoord="87"/>
</arc>
</net>
<net active="true" id="Integrity3" type="P/T net">
<place id="P19" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P19"
nameOffsetX="26.0" nameOffsetY="-1.0" positionX="150.0"
positionY="60.0"/>
<place id="P20" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P20" nameOffsetX="-
3.0" nameOffsetY="20.0" positionX="285.0" positionY="5.0"/>
<place id="P21" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P21"
nameOffsetX="23.0" nameOffsetY="-4.0" positionX="255.0"
positionY="60.0"/>
<place id="P22" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P22"
nameOffsetX="32.0" nameOffsetY="43.0" positionX="300.0"
positionY="135.0"/>
```

```
<place id="P23" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P23"
nameOffsetX="8.0" nameOffsetY="-1.0" positionX="360.0"
positionY="60.0"/>
<place id="P24" initialMarking="0" invariant="&lt; inf"
markingOffsetX="0.0" markingOffsetY="0.0" name="P24"
nameOffsetX="25.0" nameOffsetY="3.0" positionX="450.0"
positionY="60.0"/>
<transition angle="0" id="T41" infiniteServer="false" name="T41"
nameOffsetX="52.0" nameOffsetY="50.0" positionX="90.0"
positionY="60.0" priority="0" urgent="false"/>
<transition angle="0" id="T1" infiniteServer="false" name="T1"
nameOffsetX="23.0" nameOffsetY="51.0" positionX="195.0"
positionY="60.0" priority="0" urgent="false"/>
<transition angle="0" id="T2" infiniteServer="false" name="T2"
nameOffsetX="20.0" nameOffsetY="42.0" positionX="300.0"
positionY="60.0" priority="0" urgent="false"/>
<transition angle="0" id="T3" infiniteServer="false" name="T3"
nameOffsetX="23.0" nameOffsetY="42.0" positionX="405.0"
positionY="60.0" priority="0" urgent="false"/>
<arc id="T41 to P19" inscription="1" source="T41" target="P19"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="106" yCoord="72"/>
<arcpath arcPointType="false" id="1" xCoord="147" yCoord="72"/>
</arc>
<arc id="P19 to T1" inscription="[0,inf)" source="P19" target="T1"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="176" yCoord="72"/>
<arcpath arcPointType="false" id="1" xCoord="201" yCoord="72"/>
</arc>
<arc id="T1 to P21" inscription="1" source="T1" target="P21"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="211" yCoord="77"/>
<arcpath arcPointType="false" id="1" xCoord="252" yCoord="73"/>
</arc>
<arc id="T1 to P20" inscription="1" source="T1" target="P20"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="212" yCoord="67"/>
<arcpath arcPointType="false" id="1" xCoord="284" yCoord="24"/>
</arc>
<arc id="P21 to T2" inscription="[0,inf)" source="P21" target="T2"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="281" yCoord="72"/>
<arcpath arcPointType="false" id="1" xCoord="306" yCoord="72"/>
</arc>
<arc id="P22 to T2" inscription="[0,inf)" source="P22" target="T2"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="312" yCoord="132"/>
<arcpath arcPointType="false" id="1" xCoord="312" yCoord="87"/>
</arc>
<arc id="T2 to P23" inscription="1" source="T2" target="P23"
type="normal" weight="1">
```

```
<arcpath arcPointType="false" id="0" xCoord="316" yCoord="72"/>
<arcpath arcPointType="false" id="1" xCoord="357" yCoord="72"/>
</arc>
<arc id="P23 to T3" inscription="[0,inf)" source="P23" target="T3"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="386" yCoord="74"/>
<arcpath arcPointType="false" id="1" xCoord="411" yCoord="77"/>
</arc>
<arc id="P20 to T3" inscription="[0,inf)" source="P20" target="T3"
type="timed" weight="1">
<arcpath arcPointType="false" id="0" xCoord="310" yCoord="23"/>
<arcpath arcPointType="false" id="1" xCoord="412" yCoord="67"/>
</arc>
<arc id="T3 to P24" inscription="1" source="T3" target="P24"
type="normal" weight="1">
<arcpath arcPointType="false" id="0" xCoord="421" yCoord="72"/>
<arcpath arcPointType="false" id="1" xCoord="447" yCoord="72"/>
</arc>
</net>
<k-bound bound="3"/>
</pnml>
```