MITIGATE DENIAL OF SERVICE ATTACKS IN MOBILE AD-HOC NETWORKS

ALBANDARI ALSUMAYT

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

Doctor of Philosophy

School of Science and Technology
Nottingham Trent University

March 2017

A Copyright statement

Acknowledgment

First and foremost, I would like to thank almighty Allah (God) who gave me the power, patience, health, environment and people to support me during my PhD study, and blessed me in completing this research.

In addition, I would like to express my deepest gratitude towards my Director of Study, Dr John Haggerty, for all his advice, valuable support, guidance, constructive comments, patience, kind encouragement, time and knowledge, which he provided during my study and without which I would never have reached this stage.

I would like to sincerely thank my co-supervisor, Professor Ahmad Lotfi, for all his advice, guidance and support during my study at the university.

I would like especially to thank my husband, Sattam, for all his help, endless love, support, patience and continuous encouragement during my study, without which the research could not have been completed. I am truly thankful and indebted to my beloved three kids Lyan, Abdullah, and Reem for all their patience, pure love and their innocent smiles which have helped me forget me my tiredness during the writing of this thesis.

I would like to thank my closest family members for their love and support. My mum, no words can be enough to ever thank her. I would say thank you for your love, taking care of my children and all your help during this study. My father, thank you for your advice and support. My sweet sisters, I would say thank you for everything, love, and encouraging me to strive towards excellence. In particular, I want to thank my sister Monirah, as she visits me regularly and has cheered me up and supported me in my hard times.

I would also like to extend my sincere thanks to my friends in Manchester, Nottingham, and Saudi Arabia for their understanding, help, love and support during these years of study.

I would also like to thank my uncle, Saad; although he passed away in 2013, I wish he were still here today. He encouraged me to achieve at this level, and I will always be grateful for his advice, support, and love. Last but not least, I thank my father-in-law, Abdullah, who recently passed away. I very much wish that he were among us today, as he was a constant source of hope and advice.

Abstract

Wireless networks are proven to be more acceptable by users compared with wired networks for many reasons, namely the ease of setup, reduction in running cost, and ease of use in different situations such as disasters recovery. A Mobile *ad-hoc* network (MANET) is as an example of wireless networks. MANET consists of a group of hosts called nodes which can communicate freely via wireless links. MANET is a dynamic topology, self-configured, non-fixed infrastructure, and does not have any central administration that controls all nodes among the network. Every device, used in day-to-day living, is assumed to be a network device, and it is managed using Internet Protocols (IP). Information on every electronic device is collected using infrared sensors, voice or video sensors, Radio-Frequency Identification (RFID), etc. The new wireless networks and communications paradigm known as Internet of Things (IoT) is introduced which refers to the range of multiple interconnected devices which communicate and exchange data between one another.

MANET becomes prone to many attacks mainly due to its specifications and challenges such as limited bandwidth, nodes mobility and limited energy. This research study focuses specifically on detecting Denial of Service attack (DoS) in MANET. The main purpose of DoS attack is to deprive legitimate users from using their authenticated services such as network resources. Thus, the network performance would degrade and exhaust the network resources such as computing power and bandwidth considerably which lead the network to be deteriorated.

Therefore, this research aims to detect DoS attacks in both Single MANET (SM) and Multi MANETs (MM). A novel Monitoring, Detection, and Rehabilitation (MrDR) method is proposed in order to detect DoS attack in MANET. The proposed method is incorporating trust concept between nodes. Trust value is calculated in each node to decide whether the node is trusted or not. To address the problem when two or more MANETs merge to become one big MANET, the novel technique of Merging Using MrDR (MUMrDR) is also applied to detect DoS attack. As the mobility of nodes in MANET, the chance of MANETs merge or partition occurs. Both centralised and decentralised trust concepts are used to deal with IP address conflict and the merging process is completed by applying the MUMrDR method to detect DoS attacks in MM. The simulation results validate the effectiveness in the proposed method to detect different DoS attacks in both SM and MM.

Publications

The following publications result from this research by the author during the course of this doctorate study.

Journal papers

- Alsumayt, A., Haggerty, J. and Lotfi, A., "Using Trust to Detect Denial of Service Attacks in the Internet of Things Over MANETs" , *the International Journal of Space-Based and Situated Computing (IJSSC),* forthcoming 2017.
- A journal paper titled: " Detect DoS attacks using decentralised trust concept in MANETs" to be submitted to Computers and Security Journal.

Conference papers

1. Alsumayt, A. and Haggerty, J., 2014. Using Trust Based Method to Detect DoS Attack in MANETs. *PGNet: Proceedings of the 15th Annual Postgraduate Symposium on the convergence of Networking, Broadcasting, and Telecommunications* , June. 2014. Liverpool John Moores university. Liverpool. UK.
2. Alsumayt, A.F. and Haggerty, J., 2014. A Taxonomy of Defence Mechanisms to Mitigate DoS Attacks in MANETs. In *Proceedings of the Tenth International Network Conference (INC 2014)* (p. 3). Lulu. com.
3. Alsumayt, A. and Haggerty, J., 2014, August. A survey of the mitigation methods against dos attacks on manets. In *Science and Information Conference (SAI), 2014* (pp. 538-544). IEEE.
4. Alsumayt, A., Haggerty, J. and Lotfi, A., 2015, September. Performance, Analysis, and Comparison of MrDR Method to Detect DoS Attacks in MANET. In *Intelligence and Security Informatics Conference (EISIC), 2015 European* (pp. 121-124). IEEE.
5. Alsumayt, A., Haggerty, J. and Lotfi, A., 2015, October. Comparison of the MrDR method against different DoS attacks in MANETs. In *Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference on* (pp. 219-224). IEEE.

6. Alsumayt, A., Haggerty, J. and Lotfi, A., 2016, March. Detect DoS Attack Using MrDR Method in Merging Two MANETs. In *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (pp. 889-895). IEEE.

In addition to these publications, the following research posters are also presented:

Posters

1- Postgraduate conference SPARC in Salford University on 3rd -5th June 2013, participated with a poster title: (Be careful your computer is in danger).
2- STAR conference 2014 , school of science and Technology in Nottingham Trent University, on 7th -8th May 2014.participated with a poster title: (Using Trust Based Method to Detect Denial of Service Attack in MANETs)
3- Participate with a poster in the 8th Saudi conference in London, Queen Elizabeth, 31st January 2015 – 1st February 2015. Poster title, (Using MrDR trust based method to detect DoS attack in MANET). The 8th Saudi Students Conference is sponsored by the Saudi Ministry of Higher Education and King Abdullah University of Science and Technology (KAUST). It took place at the hosting university, Imperial College London, United Kingdom.
4- STAR conference 2015, school of science and Technology in Nottingham Trent University, on May 2016 Participated with a poster title: (Detect DoS attack using MrDR method in merging two MANETs).

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AA	Address Authority
AACK	Adaptive Acknowledgment
ACCM	Acceptance of merger
ACK	Acknowledgment Packet
ACN	Address Conflict Notice
AIPAC	Automatic IP Address Configuration
AODV	Ad-hoc On-demand Distance Vector
ATV	Accomplichment Trust Value
BEFORE	BEst FOrwarding Route Estimation
BET	Behavioural Trust
BRE	Bit Rate Error
BSS	Basic Service Set
CA	Certificate Authority
CAN	Campus Area Network
CC	Common Criteria
CFAA	Conflict-Free Auto-configuration Addresses
CIA	Confidentiality, Integrity, and Availability
COLT	Collaboration Trust
CONFIDANT	Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTwork
ConfM	Confirmation of Merger
CORE	COllaborative Reputation
CTV	Check Trust Value
DAAP	Dynamic Address Allocation Protocol
DACP	Dynamic Address Configuration Protocol
DAD	Duplicate Address Detection
DAP	Duplicate Address Probe
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DICOTIDS	Distributed Cooperative Trust based Intrusion Detection
DIs	Direct interactions
DOE	Design of experiments
DoS	Denial of Service
DPM	Deterministic Packet Marking

DSDV	Destination Sequenced Distance Vector
DSR	Direct Source Routing
DYMO	DYnamic MANET On-demand
EAACK	Enhanced Adaptive ACKnowledgment
EAL	Evaluation Assurance Level
ESS	Extended Service Set
ETT	Equation Total Time
E-TWOACK	Enhanced TWOACK
HAN	Home Area Network
HID	Host Identifier
HMM	Hidden Markov Model
HTV	Honesty Trust Value
ICMP	The Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	The Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoE	Internet of Everything
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
ISO	International Organisation for Standardisation
IT	Information Technology
ITrace	ICMP traceback scheme
LAN	Local Area Network
LARS	A Locally Aware Reputation System
MAN	Metropolitan Area Network
MANET	Mobile ad hoc Network
Mbps	Megabits per second
MCHK1	Merge Check 1
MCHK2	Merge Check 2
MM	Multi MANET
MRA	Message Report Authentication
MrDR	Monitoring, Detection, and rehabilitation
MREQ	Merge Request
MUMrDR	Merging Using MrDR
NIC	Network Interface Card

OCEAN	Observation-based Cooperation Enforcement in Ad hoc Networks
OSI	Open Systems Interconnection basic reference model
OSPF	Open Shortest Path First
Otcl	Object-oriented support
PACMAN	Passive Auto-Configuration for Mobile Ad hoc Networks
PAN	Personal Area Network
PDHCP	Prime DHCP
PPM	Packet marking schemes
PRNET	Packet Radio Networks
REPT	Reply IP Table
REQIP	Request IP Address
RET	Reference Trust
RFID	Radio-Frequency Identification
RREP	Route Reply
RREQ	Route Request
RTV	Reputation Trust Value
SA	Simple Averaging
SCADA	Supervisory Control And Data Acquisition
SFP	Security Function Policy
SFR	Security Functional Requirement
SHDACP	Scalable Hierarchical Distributive Auto Configuration
SM	Single MANET
SORI	Secure and Objective Reputation based Incentive
SPRITE	Simple cheat-proof credit-based system
ST-AODV	Simple Trust AODV
SURAN	Survivable Adaptive Radio Networks
SWV	Simple trust-based Weighted Voting
TCP SYN	Transfer Control Protocol Synchronize
TCP/IP	Transmission Control Protocol/ Internet Protocol
T-DAAP	Tree based Dynamic Address Auto-configuration Protocol
TEAP	Trust Enhanced Anonymous on-demand routing Protocol
TF	Trust Factor
TORA	Temporally Ordered Routing Algorithm
TSAODV	Trusted Secure AODV routing protocol
TSR	Trust based Source Routing protocol
TTSV	Total Trust Value

TVs	Trust Values
TWOACK	TWO network-layer ACKnowledgment-based scheme
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WMN	Wireless mesh network
WPAN	Wireless Personal Area Network
WSN	Wireless sensor network
WWAN	Wireless Wide Area Network
WWW	World Wide Web
ZRP	Zone Routing Protocol
ZSBT	Zone Sampling-Based Trace

Chapter 1: Introduction

The current wireless network technology revolution has occurred due to the implementation and availability of many wireless devices in different sectors, such as in the military arena, at conferences and in cafes. A wireless network enables two or more computers to connect with each other without using cables. There are many types and modes of wireless network communication, each of which has a different architecture. Available architectures include *ad-hoc*, peer-to-peer, infrastructure, Wi-Fi, and WiMAX.

A wireless *ad-hoc* network involves a set of mobile devices, or hosts that can connect to each other wirelessly with no requirement for access, or centralised points. This network type can be employed as long as the devices are both within a specified range. The devices can connect and share data via radio waves. A Mobile *Ad-hoc* Network (MANET) is one type of ad-hoc network and it is the focus of this research. Due to the nature of MANETs, they are prone to many attacks, such as Denial of Service (DoS) attacks.

This chapter outlines the problem addressed by this research, the aims and objectives of this research, and thesis novel contributions.

1.1 Problem definition

MANET is a temporary, self-configuring, wireless network that consists of nodes, which can communicate with each other without any fixed infrastructure. MANET has a dynamic topology, meaning nodes can move in and out of the network frequently without any previous announcement. As such, nodes can move independently in any direction. Nodes can refer to smart phones, tablets, MP3 players, iPads, personal computers, or even laptops. In addition, nodes in MANET do not have a central administration point (Jain and Buksh, 2016).

Instead, each node in MANET behaves as a router and a host by sending and receiving packets. As such, each node can communicate separately with each other

node and may provide services to, or act as a client, with other network entities. MANET has received much interest as it is easy to use and setting-up the network architecture is not complex. For example, it can be used in emergency relief situations, such as search, disasters, and rescue, military services, such as use in transport and by soldiers, civilian usage, such as at airports, conferences, cafes, lectures and planes, and personal usage, such as personal laptops, wrist watches, and smart phones (Agrawal and Chauhan, 2015). This type of network is increasingly important with society's move towards Internet of Things (IoT) computing. Detailed of IoT paradigm will be presented in Chapter 3.

Due to the nature of MANET, many security concerns and challenges have been raised. MANET contains a number of flaws that make it an easy target for attackers. First, as each node can communicate with each other node separately, there is no central computer capable of monitoring the entire network and ensuring correct behaviours by participants. Second, nodes can move arbitrarily. As such, the topology changes unpredictably and frequently. Third, each node needs energy to communicate with another node. This means that power constrains are a significant concern in MANET. Scalability is another concern in MANET as each node can access the network and also leave dependently. As such, the number of nodes within the network often changes and is unpredictable and particularly the case as MANETs merge. The fifth issue is that the bandwidth in MANET is constrained compared to other wireless networks, and the links between variables have a low capacity.

Wireless networks are vulnerable to many problems, such as interference, external noise, and signal effects. All of these factors mean that MANET is vulnerable to numerous internal and external attacks. For example, eavesdropping, fabrication, and DoS attacks can occur in MANET due to these vulnerabilities. The aim of these attacks differs and requires different responses from the security services to ensure the maintenance of Confidentiality, Integrity, and Availability (CIA) (Conti and Giordano, 2014). More details about CIA are provided in Chapter 2.

There are many security services that are required from MANET and any other network. Confidentiality, integrity, availability, non-repudiation, authorisation and authentication are the main security services that are required for a communications system to be considered safe. Confidentiality ensures that the transmitted data is only read at the intended destination, thus protecting transmitted data from eavesdropping. Integrity protects the transmitted message from

modification by adversaries, meaning that only the intended recipients can edit the data. Availability ensures that the data is available whenever the legitimate users need to access it. In addition, it ensures that data can be transmitted from the source to the target destination promptly (Berman and Mukherjee, 2006).

The most critical and crucial type of attack in modern society is known as a DoS (Malhotra et al., 2013). In this research, the focus is specifically on this type of attack. DoS attacks paralyse, deprive and disrupt the availability of the network, thereby preventing legitimate users from accessing the services. Also, this kind of attack reduces the performance of the network and can cause harm in many ways, both financially and in terms of resources (Patel and Sharma, 2013). For example, if the MANET connects to the Internet (connected MANET) and one of the most popular sites, such as Amazon or eBay, is subject to a DoS attack, even for a short time, the financial losses would be huge (Lotfy and Azer, 2013). Moreover, DoS attacks are a severe problem because many users may not realise that they are under attack, instead thinking that the delay is merely the result of network congestion (Ponsam and Srinivasan, 2014).

Distributed DoS (DDoS) attacks utilise many devices such as botnets or zombies as well as multiple Internet connections to launch an attack, whereas DoS attacks are launched by employing a single device and a single Internet connection (Sharma et al., 2013a). In this thesis, DoS and DDoS are used interchangeably.

It will be demonstrated later on in this thesis that, traditional approaches to mitigate DoS attacks in fixed-wire networks cannot be applied to MANET due to certain characteristics it presents. There are many methods that can be used to detect a DoS attack in MANET, such as distributed firewalls, filtering, IDS (Intrusion Detection System) and so on. The majority of existing methods used to detect DoS attacks have advantages and disadvantages. For example, there are some limitations in the use of distributed firewalls because of the vulnerabilities of host networks. Essentially, if users do not keep systems up to date, some complex systems can succeed in launching an attack that firewalls are unable to distinguish from normal traffic (Alicherry et al., 2008). These existing methods with their advantages and disadvantages are illustrated in detail in Chapter 4.

The use of ‘trust concepts’ to detect DoS attacks in MANET are studied in this research. The proposed method is called **MrDR** (**M**onito**r**ing, **D**etection, and **R**ehabilitation) and it is used in this research to detect DoS attacks in both Single MANET (SM) and Multiple MANET (MM) systems. MM systems refer to those

with two merged MANETs as well as those with more than two MANETs. This method relies on the use of the trust concept between nodes in order to detect DoS attacks in the early stages. *Monitoring* the network ensures that any irregular activity is detected as early as possible. *Detection* identifies misbehaving nodes and determines whether they are malicious or selfish. *Rehabilitation* refers to the return of the network to a secure state. In order to achieve this system's goals, this approach recognises the issues discussed above, and uses a trust-based approach to mitigate DoS attacks in MANETs.

The Merging Using MrDR (MUMrDR) method will be used to detect DoS attacks when merging multiple MANETs. Two situations will be discussed in this thesis: merging two MANETs; and merging four MANETs. The reason why these numbers are selected is due to the fact that two which are related to any standard networks and four MANETs reflects the situation when there are more than two networks while this number can be increased by five, six, or more networks. According to the trust concept, MUMrDR would detect DoS attacks when merging MANETs. Another issue that must be considered is whether the IP addresses in the network are unique after merging. Centralised and decentralised trust concepts are used to help MM to merge in this study.

1.2 Research aims and objectives

The aim of this research project is to investigate and recommend a novel method for the identification of DoS, specifically in MANET. The two types of MANET discussed above, SM and MM will be considered in this research. This method will implement the trust concept in an effort to encourage cooperation between nodes to detect, respond, and rehabilitate the network following an attack. Furthermore, this method rehabilitates misbehaving nodes in an attempt to reuse them, which could drastically increase the performance of the network.

In order to achieve the above aim, the following project objectives are identified:

- To study and understand the nature of MANET and its security challenges and vulnerabilities. The research will focus on DoS attacks in particular in order to determine how they occur, the various types, and the threat they pose to MANET architecture, resources, and users.

- To critically evaluate existing countermeasures used to identify DoS attacks on MANET and identify their advantages and disadvantages. This will highlight any flaws in the existing detection methods.
- To design and implement a novel method for the early identification of DoS attacks in both SM and MM, acknowledging the disadvantages of existing methods.
- To evaluate the proposed novel method in an effort to establish its strengths and weaknesses, particularly with respect to SM, under various types of DoS attack.
- To compare the performance of the proposed method with existing methods using the trust concept to detect DoS attacks on SM.
- To use the trust concept to assign IP addresses on MM.
- To test the proposed method in MM where two MANETs merge, and in MM where more than two MANETs merge. This is the first attempt to use the trust concept to detect DoS attacks during the merger of MM.

1.3 Thesis contributions

There are **four novel contributions** to this research. **First**, the MrDR method is used to detect DoS attacks in SM. This method involves calculating the trust value for each node in the network. However, this value is short-lived and needs to be recalculated each time the node displays a different behaviour. This method enables detection and response to attacks in a timely manner whilst preserving network, coup, and power resources. In addition, this method allows rehabilitation of the network following an attack, to mitigate the resultant damage. Rehabilitation is important in MANETs, with their dynamic topology, as nodes cannot be continuously of a single value.

Second, the trust values of nodes will be used to assign IP addresses in the network when new nodes join or when networks merge. Thus, IP conflict would be controlled in a MANET as the trust value of each node would be continuously updated and all information, such as vacant IP addresses, would be up to date. It is important to emphasise that this is the first work that presents this trust concept to assign IP addresses in during MM merger.

Third, the Merging Using MrDR (MUMrDR) method will be used to detect a type of DoS attacks when two MANETS merge. Many factors need to be considered in this situation, such as assigning IP addresses and ascertaining that there is no IP conflict after

merging. This is the first work to use the trust concept to detect DoS attack when merging two MANETs. Centralised trust concept will be used in this situation.

Fourth, the MUMrDR method will be used to detect four types of DoS attacks when four MANETs are about to merge. Decentralised trust concept will be used in this scenario to complete the merging process. Again, this is the first work to use the trust concept to detect DoS attacks when more than two MANETs merge. These contributions provide protection during attacks on MANETs.

The MrDR method is considered novel for many reasons. *First*, trust has only two values: trusted (= 1) and untrusted (= 0). This is the first method known to assume this concept as a binary (trusted =1 or untrusted =0). The reason for why there are only two values of trust in the proposed method rather than a continuous value in a range is to safe the power of nodes in MANET as MANET has limited energy; therefore, the node can be trusted or not. *Second,* this method uses different values to calculate the total trust value. Because many challenges exist in MANETs – such as dynamic topology, non-fixed infrastructure, and the absence of central administration – calculated trust must be based on many factors. *Another novel component* is that trust is defined as a temporal action, which needs to be calculated regularly. Nodes in MANET move in and out of the network frequently. Trust values therefore need to be recalculated regularly. The rehabilitation of misbehaving nodes will be considered in this study as nodes cannot always be trusted in an environment such as MANET with its dynamic topology.

The ability of this method to detect many different types of DoS attack in the MANET environment – both SM and MM – is also novel. It is worth noting that no previous method has been capable of detecting DoS attacks when two or more MANETs are about to merge. In such an environment it is vital that the MANET is able to detect misbehaving nodes in real time, as nodes can enter and exit the network frequently. In addition, this method is heuristic, allowing it to monitor the network in numerous possible scenarios, such as the merging of two or more MANETs.

1.4 Chapters summaries

The research in this thesis is organised into eight chapters. Every chapter starts with a brief introduction that highlights the main overview and what is going to be discussed in the chapter. At the end of each chapter, a brief summary is presented. The next seven

chapters contain more detailed information about the history of this research and how the contributions are presented in different aspects. Figure 1.1 illustrates how the thesis is structured and how the chapters are connected.

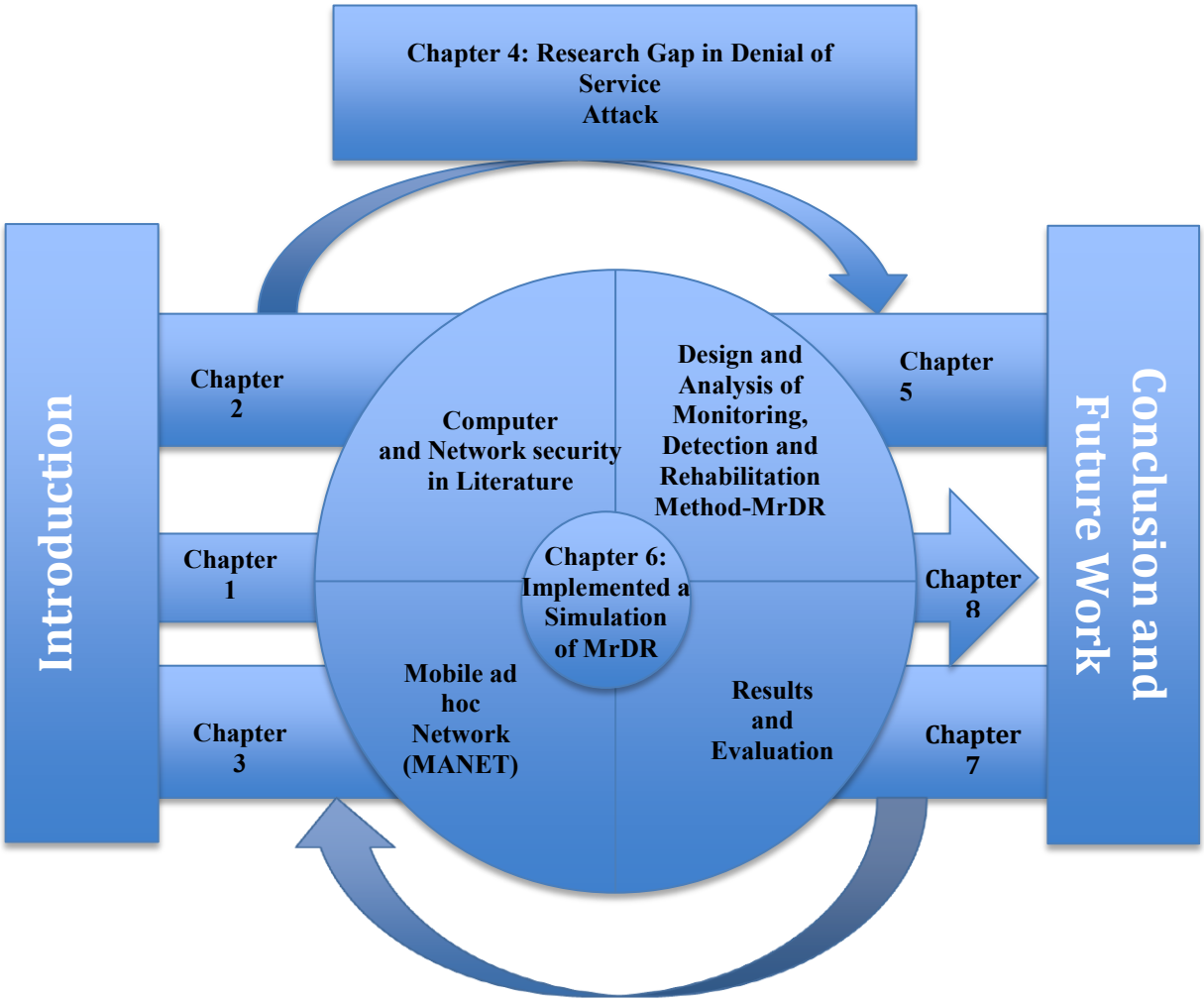

Figure 1.1. Thesis structure.

Chapter two (Computer and Network security in Literature)-

In this chapter, computer and network security are defined. Increased use of wireless networks has led to an increase in security threats. Security services refer to the CIA Triad, as well as Authentication and Non-Repudiation (or Accountability). These services are essential in ensuring that effective security is implemented. MANET, an example of a wireless network, has been controversial due to its uncomplicated nature. As such, security in wireless networks such as MANET is important because there is no central administration to monitor all devices or nodes within the network. Security threats

against wireless networks, such as DoS attacks, could lead to a loss in revenue, time and reputation.

Chapter three (Mobile ad-hoc network (MANET)-

Chapter three gives a detailed explanation and definition of MANET itself, such as its history, features and the routing protocols used in it. Three types of routing protocol are used in MANET and are different in their performance and usage. Due to the ease of infrastructure, MANET is used in many sectors such as disaster relief situations. However, due to the special characteristics of MANET, it is also vulnerable to many attacks. The security challenges are discussed briefly in this chapter. In addition, attacks types based on their location or on their performance are debated. The definition of a DoS attack is also presented and how this attack takes place is also explained. Different DoS attacks according to the different layers in the TCP/IP model are also discussed, along with attack definitions. A definition and description of IoT is also outlined in this chapter.

Chapter four (Research Gap in Denial of Service Attack)-

This chapter provides and discusses the comprehensive review of relevant work in this area based on three dimensions: traditional methods to detect DoS attacks in MANET, methods which are based on trust concept to detect DoS attacks in MANET, and IP address configuration methods in MANET. Thus, this area includes a broad range of topics worth investigating and comparing in terms of their performance. Identifying the advantages and disadvantages of the available literature helps to improve the proposed method considerably. This method tries to take the features of the existing studies and bypass any limitations, in order to improve the method to combat a DoS attack in a challenging environment such as MANET.

Chapter five (Design and Analysis of Monitoring, Detection and Rehabilitation Method-MrDR)-

This section illustrates the design and hypothesis of the proposed method with its different stages, elements and performance. Moreover, an example, which shows the performance of the proposed method, is explained in detail in this chapter. However, the proposed method also applies with MM, and analysis of different trust concepts used, such as centralised and decentralised trust concepts are examined in order to check the IP address and complete the merging process smoothly. The experimental design in three different scenarios would express the robustness of the proposed method in both SM and MM.

Chapter six (Implemented a Simulation of MrDR)-

This chapter describes the simulation scenario for the three experiments. The first experiment on SM is where the proposed method would be applied to detect different DoS attacks: wormhole attack; blackhole; grayhole and jellyfish attack. These attacks would be detected on four experiments as each study will measures the network performance every specific time depends on the experiment time. Three aspects of network performance are considered: network throughput; packet delivery ratio and packet delay ratio. Furthermore, the proposed method will be applied on MM and two experiments will be conducted to evaluate the effectiveness of the proposed method in this situation. The first experiment will be on two independent configured MANETs and it uses the centralised trust concept to merge. The second experiment will be on four independent configured MANETs. Decentralised trust concept in used in this experiment. Grayhole attacks will be used with two MANETs. In addition, all four types of DoS, which are used in the first experiment, also will be used when four MANETs merge. The complete scenario of each experiment is illustrated and discussed in detail in this chapter.

Chapter seven (Results and Evaluation)-

Here the overall findings of the three experiments are presented. The comparison between the performances of each attack in the first experiment indicates that the performance of the proposed method would vary from one attack to another. In addition, in each experiment on MM, the network performance will be measured multiple times pre-merging and post-merging. Subsequently, the evaluation of the performance of the proposed method on SM will be conducted between these different DoS attacks. In addition, one method, which is based on trust to detect misbehaving nodes (mentioned in the literature section in Chapter 4), will be used to evaluate this proposed method. However, there is no existing method to study the case of detecting DoS attacks in the merging MM scenario, therefore there is no evaluation made at this stage as it is unique.

Chapter eight (Conclusions and Future Work)-

An overall conclusion pertaining to this research is drawn in this chapter. It also describes how the research objectives were attained, the strengths and limitations of the study, as well as the proposal of a number of recommendations for future work. These recommendations would improve the study to test and cover different scenarios.

1.5 Chapter summary

The goal of this chapter is to illustrate the problem area of this thesis. In addition, the aims and objectives of this thesis are presented. Furthermore, the main four contributions that are proposed in the thesis are also discussed. There are many concerns related to the security of data in wireless networks because they do not depend on routers which control packets, unlike wired networks. In addition, wireless *ad-hoc* networks raise greater concerns than other infrastructures or managed wireless networks because there is no access point. MANET is a type of *ad- hoc* wireless network that consists of nodes. Each node is considered to be both a router and a host, sending and receiving packets. As MANETs lack any central supervision point, MANETs are prone to attacks, such as eavesdropping, fabrication, and DoS attacks. The focus of this study is to detect DoS attacks in MANETs; both SM and MM. The MrDR method is used in this research to detect DoS attacks in SM and MM. This method uses the trust concept to calculate the trust value for each node. The next chapter will explain the computer and network security definitions. Moreover, the three pillars of security (or the CIA triad) will be explained in detail. Other aspects that related to the CIA triad also discussed. Furthermore, the importance of security to both customers and industry is posited from many aspects.

Chapter 2: Computer and Network Security in Literature

Both wireless and wired networks are used for communication between devices and data sharing. However, these networks differ in terms of topology, transmission method and features. More recently, wireless networks are used widely due to the ease of installation and low requirements, important in certain situations such as emergency relief at disasters. Network security becomes the major concern due to the extra demands on the network. There are many security requirements that need consideration in order to ensure that a network is secured. In this chapter, different types of network, and wireless network, will be discussed, focussing on wireless networks. The comparison between wired and wireless networks will be explained. Also, the available security services will be outlined and the importance of security for both customers and the industrial sector will be discussed.

2.1 Types of network

There are four main types of network *based on the geographical area* they cover: Wide Area Network (WAN), Metropolitan Area Network (MAN), Local Area Network (LAN), and Personal Area Network (PAN) (Kizza, 2009). WANs cover large geographical areas and usually consist of many connected LANs. In contrast, LANs cover small geographical areas such as buildings or schools. An example of this type of setup is a school LAN network which, when it connects to the Internet, becomes part of a WAN.

MANs are larger than LANs. MAN refers to a computer network across an entire college campus, city, or small region, and is typically limited to a single site or even building. MANs may cover an area up to tens of miles depending on their configuration. Usually, many LANs are connected together to form a MAN. This type of network is commonly used on sites such as college campuses, and is sometimes referred to as a Campus Area Network (CAN). A PAN is a computer

network that is organised around an individual person in a single building or location, such as a small office. Typically, a PAN could include one or more telephones, computers, video game consoles, or other personal devices. When several individuals use the same network in a residence, then the network is referred to as a Home Area Network, or HAN. In a typical setup, a residence might have a single wired Internet connection linked to a modem. This modem can provide wired and wireless connections for various gadgets. A single computer in the network can manage from and also can access to the network from any device. PAN has many uses. For instance, it allows a user to send a document to a wireless printer in another room (Han, 2012).

A wireless equivalent of each of these network types exists: Wireless Wide Area Network (WWAN); Wireless Metropolitan Area Network (WMAN); Wireless Local Area Network (WLAN); and Wireless Personal Area Network (WPAN). A comparison of the coverage between the different wireless networks indicated that WWAN gives a low performance, WPAN gives a moderate performance, and WMAN and WLAN give high performances (Hucaby, 2014).

2.1.1 Wired network

Wired network refers to the physical configuration of devices and it is also called an Ethernet network. A wired network is a collection of two or more devices, such as computers, printers, scanners or even a piece of network hardware such as a router, hub, or switch, which are linked using Ethernet cables. A wired network can be used as part of other wireless or wired networks. In order to connect a device to the network using Ethernet cables, a Network Interface Card (NIC) must be included in the device.

The fastest wired network protocol is Ethernet, as it provides a connection speed ranging from 10 Megabits per second (Mbps) to 100 Mbps, or even higher. There are three main network topologies that are commonly utilised in wired networks: star network; bus network; and ring network (Jiang, 2012). Figure 2.1 shows the bus topology of a wired network, where devices connect to the hub.

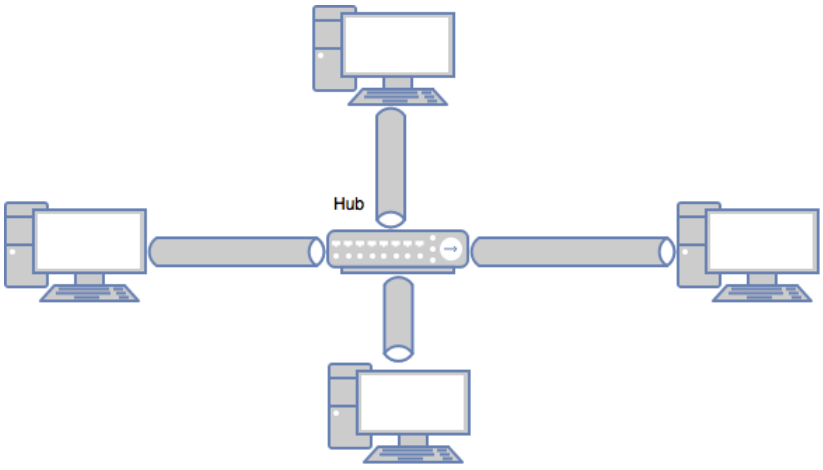

Figure 2.1. Wired network (bus topology).

2.1.2 Wireless network

A wireless network uses high-frequency radio waves, rather than wires, to communicate between nodes. Organisations and individuals can use this type of network to expand their existing wired network, or to go completely wirelessly. A wireless device is able to share data without networking cables, which decrease range; mobility is thereby increased in a wireless system. There are two main types of wireless network: infrastructure and peer-to-peer, or *ad-hoc*. There are several differences between each mode, in terms of their requirements, efficiency and format (Bosworth et al., 2009).

An infrastructure network requires a base station or an access point. The access point acts as a hub, providing connectivity for wireless devices. The access point converts data to radio signals and transmits them using the IEEE.802.11 protocol. There is usually one access point in the wireless network, which connects the devices; this set up is called the Basic Service Set (BSS).

Sometimes there is more than one access point allowing connection to the network; in this case the wireless infrastructure is called the Extended Service Set (ESS). This allows wireless computer access to LAN resources as file servers or existing Internet connections. It is also possible to bridge or connect the wireless LAN to a wired LAN (Loo et al., 2011). Figure 2.2 shows the architecture of this type of network.

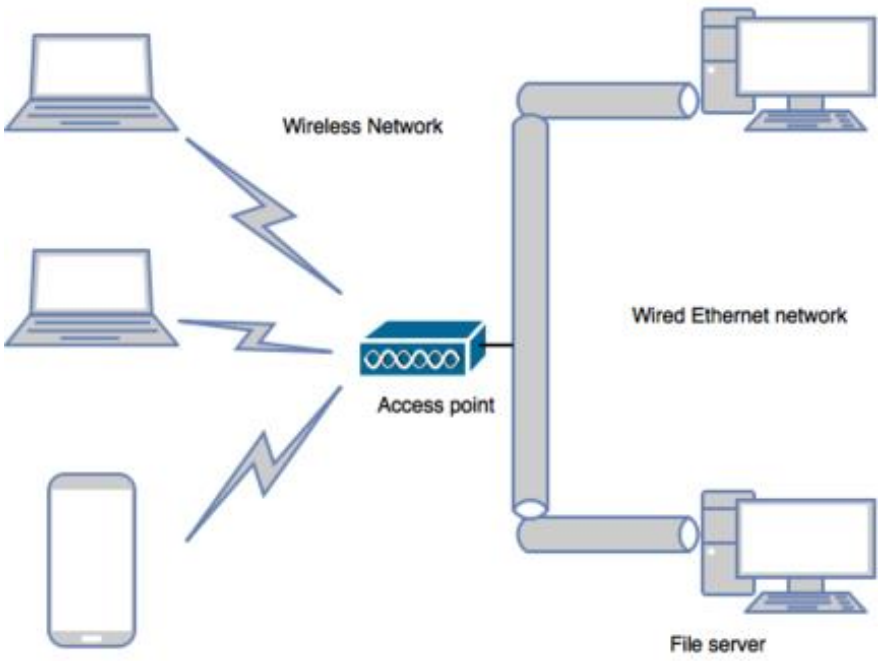

Figure 2.2. Infrastructure wireless network.

According to the Institute of Electrical and Electronic Engineers (IEEE), there are four main transmission standards for wireless networks: 802.11; 802.11a; 802.11b; and 802.11g. The four standards differ in terms of radio frequency and connection speed. The slowest are 802.11 (1 or 2 Mbps) and 802.11b (5.5 to 11Mbps) (Dean, 2012).

Peer-to-peer or *ad-hoc* networking involves a number of devices, such as computers, each equipped with a wireless NIC. Each computer, or node, communicates with all other nodes directly, without any need for an access point or a centralised point (Seet, 2009). This can be used as long as the device is located within the range of the other devices or nodes. They can share printers and files, but may not be able to access wired LAN resources. One of the nodes can act as a bridge to the wired LAN using special software, so the network would be able to access other wired resources. This mode is flexible and allows quick installation. *Ad-hoc* wireless networks can be divided into three groups according to their performance: Mobile *ad hoc* network (MANET); Wireless Mesh Network (WMN); and Wireless Sensor Network (WSN). Figure 2.3 shows the architecture of the *ad hoc* network (Shen et al., 2010).

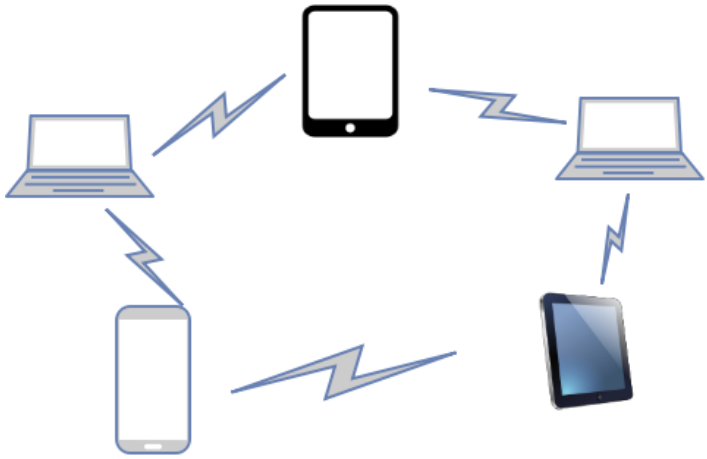

Figure 2.3. Ad hoc network architecture.

MANET will be explained in detail in Chapter 3. WMN is a mesh network, established via the connection of wireless access points installed in every network user's locale. Every network user is considered as a provider, so it can forward data to the next node. The networking infrastructure is simplified and decentralised as each node needs only transmit as far as the next node. Topology of WMN is illustrated in Figure 2.4. WMN allows users living in remote areas, and small businesses operating in rural places, to connect their networks together to gain affordable internet connections (Misra et al., 2009a).

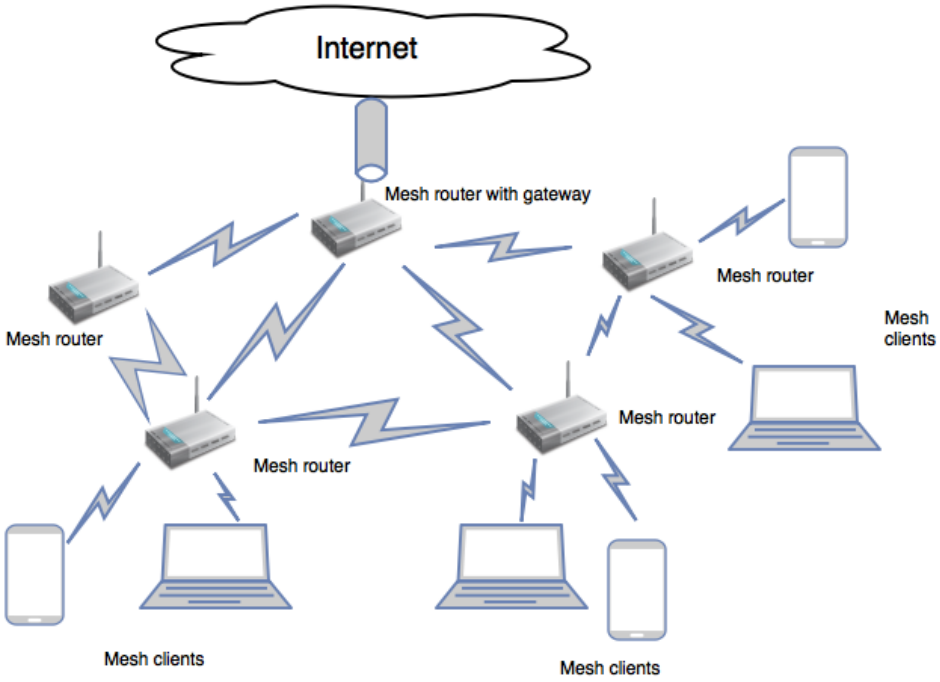

Figure 2.4. Wireless mesh network topology.

WSNs are composed of spatially distributed autonomous gadgets utilising sensors to monitor environmental or physical conditions. WSN systems incorporate a gateway, which wireless connects the distributed nodes to the wired network. Figure 2.5 illustrates wireless sensor network topology. There are three components of a WSN: nodes, gateways, and software. The wireless protocol utilised depends on the application requirements (El Emary and Ramakrishnan, 2013).

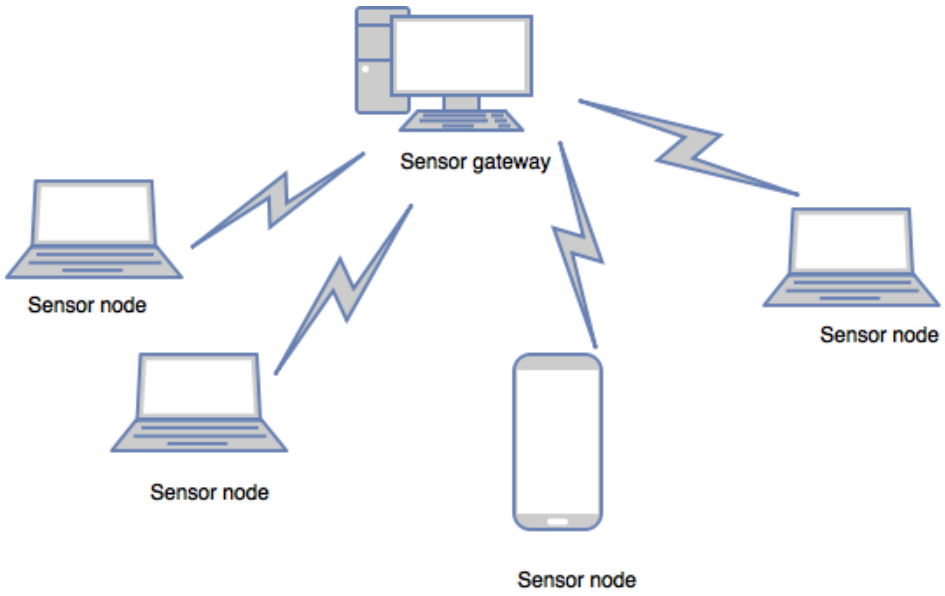

Figure 2.5. Wireless sensor network topology.

2.1.3 Comparison between wired and wireless networks

The major difference between the two types of network is the method of connecting nodes; a wired network uses cables whilst a wireless network uses radio waves. Generally, the wired network gives a faster and more secure connection. However, it is only suitable for connection over distances of less than 2,000 feet. Conversely, the transmission speeds of wireless networks can be limited by external interference. In a wireless network, the network is usually 150-300 indoors and around 1000 feet outdoors, depending on the terrain (Randhawa and Hardy, 2013).

Another drawback of a wired network is the necessity for complicated installation procedures. Cables must be connected to all computers in the network. Reliance on radio waves to transmit data means that wireless networks do not require cables to connect devices (Kaur and Monga, 2014).

In respect to the cost, the equipment required for a wireless network costs more than the equivalent wired Ethernet products. Access points and wireless adapters could cost three to four times as much as Ethernet. Wired networking is

inexpensive. For example, hubs, Ethernet cables and switches are all cheap. Broadband routers may cost more, but these components are optional in wired networks. Usually, the higher cost translates into benefits such as built-in security features and easier installation. Wired LANs enable superior performance. A traditional Ethernet connection gives about 10 Mbps bandwidth. Interestingly, fast Ethernet technology, giving around 100 Mbps, costs only marginally more and is readily available. Fast Ethernet is sufficient for gaming, high-speed internet access and file sharing.

Wired networking that uses hubs may experience performance slowdown when several devices use the network simultaneously. It is possible to use Ethernet switches rather than hubs to avoid this problem, but this setup is more expensive (Liu et al., 2009). In a wireless network there are many wireless standards with different speeds. For instance, 802.11a with a speed of 54 Mbps, and high-speed 802.11ac at 1300 Mbps, faster than a wired network speed (Nikolikj and Janevski, 2014).

The mobility and flexibility of a wireless network helps offset the performance limitations. Mobile devices such as computers and cellular do not need to be tied to an Ethernet cable and are able to roam freely within the wireless network range. This is in contrast to wired networks where devices must remain connected with Ethernet cables. However, the openness and high mobility of wireless networks leaves them vulnerable to attacks (Balandin, 2010).

Wireless networks have a higher rate of interference than wired ones. A wired network is invisible to other wired networks. Thus, the presence of one wired network would not affect the performance of other networks. Consequently, signal loss and fading is a less common occurrence than in wireless networks. Wireless networks can suffer from radio interference due to other wireless devices, obstructions by walls, or weather conditions. As a result, signal loss and fading occurs more frequently than in wired networks (Noda et al., 2015).

Wireless networks are less secure than wired networks. In wired networks, firewalls as the primary security defence when a connection is made to the internet. However, the wired Ethernet switches and hubs do not support firewalls. Firewall software products, such as Zone Alarm, can be installed on the computers themselves. Also, broadband routers enable equivalent firewall capability, which is configurable through its own software and built into the device (Xiao et al., 2007).

Overall, wireless networks are less secure than wired networks because information is travelling via the air and can easily be intercepted. The limitations of

wireless security are more theoretical than practical. Wireless networks conserve their data by using the Wired Equivalent Privacy (WEP) encryption standard that ensures the safety of wireless communications is close to that of wired networks (Liang and Yu, 2015).

In summary, no computer network is completely secure. For organisations, the main security considerations tend not to be whether the network is wired or wireless, but rather to ensure that the safety measures taken, such as firewalls, are properly configured, and that employees are aware of vulnerabilities such as spoof emails. Table 2.1 shows the differences between both wired and wireless networks based on different aspects.

Table 2.1. Comparison between wired and wireless networks.

Comparison factor	Wired network	Wireless network
Requirements	Ethernet cables; hubs and switches for connections.	Two modes: *ad hoc* or infrastructure. Wireless devices need WLAN cards and access points to communicate. Works by radio waves; does not need hubs or switches.
Cost	Ethernet cables and switches are not expensive.	Wireless Adapters and access points are expensive.
Mobility	Mobility is limited as computers need to be physically connected to the network.	More mobility as devices can be moved around freely within the wireless network.
Performance	High; can give up to 100 Mpbs bandwidth using fast Ethernet technology.	There are currently many wireless standards with different speeds, some of which are higher than wired networks.
Reliability	Ethernet cables and switches are reliable.	Less reliable than a wired network.
Interferences	Low	High
Security considerations	More secure than wireless networks. Use software such as firewalls.	Less secure than wired networks. Signals travel via the air and may easily be intercepted.

2.2 Security trends in modern technology

There are a number of definitions of security. It can refer to a group of individuals that are responsible for the protection of people or organisations. Another meaning of security, which is related to this research, refers to the protection of an

entity, be it an organisation, building, country, or individual against threats, attacks, or crimes (Alpcan and Başar, 2010). Computer security is defined as the protection of automated information systems via the preservation of the three pillars of the security; Confidentiality, Integrity, and Availability (CIA) triad. This also encompasses information system resources, such as hardware, software, information, and data (Stallings, 2014).

As a result of the rapid growth of technology, devices have become omnipresent. Subsequently the threats against these technologies have increased. Mobility and flexibility are the most popular benefits of a wireless network (Reardon, 2015). Although security threats can appear in both wired and wireless networks, it is easier to launch attacks in wireless networks because in wired networks the adversary needs to pass many defensive lines in order to launch attacks. By contrast, in wireless networks the adversary can launch attacks from anywhere in the network if the wireless node is within the radio transmission range (Ahmad et al., 2012).

The use of wireless networks has grown exponentially in the 2000s. Many devices are available with different specifications and features in MANET. For example, smart phones, MP3 players, iPods, computers, and laptops are devices that can use the same wireless connection (Reardon, 2015). In addition, wireless networks are deployed widely in different sectors, such as academic institutions. From a security perspective, these networks need to be monitored closely to detect any misbehaving node as these can have serious effects, such as data loss or even theft (Shorey et al., 2006).

There are many reasons that threats to wireless networks have increased to the point that it is described as commonplace nowadays. First, the users of these devices are not usually technically minded and do not know of the potential threats.

Second, a person can open an anonymous email without knowing whether it contains a virus or if it is allowing hackers to gain control over a device. In MANET, security threats and challenges emerge due to its ease of use.

Third, the technological revolution has increased the occurrence and use of wireless networks. People can often easily acquire the password to a network within different sectors, such as hotels, cafes, airports, and even when visiting friends. For instance, nodes in MANETs can join or leave a network anytime, so nodes do not know each other.

Fourth, the majority of all modern devices, if not all, support a wireless connection.

Finally, modern social media encourages people to use wireless network and share information, which is really resourceful. An attacker can easily launch an attack by advertising a link under an attractive title or scandal (Vacca, 2012). Accordingly, security is a critical issue especially in wireless networks where the control and monitoring processes are quite difficult.

Security is an essential component of any network or organisation. Data loss, theft, or be compromised is a critical issue but can avoided by applying appropriate security measures. Some security mechanisms, such as cryptography and the use of secret keys, can exhaust the network's power. This is especially true of MANETs due to its limited energy (Sastry et al., 2013).

2.3 Pillars of security

There are three pillars of security that must be applied for a system or network to be described as secure. Figure 2.6 shows the CIA triad (also known as the security triad): Confidentiality, Integrity, and Availability (Bishop, 2005). These three integral components were supplemented with two desirable items in communications added in International Organisation for Standardisation ISO7498-2 [ISO89]: Authentication and Non-Repudiation (or accountability) (Pfleeger et al., 2015) .

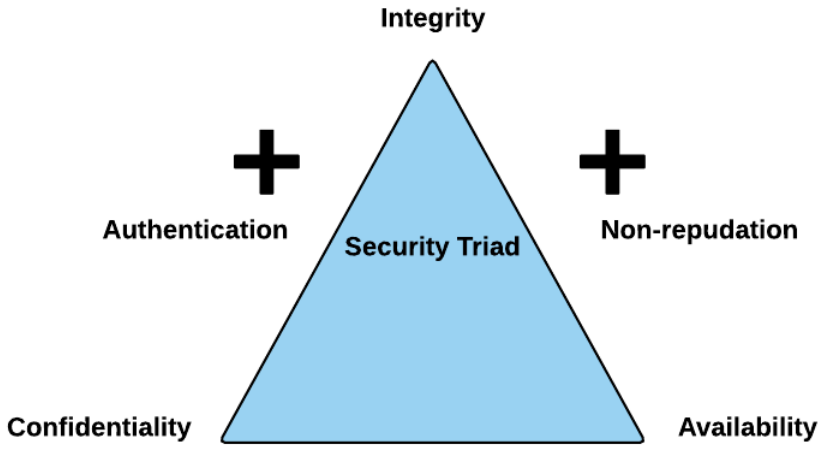

Figure 2.6. CIA triad.

2.3.1 Confidentiality

Confidentiality means ensuring and preserving access to, and disclosure of, information according to authorised restrictions. For example, protecting property information and personal privacy. When confidentiality is lost, this is deemed to be an unauthorised disclosure of information (Bishop, 2003).

2.3.2 Integrity

This process guards against the improper modification, fabrication, or even destruction of information. This includes checking and ensuring the authenticity and non-repudiation of information. A lack of integrity leads to the production of unauthorised information (Hrabik et al., 2006).

2.3.3 Availability or Access control

This ensures that intended users have reliable and timely access to information. The loss of availability to a legitimate user means the disruption of access to or use of information, a network, or system (Seidl et al., 2015).

2.3.4 Authentication

Authentication is important to ensure that data is genuine, trusted, and verified. It is pivotal users' identities are verified and that they are who they say they are. In addition, authentication must ensure that data entering the system comes from a trusted sender (Stapleton, 2014).

2.3.5 Non-repudiation or accountability

Repudiation literally means "denial"; therefore non-repudiation is the "inability to deny". In network security, non-repudiation refers to the ability of the system to confirm that the sender of a message cannot convincingly deny sending that message. Therefore, it is a process of confirming that the user performed a specific action (Ciampa, 2014).

2.4 The importance of security for both customers and industrials sectors

The legislative measures conducted in the name of security aim to decrease the number of threats. A number of detection technologies used in congestion with each other, such as IDS, firewall, antiviruses, each focusing on different aspects of

security. However, incidents can still arise despite the high implementation on security countermeasures. There is no doubt that security is something requisite and essential with our widespread use of technology. For example, in hospitals there is a high level of authentication required to access patients' files. Another example, using it in military arena (Ancona et al., 2000).

The available safeguards and increasing awareness of risk could decrease the chance of an attack but cannot fully prevent it. Nowadays, people consider data breaches in some organisations, such as banks, as a scandal and they request compensation (Koch et al., 2012). As such, many financial losses can be connected with compromised data. According to (Martin, 2015), one of the biggest communications companies in the UK, TalkTalk, had a major security breach in October 2015 that resulted in the theft of clients' information. In addition, around £3,500 was stolen from customers' accounts. The company tried and failed to mend its relationship with its customers by paying them compensation of around £30.20 each. This cost the company many customers as many cancelled their contracts due to a loss of trust (Martin, 2015).

Another incident specifically related to a DDoS (Distributed DoS) attack was against a popular web hosting service. Freeparking was hit by DDoS attack in June 2015. Customers complained as they have many domains that rely on Freeparking's named servers. Unfortunately, due to the nature of this attack it took long to mitigate and resolve the problem (Hall, 2015b).

Another security concern that is raised is when a personal device is brought into an organisation. There are some advantages when employees supply their own device, such as a tablet, iPad, or laptop. For example, this can increase productivity, flexibility, and efficiency while also allowing employees to log-in to the organisation from anywhere at any time (Miller et al., 2012).

Despite these benefits, there is still a concern about the effect of these private devices on the security within an organisation. The organisation's security needs to consider the CIA triad for both the organisation's resources and its assets. Assets refer to data and information that is stored, recorded, or even processed within the organisation. It is difficult to prevent employees from bringing their own devices into work. In near future, the devices will be even smaller, such as computerised glasses and wristwatches, which will be even more difficult to detect. As such, an appropriate security policy and privacy settings are important in order to accommodate these incidents in organisations. Multiple aspects of information

security, processes, and privacy functions need to be combined in order to protect confidential information (Bello Garba et al., 2015).

All in all, there is a potential need for security in wireless networks. The idea is not only to allow users to communicate with each other and use the service, but also to be secure in doing so. Applying security in such an area effectively involves the consideration of many aspects. For example, in a wireless network, such as MANET where nodes can join in and leave the network arbitrarily, determining a solution can be hard. Consequently, a security mechanism for a MANET network should be appropriate to its specific characteristics, such as limited energy supply (Kahate, 2013).

2.5 Chapter summary

This chapter aims to give an overview of computer networking and security systems in literature, focusing on wireless networks, and the various types of wireless network. This general information is a base to understand the idea of the project. Knowledge and understanding of network security is vital. Despite the fact that wireless networks help people to perform many tasks online easily, there are many threats and challenges associated with them. A comparison of many aspects of wired and wireless networks has been given. The technology revolution in the last five years has dramatically increased people's reliance on wireless networks. This chapter illustrates many reasons why the threat of an attack has increased through the use of wireless networks. In addition, five security aspects or services are discussed that are important in ensuring the security of communications. Finally, the importance of security to both customers and organisations is explained, relating to many factors such as financial factors and reputation. In the next chapter, the MANET network will be explained in detail, as this is the focus of this research. MANET's characteristics, features, and vulnerabilities will be discussed in detail. Moreover, Denial of Service attacks and the Internet of Things paradigm will be illustrated.

Chapter 3: Mobile *ad-hoc* Networks (MANET)

This chapter provides a concise overview of MANET. Many aspects of the network are considered including MANET's history, characteristics, specifications, routing protocols, challenges, and attacks including DoS attacks. In addition, an overview of the Internet of Things (IoT) is discussed. The arguments presented in this chapter are supported with relevant literature and discussion of other studies.

3.1 History of MANET

Ad-hoc networks have now reached their third generation. The first generation was developed in 1972 and called Packet Radio Networks (PRNET), a system which was used for military research purposes in the 1970s. The second generation emerged in the 1980s when the *ad-hoc* network was implemented as part of the Survivable Adaptive Radio Networks (SURAN) programme (Bang and Ramteke, 2013).

This generation had the merit of providing a packet-switched network to the mobile field without infrastructure. Furthermore, this programme improved the radios' performance and made them resilient against electronic attacks, cheaper and smaller than the first generation. The third generation was developed in the 1990s, notebook computers and other viable devices reflected considerable improvements in the concept of commercial *ad-hoc* networking (Kumar et al., 2013). The MANET group was conceived by Internet Engineering Task Force (IETF), who worked hard to standardise the routing protocols for *ad-hoc* networks (Suri and Singh, 2014).

3.2 Characteristics of MANET

Wireless *ad-hoc* networks were first unveiled in the 1990's. A MANET is a temporary, short-lived, spontaneous network with a non-fixed infrastructure and self-

organised wireless network. This consists of nodes which communicate with each other without an infrastructure or a topology. These nodes or devices can be iPads, smart phones, computers, laptops or even MP3 players (Perkins, 2008). Nodes in this environment act as routers and hosts, sending and receiving packets. In addition, nodes can join or leave the network arbitrarily without giving any prior warning and organise themselves arbitrary.

Moreover, a MANET can operate in a standalone fashion where it is unconnected to any network or even the Internet or in a connected fashion where it connects to the Internet (Sarkar et al., 2007). MANET has multi-hop routing, which means that when packets are delivered from a source to a destination which is out of the direct transmission range, then the packets will be forwarded to other intermediate nodes.

Due to the simple architecture of MANET and the advent of the Internet, the prevalence and usage of MANET have shown a clear increase in many sectors, for example in emergencies such as relief situations and disasters, military services, airports, conferences, lectures, cafes and so on (Carrell et al., 2012 ; Su et al., 2014). Mobile users usually use this network to communicate when no fixed wired infrastructure is available (Ambhore et al., 2013).

For instance, a teacher can utilise MANET to interact with students during a lecture. In such situations, a group of mobile hosts with wireless network interfaces form a short-lived network without the need for any fixed infrastructure. Figure 3.1 shows the basic classification of networks whereas wired or wireless. In addition, wireless networks can be whether ad-hoc or infrastructure. The former do not include a central point to monitor the other devices and every device can connect directly to each other, whereas the latter include the central point that all devices connect to it. Three types of ad-hoc networks: mesh wireless network; sensor wireless network; and mobile ad-hoc network. The focus of this research on MANET environment (Alnaghes and Gebali, 2015).

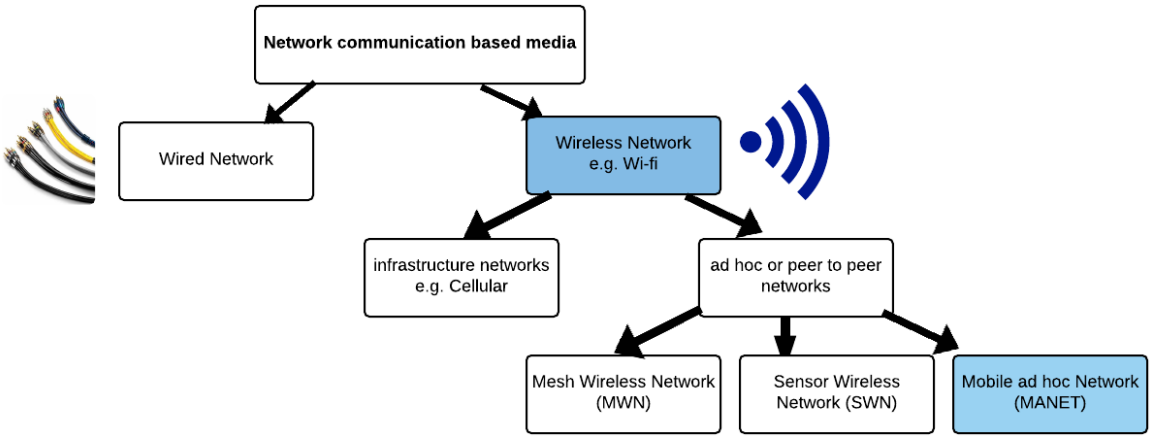

Figure 3.1. Network classification: wired and wireless networks.

For a MANET to be constructed, a node willing to send data to a node willing to accept data are the sole requirements (Micheal and Arunachalam, 2014). The nature of omnipresent devices makes wireless networking a favourable option for their interconnection due to the mobility and flexibility this technology enables (Bang and Ramteke, 2013).

Figure 3.2 shows the architecture of a simple MANET which consists of six nodes (Park and Yoo, 2013). Despite the fact that MANET can consist of multiple smart phones, there are many differences between the two. Cellular is an infrastructure network whereas MANET is not. Moreover, cellular has high setup costs and takes more time to setup than MANET, while MANET is more cost-effective (Sarkar et al., 2007).

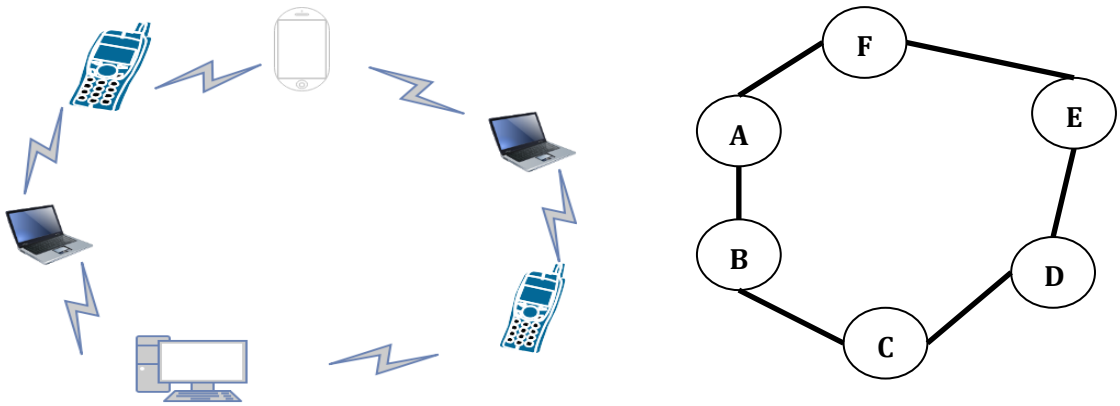

Figure 3.2. MANET architecture.

3.3 Routing protocols in MANET

Routing in MANET means choosing the most suitable and viable path between the source and the destination nodes. In addition, protocols mean a set of rules and instructions which allow different nodes to communicate with each other properly. Therefore, routing protocol in MANET means that nodes, according to a set of rules, will search for the other nodes in order to communicate and share packets (MCA, 2015).

The impact of different routing protocols in MANET has varied for different reasons. For example, one study in (Bai et al., 2003) proposes that mobility affects the performance of many routing protocols, including DSDV, AODV, and DSR. As a result, simulation studies have been conducted on multiple MANET routing protocols to assess memory, control overheads, communication, time complexity, route discovery, and maintenance. For example, (Cano and Manzoni, 2000) compared measurements and energy consumption behaviour of four routing protocols: Destination Sequenced Distance Vector (DSDV); Ad-hoc On-demand Distance Vector (AODV); Direct Source Routing (DSR), and; Temporally Ordered Routing Algorithm (TORA). Although simulations and comparisons show that AODV and DSR give better performance results than others, TORA is the worst performing. Further research indicates that the number of nodes affects the impact of routing protocols including AODV, as is discussed (Bagwari et al., 2012).

There are different routing protocols in MANET. Generally, these routing protocols can be classified into three groups in MANET: proactive, reactive and hybrid. Under the proactive routing protocol each node discovers the route to the next node before the actual communication is requested. This cuts the time delay but adds to overhead costs (Muralishankar and Raj, 2014). A full comparison between proactive and reactive routing protocols in (Mohseni et al., 2010) emphasised that the former, including DSDV, have a higher control overhead when compared with the latter, for example AODV.

There are different proactive protocols such as DSDV, OLSR and Open Shortest Path First (OSPF) (Dhenakaran and Parvathavarthini, 2013). In contrast, a reactive approach is considered as a demand-led protocol. Nodes can be described as being in sleep mode and they are activated only if there is a request to communicate with other nodes. Therefore, the network overhead will be lower than that associated with the proactive protocol, but more time will be needed to establish

communications than is the case with the proactive protocol. DSR and AODV are examples of reactive protocols (Tayal and Gupta, 2013).

Hybrid protocol combines the advantages of the proactive and reactive protocols. Zone Routing Protocol (ZRP) is an example of this type (Han and Lee, 2013). Choosing the suitable routing protocol depends on the amount of traffic being handled by the network and the number of flows (Patil and Sidnal, 2013). These protocols are proposed in order to increment scalability by allowing mobile nodes close to one another to work together to form some sort of backbone to decrease route discovery overheads (Patel et al., 2015b). This is achieved by proactively maintaining routes to nearby nodes, and identifying routes to far away nodes, by utilising a route discovery method (Aujla and Kang, 2013).

Table 3.1 presents the key differences between the three types of routing protocol and discusses their advantages and disadvantages (Bansal et al., 2015) .

Table 3.1. Comparison of routing protocol.

Protocol	Advantages	Disadvantages
Proactive	Latency is decreased in the network; the information is always available to use; periodic update of the routing information	High overheads; routing information is flooded throughout the network
Reactive	The path is only available on demand; the overhead is low; no need to distribute the routing information	Increases latency in the network
Hybrid	It is suitable for large networks; the information is frequently updated and readily available	High complexity

Various types of threats have an effect on the routing of ad-hoc networks, such as confidentiality, integrity, and availability. In regard to confidentiality within the realm of routing protocols, the main threat is the privacy of the routing data.

When the routing data is compromised, a secondary threat may be posed to other forms of information such as geographical location. The integrity of the network relies on the accuracy of every node's routing information. Attacks may occur, including those that can alter existing routing data or introduce incorrect, routing data. In regard to the availability aspect, it is required that nodes can obtain access to routing information at all times. In addition, routing operations must not delay nodes from being provided with up to date information. Furthermore, every node in the network is able to behave normally without interference from security.

3.4 Security challenges in MANET

Due to the specific features of MANET such as dynamic topology and the lack of certification authority, it becomes prone to many security breaches. In MANET, attacks might come from all directions and affect any node. Therefore, attacks could cause congestion, propagate false routing information, and prevent services from working normally or even shutdown them completely. This subsection highlights these challenges in detail.

3.4.1 Vulnerabilities and Challenges

As a consequence of the openness and dynamic nature of MANET, such as its shared wireless medium, open peer-to-peer network architecture, high dynamic topology and stringent resource constraint, many security concerns have been raised (Ponsam and Srinivasan, 2014).

In wired networks, firewalls are the main security method used by computers and routers to detect vulnerabilities; this, however, present a significant challenge for MANET, because a firewall in this network cannot distinguish between normal and malicious traffic, including denial of service attack (Sharma and Fatima, 2013). Therefore, identifying or making the decision about whether the neighbouring node is a legitimate node or malicious node is a difficult and tedious task in MANET (Chitkara and Ahmad, 2014).

MANET exhibits a number of shortcomings that compromise security and make them easy targets for attackers. Because each node can communicate with others separately, there is no central nodal point as used by other systems to monitor traffic, other nodes in the network, control transmission of packets across the whole

network, and allow, or prevent, devices from launching attacks (Raghavendran et al., 2013).

Second, nodes can move arbitrarily, thus its topology changes unpredictably and frequently (Bang and Ramteke, 2013).

Third, nodes rely on batteries and have constraints on the network and state information that may be stored, particularly for security-related tasks. Each node needs energy to communicate with another node, so power and bandwidth constraints are a major concern (Jain and Garg, 2013).

Fourth, scalability is another concern in MANET as each node can access the network and leave dependently. This is in contrast to wired networks where the scale is predefined when a network is being designed and will not generally change much during its usage. The scale in MANET is constantly changing with due to the mobility of nodes. Indeed, MANET networks are designed to be scalable, often forming unpredictable topologies. They are transient, dynamic environments with nodes joining, or leaving, at any time. This results in issues surrounding trust establishment, as we do not know the intentions of these nodes (Singh and Dua, 2014).

Fifth, Bandwidth constraints and the mobility of MANET nodes increase the volume of packet losses due to interference and high Bit Rate Errors (BREs) (Chitkara and Ahmad, 2014). Thus, MANETs remain vulnerable to a range of attacks by malicious nodes (Singh et al., 2014a). All the previous factors have made MANET vulnerable to many intrusions and attacks (Patel, 2015). Figure 3.3 shows a summary of the challenges faced by MANET (Raj et al., 2015 ; Agrawal and Chauhan, 2015).

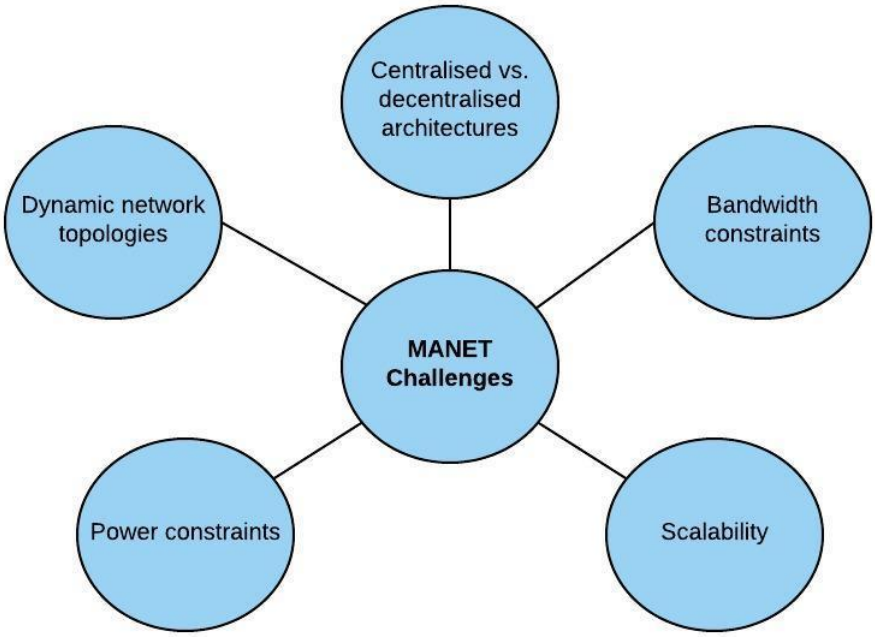

Figure 3.3. MANET Challenges.

3.4.2 Attacks in MANET

Attacks in MANET can be classified as internal or external attacks depending on the location.

3.4.2.1 Internal attack

Compromised nodes which are part of the network launch this kind of attack. As a result, nodes gain unauthorised access to the network and pretend to act as normal nodes. These nodes aim to launch the attack for two specific reasons (Tayal and Gupta, 2013). The first is to hijack or subvert authorised nodes with the help of an external attacker and use them to start an internal attack in the network (Faisal et al., 2013).

Another kind of attack is selfish ones that enable a node to save resources, including processing capabilities, bandwidth, and power, exploiting the resources of other nodes, including their power. An example of internal attack on a MANET network, composed of seven nodes, is shown in Figure 3.4. In this example, node M in the network is a malicious node that drops packets, so when these are sent from the source node A they cannot reach their destination (node F) as node M drops the packets (Jain, 2014).

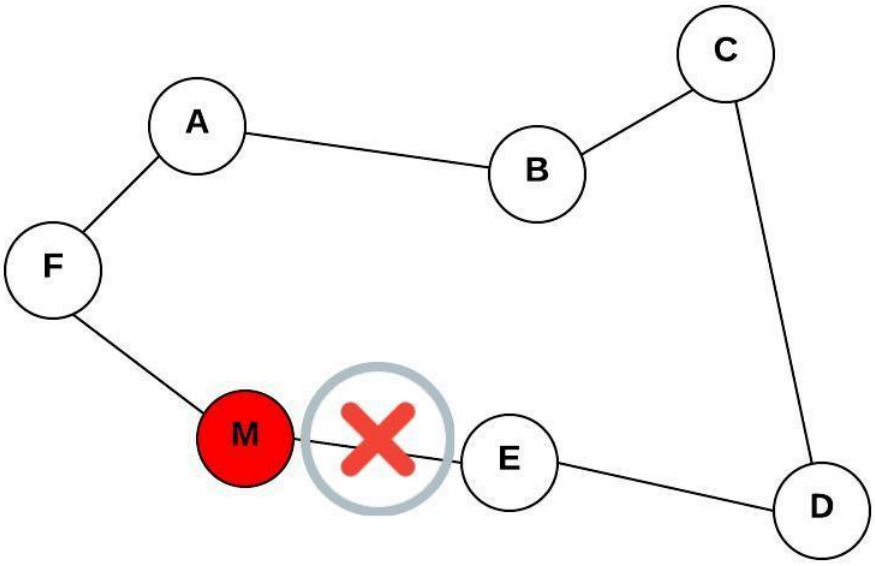

Figure 3.4. Internal attack in MANET.

3.4.2.2 External attack

Unauthorised nodes that are not within the network launch an external attack. This attack may flood the network with bogus packets and even use impersonation (Nadeem and Howarth, 2013). The main aim of this attack is to disturb the normal functioning of the network and cause congestion. Figure 3.5 presents the architecture of this attack. Node M, which launches the attack against this MANET, is not a part of this network. Besides, it drops the connection between node D and node E (Sivakumar and Selvaraj, 2013).

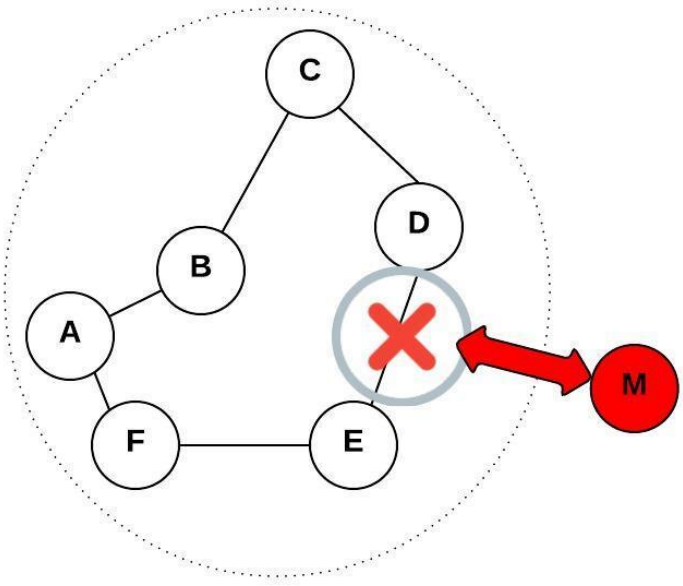

Figure 3.5. External attack in MANET.

3.4.3 Attack types in MANET based on performance

Attacks are classified into two groups according to performance and the nature of the attack: Passive attack and Active attack.

3.4.3.1 Passive attack

The aim of this attack is to operate stealthily and steal important information from the targeted network. Usually, the attacker does not disturb the normal network activities such as dropping packets (Goyal, 2014). Accordingly, the attacker becomes part of the network and listens and monitors the network traffic which violates message confidentiality (Kaushik and Sharma, 2015). Detecting this kind of attack is very challenging as the activities and operations of the network are unaffected and no new traffic is introduced.

For example, although such a passive attack may not be detected, associated interferences will. In addition, the malicious node which launches this kind of attack may not even be part of the network, further complicating the detection process (Rajakumar et al., 2014). Examples of this type of attack include eavesdropping attacks and traffic analysis attacks. Figure 3.6 illustrates the architecture of this attack; as an attacker sniffs the connection, between the source and destination, confidentiality, and thus security, is affected.

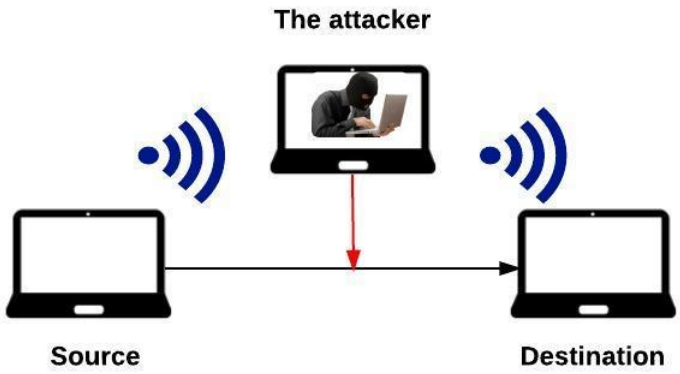

Figure 3.6. An illustration of passive attack.

3.4.3.2 Active attack

The attacker, an unauthorised party, disturbs network operations, and modifies or fabricates messages (Mani and Kamalakkannan, 2013). The attacker

disturbs the normal activities of the network. In addition, the intruder can insert, modify, delete, reply, or drop packets using this attack (Mori and Jethava, 2013). Although it is possible to detect these attacks quickly compared to a passive attack, they cannot be prevented (Aggarwal and Dhankhar, 2014).

For example, masquerading and message modification are examples of this type of attack. The malicious nodes which launch this attack can be internal or external (Nandini and Aggarwal, 2015). Figure 3.7 shows the format of this attack where the attacker disturbs the connection between source and destination and drops the connection.

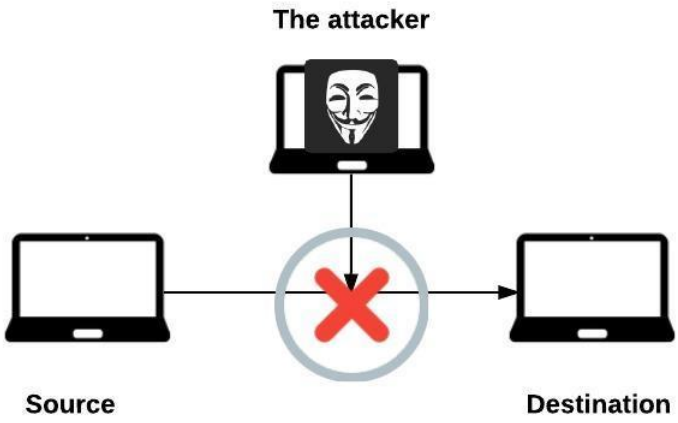

Figure 3.7. An illustration of active attack.

3.5 Denial of Service attack in MANET

Denial of Service attack (DoS) is one form of attack that paralyses, deprives and disrupts the availability of the network, thereby temporarily preventing legitimate users from accessing services (Lotfy and Azer, 2013). Moreover, this type of attack degrades the performance of the network and causes harm in many ways, such as financial damage and in terms of the use of resources (Patel and Sharma, 2013).

In an example of connected MANETs, if one military system were attacked by a threat like this, even for a short time, this could be enough to destabilise security and cut communications between soldiers and the command centre (Burbank et al., 2006). Moreover, because a DoS attack is a complicated problem, many users do not realise they are under attack, thinking the issue is just network congestion.

Furthermore, this type of attack exhausts the victim's network resources such as computing power and bandwidth (Dhanalakshmi, 2013).

A complex version of DoS attack is Distributed Denial of Service attack (DDoS). It is important mentioning that DDoS attack is a subset of DoS attack (Gulia and Sihag, 2013). Both attacks are applicable to MANET (Kumar and Singh, 2015). In DoS the attacker uses one Internet connection and one device to overwhelm their victim with packets (Chhabra et al., 2013).

For example, an attacker can launch this kind of attack against a specific user, using just one device and one Internet connection (Vishwakarma and Rao, 2014). In contrast, when an attacker uses many devices to launch this kind of attack against many users, for example bank customers, many Internet connections and zombies are used (Mittal, 2015). However, in DDoS attack the attacker uses multiple compromised devices usually called (botnet or Zombie) and multiple Internet connections to launch this attack (Abdelaziz et al., 2013). Figure 3.8 shows the architecture of both DoS and DDoS respectively.

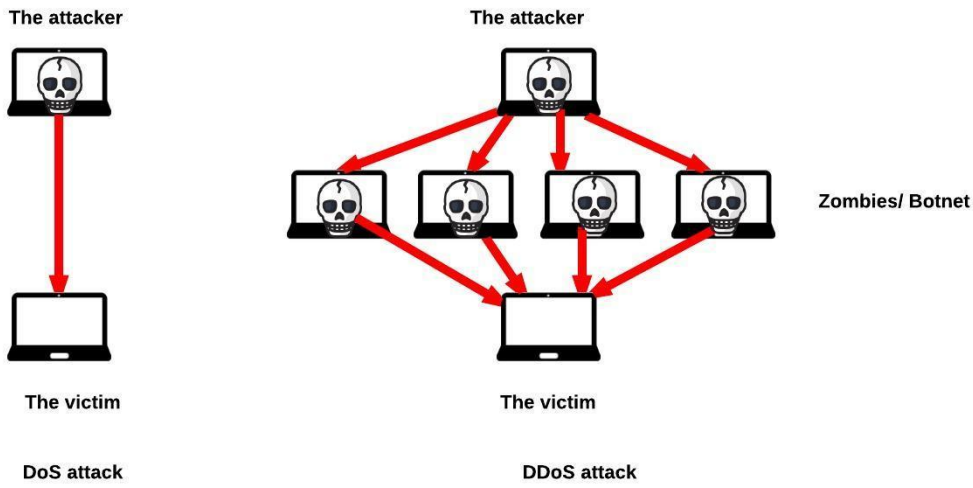

Figure 3.8. DoS and DDoS attacks architecture.

People who perpetrate such attacks do so for varying motives (Sinha et al., 2013). For example, it might be for personal reasons if it is considered as revenge against specific people or work. In addition, it could be for fun or for prestige and the attacker might think that it will help to gain respect or a good reputation among the peers (Hashmi et al., 2012). Moreover, it can be for political reasons, such as in

military operations to disrupt the enemy by flooding their network and crippling it. As a result, soldiers (for example) cannot receive instructions from their commander (Udhayamoorthi et al., 2014 ; Yadav and Sharma, 2015).

A DoS attack essentially increases network delay and affects the network activities to deny availability to legitimate nodes. DoS attack floods the victim with an enormous number of packets which render the victim's device unavailable. As a result, the victim is unable to provide services to legitimate users. Time, effort, financial losses, reputation, secrecy and trust are all factors that are affected as a consequence of DoS attacks. It is notable that DoS attacks can be launched using a variety of methods. However, these attacks share a common general goal, which is to prevent authorised users accessing to authorised services and to degrade the performance of the network and inflict considerable problems on service users.

Eclipse is an online Internet provider which has been hit by DDoS attack twice in quick succession. The first hit was on Monday 23rd November 2015, and the second wave was on Wednesday 25th November 2015. Eclipse sent an email to customers confirming that it had been attacked and informed their users that Internet-based services might not be working until the attack had been dealt with. The email also contains apologies for inconveniences to service users (Hall, 2015a).

Rutgers University in the USA was hit by DDoS attack in September 2015 for the whole morning and the first part of the afternoon. According to the New Jersey news, the hacker who launched this attack is alleged to have taunted the school on social media. The hacker claimed that he or she was being paid around 500 dollars an hour by someone who bears a grudge against the school. The reason for the grudge was that the school had increased tuition fees to improve cyber security following previous cyber-attacks (MARAS, 2015).

3.6 Types of DoS attack in MANET

A DoS attack can be launched against different layers in the Transmission Control Protocol/Internet Protocol (TCP/IP) model. The TCP protocol was designed in 1974, and was spilt into TCP and IP protocols in 1978 (Carrell et al., 2012). A TCP/IP stack is an informal collection of protocols loosely organised as a stack (Alani, 2014), while TCP/IP protocols are widely used, forming the basis of the Internet, and can be compared to the Open Systems Interconnection basic reference model (OSI) which is never used in practice. Instead, OSI is normally used to

describe network structure, explain functions, and illustrate relationships between various networking protocols and technologies.

The OSI model was developed in 1977, designed based on LAN, and fits poorly in WAN. The reason for the latter is that there are many overlapping, even partial coverage of layers; the OSI model is a framework that can be used to explain how any network works in a generic sense. In the OSI model, a network is broken down into seven layers: Application; Presentation; Session; Transport; Network; Data Link, and; Physical. In this sense, OSI is not a suite of protocols in the way that TCP/IP is, and this latter kind of stack is implemented on almost all networked hardware everywhere. In contrast to OSI, the TCP/IP model has four layers: Application; Transport; Internet, and; Network access or host-to-network (Hunt, 2002 ; Casad, 2011). The TCP/IP and OSI models are illustrated below in Figure 3.9.

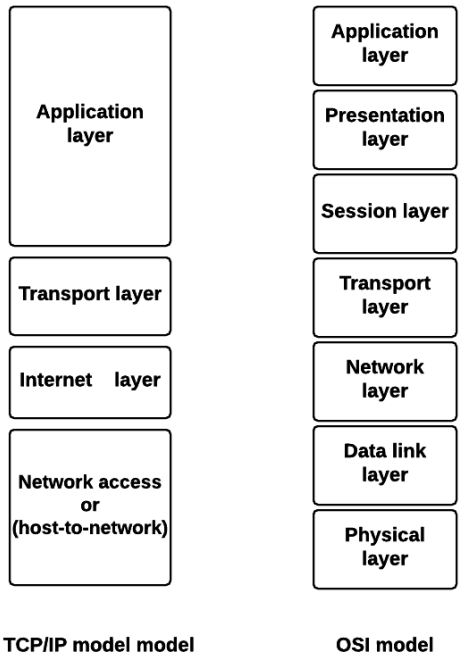

Figure 3.9. TCP/ IP model vs OSI model.

TCP/IP are a group of protocols which support network communications, identify network processes, and illustrate data format and information content (Carrell et al., 2012). In summary, the application layer provides the processes, programs, and applications used in the network, while the transport layer provides the end–to-end data delivery service and transmission. The network, or Internet, layer determines and defines the datagram, or packet construct, to be transmitted, and

handles data routing, while the network access layer encapsulates IP packets into frames for transmission, and maps IP addresses to physical hardware (Alani, 2014).

A DoS attack can be classified as active and passive attack depending on the attack's aims and performance as with other types of malicious activity. DoS attack can be launched against different layers in the TCP/IP stack (Singh and Gupta, 2013). Table 3.2 shows some attacks and multiple DoS attacks which can appear in each layer in TCP/IP stack with their definitions (Tyagi, 2013). Jellyfish attack, wormhole attack, blackhole attack, grayhole attack are explained in detail later in Chapter 6.

Table 3.2. Different attacks and their definitions.

Attack	Definition
Repudiation attack	This attack is also called a 'denial of participation' as it can include all or some part of communications. For instance, a user might deny purchasing a credit card online or even making any online transaction (Rai et al., 2010).
Worms and viruses	Defined as the selfish and malicious behaviour of nodes.
TCP/SYN attack	An intruder sends a succession of SYN requests to the victim's device. Thus, the device under attack is unable to complete the three-way handshake to establish a connection between client and server.
Session hijacking	An intruder spoofs the IP address of the victim's device. Thus, when the attacker defines the correct sequence number, (an expected outcome), a DoS attack is launched on the victim's device.
Sinkhole attack	This attack can take place in two ways. In the first case, a node exploits an AODV protocol, thus advertising itself as owning a valid route to a destination node, even though the route is false, with the intention of intercepting packets. In the second case, an intruder consumes intercepted packets without forwarding them to their destination (Jathe and Dakhane, 2012).
Sybil attack	In this situation, a malicious node claims many identities to violate the mapping of a one to one identity in MANET. In addition, the malicious node gives the incorrect impression of being distinct in multiple node-disjoint paths or locations (Abbas et al., 2013).
Rushing attack	This kind of attack is against on-demand routing protocols. The intruder receives Route Request (RREQ) packets then quickly floods them on the network before other nodes can react to which receive the same RREQ (Kumar and Rishi, 2010).
Malicious and selfish behaviours	These behaviours disturb the normal activities of nodes in a network. Malicious nodes give fake information and misroute other nodes. However, the selfish node does not complete missions, including forwarding packets, in order to save energy.
Traffic analysis	In this case, an attacker analyses traffic and reveals information regarding the network including the location of nodes, current sources, destination nodes, and network topology. This information can then be used to launch further attacks (Singh and Gupta, 2013).

Further, different types of DoS attacks have different goals to detect the network and different performance. As can be seen in Table 3.3, DoS attack can be launched against any layer of the *ad-hoc* network.

Table 3.3. Classification of DoS attacks in each layer.

Layer	DoS attack type
Application layer	Repudiation attack; worms and viruses
Transport layer	TCP/SYN attack; Jellyfish attack; Session hijacking
Network/Internet layer	Wormhole attack; Grayhole attack; Sinkhole attack;; Jellyfish attack; Blackhole attack; Sybil attack; Rushing attack
Network access layer	Malicious and Selfish misbehaviours; traffic analysis

3.7 An overview of the Internet of Things (IoT)

Rapid technological advancements, combined with a sudden increase in the number of users accessing a range of different network devices, have precipitated the development of various types of internetworking components. This has led to the launch of a new Internet generation or paradigm known as the Internet of Things (IoT) or the Internet of Everything (IoE). Using tools such as physical devices, virtual machines, services or processes, global communication and the exchange of data between individuals is now possible through Internet Protocols (IP).

The feature which distinguishes the Internet from other products is that it can be accessed remotely, whereby anyone can operate a system, or use a particular

device, without having to be based in a specific location. IoT is considered to be one of the most popular paradigmatic strings of thought in relation to the future state of the Internet. IoT provides multiple lenses by which to link the Internet with other real-world devices or objects (Reina et al., 2013).

Figure 3.10 illustrates the architecture of the IoT. The current dominant paradigm within the Internet is one that relies upon human-to-human interaction. However, IoT posits a novel emerging paradigm of thought, which postulates that any object, identified using a unique identifier, is assumed to be interconnected (Bahga and Madisetti, 2014). IoT authorises many technologies and communication solutions, such as wired and wireless networks, as well as exchange networked communications. Both powerful computers and small simple hardware devices are able to interconnect in an IoT setting, by using Radio-Frequency Identification (RFID) techniques (Bellavista et al., 2013).

IoT provides effective control mechanisms, whether available at hand or remotely. For instance, a car engine may be controlled using a mobile phone, as the car which is an object, connects with the phone via an IP. Another example is where a laundry machine can be programmed remotely, through the use of online communications, to commence a washing cycle.

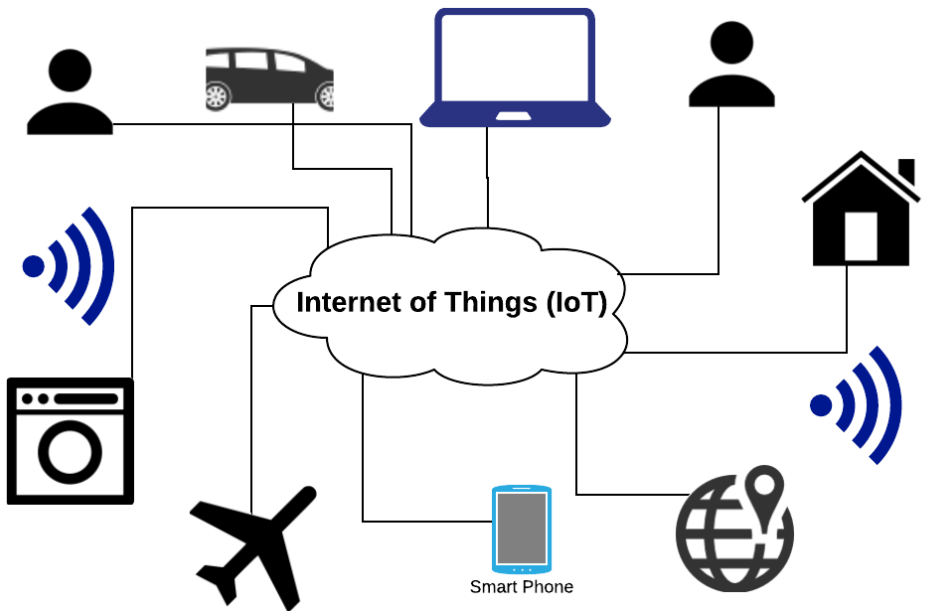

Figure 3.10. IoT architecture.

However, in the last decade, *ad-hoc* networks have been the centre of extensive attention, regardless of their appeal and specifications. A MANET requires less infrastructural networks, as they can be set up without any wired facility. Furthermore, MANET can be applied to many different sectors, as explained earlier in this chapter, and also in the IoT. The guarantees of data transfer in MANET within the large scale IoT needs to be considered (Zhou and Li, 2012).

The deployment of the IoT raises issues in relation to the dependence on computer technologies, significant infrastructural requirements, communications and multiple IoT objects, which are all constantly evolving. Thus, the vulnerability of IoT applications increases due to various potential forms of attack. Hence, an urgent need exists to develop a scalable and sustainable cyber ecosystem in IoT technology to detect and investigate attacks (Aldosari et al., 2016).

3.8 Chapter summary

MANET environment, its features and characteristics are explained in this chapter. In addition, it also covers the vulnerabilities in the MANET environment as a consequence of the system's characteristics which will help to understand the problem area of this project. All the challenges which are outlined in this chapter enable MANET to be attacked by various means such as eavesdropping, fabrication, and DoS attack. However, the focus of this study is DoS attacks and how to detect them in a MANET environment. Even though many types of DoS attack are detected in multiple layers in the TCP/IP model, this increases the severity of this type of attack. Additionally, types of attacks based on performance or location, whether passive, active, internal, or external are clearly explained and differentiated. Many examples are provided to illustrate the effects of these attacks and how they severely affect the victim's devices and resources. Moreover, an explanation of the IoT and its vibrant role with the technology revolution is discussed in brief. In the next chapter, the literature focusing on the methods used to detect DoS attacks will be reviewed and discussed. Prior to the method proposed in this study, the trust concept is used to detect DoS attack specifically in MANET. In view of this situation, the methods used to detect this attack based on the trust concept will be discussed extensively and the advantages and disadvantages of each method will be illustrated. Besides, different methods to assign IP address in MANET are discussed with identifying of their advantages and limitations.

Chapter 4: Research Gap in Denial of Service Attack

There are three research aspects which need to be considered in this research project. First, it should demonstrate the existing methods used to detect DoS attacks in MANET. Second, it should discuss the methods currently used to detect DoS attacks based on using trust; and third, it will discuss a number of methods used to assign IP address when MANETs are merged, and explain how these MANETs will be merged.

As mentioned in Chapter 1, no methods discuss the detection of DoS attacks when MM are merged, so no studies about this specific situation will be mentioned in this chapter.

4.1 Basic methods used to detect DoS attack in MANET

There are many countermeasures to control DoS attacks in MANET. A considerable amount of the published literature argues about various methods and approaches to precisely detect such attacks in a MANET environment. The basic methods used to detect a DoS attack in MANET will be discussed below.

4.1.1 Firewalls

The basic method to detect DoS attack involves using firewalls and proxies. A firewall is a system which monitors and controls traffic between two networks. Unfortunately, traditional firewalls are considered to be unreliable because they cannot distinguish between normal traffic and DoS attack traffic (Stewart, 2013). In addition, the mobile nature of MANET means that a number of traditional techniques ideal for wired networks, such as encryption software and firewalls, are insufficient. For example, firewalls use simple and basic rules such as allowing or denying certain ports or IP addresses. In addition, most people do not keep their firewall up to date, which raises the level of vulnerability. With this object, distributed firewalls work efficiently in MANET to prevent DoS attacks. Distributed firewalls use a central

policy which defines what is inbound and outbound, what is permitted to do and appropriate connectivity. In addition, this policy will be applied to all the endpoints and will be enforced for all hosts that participate in the distributed firewall. The distributed firewalls are designed to be reconfigurable, so it can be argued that distributed firewalls are used in filtering in MANET (Gupta et al., 2012).

Reverse firewall is also developed to detect flooding attacks, which is a type of DoS attack in MANET. Traditional firewalls usually protect the network from incoming packets, while reverse firewalls protect the outside from any flooding attacks that originate from inside the network. Flooding attacks aim to consume significant amounts of resources, such as battery power and bandwidth, and can even disturb normal routing processes (Zargar et al., 2013). (Filipek and Hudec, 2015) suggested another type of distributed firewall should be used in MANET with Intrusion Detection System (IDS) capabilities. This approach adds extra security to the network and protects it from DoS attacks.

4.1.2 Intrusion Detection System (IDS)

An ‘intrusion’ is any type of action by someone attempting to affect any aspect of the security triad that are discussed earlier in Chapter 2: Confidentiality, Integrity and Availability (CIA). An IDS is an important pillar of network security infrastructure. IDS is thus a system which aims to detect any intrusions or anomalies. There are three components of IDS: data collection, detection and response. Data collection involves collecting and processing data tasks, such as storing, sending and transferring data. IDS is another countermeasure used against DoS attack. The intrusion detection system works as an alarm to protect computer systems from any vulnerability.

The main problem with using IDS in MANET is the many false alarms raised by individual nodes. False alarms occur as a result of false claims or reports which have been created by anonymous nodes. In addition, the anonymity issue in MANET is considered a significant challenge due to the difficulties of disguising between trusted and untrusted nodes in MANET. When compromises occur then the IDS will issue an alert message to the security administrator, such as the website security officer. The IDS will collect, monitor and analyse the audit data in order to find any intrusive or anomalous attempts. Three classifications of intrusion detection

techniques were proposed by (Misra et al., 2009b): anomaly-based, misuse-based and specification-based.

The first technique is the anomaly-based intrusion detection method. This defines the symptoms of the normal activities of the system, such as using commands frequently. This technique detects intrusions as anomalies (Mitrokotsa and Dimitrakakis, 2013). Many techniques have been used to detect anomalies, such as statistical approaches as well as artificial intelligences such as neural networks and data mining. The challenge in this technique is to define normal behaviour, because normality can changed over time and the IDS must be up-to-date in order to detect any new vulnerabilities (Sahu and Sinha, 2013).

The second technique is misuse-based intrusion detection. This technique compares the signatures of known attacks with the activities of the current system. In commercial IDS, this technique is preferred over others since it is efficient and has low false positive rates. The main drawback of this type is that it is unable to detect new attacks. The power of this system results from its signature database, and it needs continuous updates to add new attacks.

The last technique is specification-based intrusion detection. This method places a set of defined constraints on a protocol or a program. Intrusions will therefore be detected as runtime violations of these specifications. This technique combines the strengths of the other techniques discussed above, as it detects both known and unknown attacks with low false positive rates. For instance, it could detect new attacks which do not follow the system's specifications. The limitation of this technique is that it is unable to detect some types of DoS attacks when they do not directly violate the program specifications.

There are many problems with using IDS. First, fidelity problems can occur. The information used in IDS is usually obtained from a packet on the network or from the audit trails. The data travels along a path, and could potentially be modified or even destroyed by an attacker. Second, resource usage problems have been raised. IDS will monitor the network at all times, even if there is no intrusion, which will lead it to use additional resources. Third, reliability problems exist. As the IDS is implemented as a separate program, this could be tampered with or even deleted by an attacker (CHAUDHARI and PRASAD, 2015).

The first IDS for MANET was proposed by (Zhang and Lee, 2000), who argue that many intrusion detection systems used in wired networks are not capable of working in MANET. They present an intrusion detection method for wireless *ad-*

hoc networks based on cooperative statistical anomaly recognition techniques. This method is based on running an IDS agent on each mobile node in the network. Agents collect data by gathering a real-time data and audit them from local sources and using an anomaly detection method to detect anomalies which are then updated in the routing table. One problem with using this method is that it results in a number of false positives, so it is unreliable. (Nadeem and Howarth, 2013) conducted a comprehensive survey on the use of IDS in MANET. This study uses IDS to detect many network layer attacks. A table in this research compares the use of different IDS methodologies in detecting attacks in MANET.

To sum up, IDS is more complex and challenging in MANET for many reasons. Mobility and dynamic topologies are factors which made IDS difficult in MANET and hindered its work. Fulfilling the requirements of IDS is thus difficult in MANET, such as collecting data and applying IDS techniques to detect intrusions with low false positive rates and effective responses (Begam and Murugaboopathi, 2013).

4.1.3 Filtering

Filtering is another technique used to stop excessive packets by using a router to detect them. However, this technique cannot be considered reliable as sometimes the packets can overwhelm the router and cause a DoS attack. (Tan and Seah, 2005) proposed the use of statistical filtering. This is a reactive method used to detect DDoS attacks in MANET by using traffic profiling for the purpose of filtering and detection. The main advantage of using this mechanism is that the packet delivery ratio is raised, whereas the average end-to-end delay is clearly decreased. The major limitation of this method is the cluster-based routing protocol filtering mechanism, as it does not guarantee detection of illegitimate packets and acceptance of the legitimate ones (Tyagi, 2013).

In addition, some mechanisms based on filtering use sophisticated filters. This would block any malicious nodes from sending such immoderate packet traffic to the victim node. However, this technique requires a high level of filter deployment, which is impractical and costly. Overlay filtering is suggested instead, as this technique could be deployed increasingly. For example, the CenterTrack method uses an overlay conforming from routers with network borders, which

determines the source of any DoS attack and the input debugging capabilities (Jia et al., 2013).

4.1.4 Watchdog/Pathrater

This method shows that it is possible to increase the throughput of a network despite the presence of malicious nodes. The aim of this method is to detect misbehaving nodes. A watchdog is set in the node when it forwards a packet to ensure that the next node will also forward the packet in the path. The watchdog performs this task by listening to all nodes within the transmission range in the network. The node will be tagged as misbehaving if it fails to forward the packet to the next node. If a packet is not forwarded to the next node during a timeout period, then a failure tally for the node responsible for forwarding the packet is increased. When this tally exceeds a predetermined threshold, the node is considered malicious (Arunkumar and Annalakshmi, 2014).

The watchdog mechanism's easy implementation and effectiveness means that many methods use it as a base, such as Pathrater. In the Pathrater method each node uses information obtained from the watchdog to rate its neighbours. Neighbour nodes can be classified as members, fresh, unstable or malicious. The watchdog is considered to be an intrusion detection system for MANET (Mishra et al., 2013). In addition, it is responsible for detecting misbehaving nodes by listening to the next hop and ensuring that nodes do not fail to transmit the packet to the next node (Padiya et al., 2013). If the watchdog finds a misbehaving node then it will be reported so that Pathrater and router protocols can avoid using this node in future transmission (Varshney et al., 2014).

Despite the fact that the watchdog scheme can successfully detect malicious nodes, as proven by much of the research, this method still has some limitations (Buddha, 2013). The watchdog scheme is unable to detect malicious nodes in certain situations. For instance, the watchdog cannot detect malicious nodes in the presence of receiver collisions and false misbehaviour reports, or if there is limited power for transmission (Sharma et al., 2013b).

An approach called TWO network-layer ACKnowledgment-based scheme (TWOACK) has successfully solved some of the flaws with the watchdog method. This approach resolves some of Watchdog's weaknesses such as its limited

transmission power and the receiver collision problems. The only limitation of this method is the network overhead, because the acknowledgment process is required in every packet transmission process (Abraham, 2013). In Selective TWOACK (S-TWOACK, three nodes work as one group to detect misbehaving nodes within the network. S-TWOACK is an updated version of the TWOACK scheme as it is able to detect misbehaving nodes even in situations of limited power and receiver collision. The three nodes work together in one route, so the third node is responsible for sending the S-TWOACK packet to the first node.

The use of the Message Report Authentication (MRA) method is proposed in order to discover misbehaving nodes in the presence of false misbehaving reports which are launched by intruders to mislead innocent nodes (Mahajan and Patil, 2015). The Adaptive Acknowledgment (AACK) method is used to resolve two of the watchdog's most significant problems, namely receiver collision and limited transmission power. This method is an improvement of the TWOACK scheme as its detection overhead is lower while its detection efficiency is improved. However, the AACK method does not work well on long paths as it would take a long time for end-to-end acknowledgment. This limitation means the malicious nodes would have more time to drop extra packets (Al-Roubaiey et al., 2010).

Enhanced TWOACK (E-TWOACK) is an improved version of the previous method. The main difference between TWOACK and E-TWOACK is that the former detects malicious links in the network, whereas the latter detects malicious nodes in the network (Botkar and Chaudhary, 2011). The efficiency level for detecting misbehaving nodes is therefore increased (Dave and Dave, 2014). ExWatchdog is an extended form of Watchdog which solves one of Watchdog's weaknesses: the false misbehaviour problem. Some nodes report that certain other nodes are malicious, but in fact they are the real intruders (Nasser and Chen, 2007). ExWatchdog also detects misbehaving nodes and reports them to the response system (Chaturvedi and Sharma, 2013).

The Enhanced Adaptive ACKnowledgment (EAACK) method is recommended especially for MANET to detect malicious behaviours. This method addresses three weaknesses of Watchdog: receiver collision, limited transmission power and false misbehaviour (Shakshuki et al., 2013). This protocol can be compared with TWOACK and AACK method in terms of receiver collision, limited transmission power and false misbehaviour (Elizabeth et al., 2014). Results show

that the EAACK method has the best results. EAACK is based on the concept of the hierarchical clustering of nodes (Ghodake et al., 2015).

4.1.5 Traceback

Traceback is another method which has attained satisfactory results in detecting denial of service attacks and identifying the source of an attack. There are many types of IP traceback techniques available for both wired and MANET networks: manual traceback schemes, packet marking schemes (PPM), ICMP traceback schemes (ITrace), and logging-based traceback schemes.

The strategy used to trace DoS attacks in MANET is different from that used on the Internet in three ways. First, on the Internet both the attacker and the victim are located on the same subnet. This means when the attacker sends packets to the victim, the packets should be transmitted to the gateway first and then get on the path via routers until they arrive at the victim. The gateway is usually a router or computer which has a fixed IP address. The main aim of tracing a DoS attack on the Internet is therefore to determine the attacker's subnet. Meanwhile, in MANET the nodes move arbitrarily so the relative position between two nodes will change frequently. There will consequently be no fixed gateway for every node, so the address of nodes is considered to be flat. The purpose of tracing the DoS on MANET is to find out the physical location of the attacker (Jin et al., 2006).

Second, in tracing a DoS attack in the Internet it is impossible for the attacker to succeed in displacing quickly. In addition, the path that the packets use cannot be changed considerably (Shinde and Bakal, 2015). On the other hand, in MANET the path which packets pass through can change frequently. The time needed to trace the attacker should thus be short, because the attacker could move to another position before the tracing process is completed.

Third, in the Internet different devices such as routers, computers and switches have high and reliable computational abilities, and also unlimited battery power. The tracing algorithm would then be complex and more accurate, whereas in MANET nodes have constrained battery power and low computational abilities. The tracing algorithm is therefore accurate and simple when compared with tracing on the Internet. Moreover, traceback methods on the Internet consume a lot of computational resources, battery power and even bandwidth. However, in MANET nodes have limited computational resources, battery power and bandwidth.

Subsequently, MANET needs more efficient traceback schemes than the Internet. Nodes in MANET are arbitrary and can come in and out of the network at any time, meaning the attack path will change frequently. Attackers in MANET can also spoof the source address, which makes identifying the real attackers impossible (Vegda and Sahu, 2015).

(Jin et al., 2006) proposed a novel traceback scheme called the Zone Sampling-Based Traceback (ZSBT) algorithm which is used to trace denial of service attackers in MANET. The concept of this approach is based on dividing the network into a number of zones. Each zone puts its ID in every passing packet. When the node then receives a packet and wants to forward it to another node, the node first writes its own ID on the packet and the probability (P) then forwards the packet to another node. Using zone ID, which is written in the packet, it is easy to tell if a node has suffered a DoS attack or not. The victim can then reconstruct the whole path to the attacker by combing these packets (Kim and Kim, 2008).

Manual traceback schemes have many shortcomings, such as high management costs, inaccurate results and slow tracking speeds. Many traceback schemes which are suitable for wired networks, such as manual, logging-based and ICMP-based traceback schemes are inappropriate for MANET (Foroushani, 2013). This is because its characteristics rely on assumptions which are unsuitable for the MANET platform, such as trustworthy routers and static route topology (Shinde Sandeep and Bakal, 2014).

4.1.6 Pushback

Pushback is another mechanism which can be used to defend against DDoS attacks. If it is possible to determine whether a packet belongs to an attacker and drop it, the problem will be solved. However, routers cannot determine if a packet definitely belongs to a good or malicious flow. In the pushback mechanism, routers are enabled to identify the high bandwidth aggregates that participate in the congestion rate and help to limit them. Whenever the congested router fails to sustain this control then it requests the help of its upstream neighbour. If the attackers are collocated on a path separate from the normal traffic, the performance of the pushback mechanism will be better.

Pushback is unable to work in non-contiguous deployment, and is also unable to compromise attacks that do not overcrowd its core routers (Varadharajan and

Tupakula, 2014). In selective pushback, pushback messages are sent to the routers that are closest to the attack source by analysing the traffic, which leads to a change of upstream routers at the target.

This scheme has two main features. First, the location of the attack source via traffic distribution analysis will be determined more accurately. Second, mitigating the damage from a DoS attack can be more efficient because the pushback message will be sent directly to the routers closest to the attack source. However, this scheme cannot be very accurate when it is used in multiple domains (Gasti et al., 2013).

All in all, Pushback mechanism is useful and works well if there is indication of a DoS attack. However, the power of Pushback would be severely impaired by mobility issues, as with MANET there are no fixed upstream routers but rather nodes which carry the traffic through ordinary movements.

4.1.7 Game theoretic approach

A game theoretical approach is used in order to forward the good packets and filter out the bad packets using verification. Game theory classifies games into two groups: non-cooperative and cooperative. Non-cooperative games are composed from two or more players and compete with each other. In contrast, cooperative games consist of multi-players cooperating with each other in to gain the highest possible total benefits. This method is based on using digital signatures to verify legitimate packets. If any packet does not pass this verification process, it will be dropped and named a bad packet. In addition, bad packets sometimes escape the verification process if the forwarder does not verify the packet. There is a penalty to the forwarders of bad packets (Otrok et al., 2008).

Verifying packets would help users to discover malicious attacks and drop affected packets. There is also a reward system to forwarders that verify packets, which is gained as a credit. An accounting system is responsible for calculating these rewards and continuously tracking them (Rachedi et al., 2010). This system is such a game where forwarders verify packets that they receive. It succeeds in encouraging cooperation among nodes and mitigates DoS attacks in MANET (Wu and Yau, 2007).

4.2 Commercial solutions to detect DoS attacks

The revolutionary advances in the use of wireless networks in business, airports and homes has helped to increase the risk of certain attacks, such as DoS attacks. The increased number of DoS attacks in many sectors and organisations, such as banks and universities, has led to the creation of commercial software designed to detect and diminish the effects of these attacks. With the increase of threats beyond DoS attacks, many commercial programs and solutions have been proposed to protect both individuals and organisations.

For instance, Barracuda firewalls are designed to protect users against threats, malware and DoS attacks. In addition, the software guarantees service will be restored as soon as possible. The main aims of these security companies are to respond to incidents response, backup data and keeps customers away from threats such as DDoS and phishing attacks. Security companies help individuals and firms to maintain security and protection from intrusions. For instance, Dell SecureWorks is a famous security organisation which focuses on incident response and protecting customers from cyber-attacks (Secureworks, 2015).

These security programs cannot absolutely guarantee protection from these attacks. However, they can at least try to decrease the likelihood an attack will occur, and if it does occur then they can try to detect attacks as soon as possible in order to recover the system and control the effects.

4.3 Other methods used to detect DoS attacks in MANET based on using trust

Using trust in MANET helps to encourage nodes to participate in network communications. However, regards to MANET's nature such as resources constraints, trust establishment and trust management are complex in MANET. This section defines the meaning of trust in various sectors and highlights the existing studies in this area briefly.

4.3.1 The meaning of trust in different sectors

Another method used to avoid DoS attacks in MANET is trust between nodes. First, it is essential to understand what is meant by trust in MANET. Generally, trust means one party or person believes in someone else and always expects positive behaviour from the other side. This party or person is then

considered trustworthy. Originally, the concept of trust derived from social science as a degree of subjective belief against the behaviour of an entity (Roth, 2013).

In network security and communications, the concept of 'trust management' refers to a means of specifying and interpreting security credentials, relationships and policies (Pinyol and Sabater-Mir, 2013). Trust management is an essential tool in the relationship of nodes, in particular when nodes work together without any past interactions (Menaka and Ranganathan, 2013).

In the sociology sector, trust affects every work project, relationship, business venture, effort is engaged, and communication (Misztal, 2013). Personally and professionally, trust changes the quality of each present moment, as well as the trajectory and outcome of each coming moment of life. Moreover, trust is essential to building strong relationships, which lead to cooperation between people (Harper, 2014).

Trust has different meanings in economics, and may be either impersonal and personal or informal. An example of the former is buying a product online and giving a website your personal credit card information to complete the purchase process. The latter is the trust built from personal experience, such as being friendly. Trust in economics is therefore an expectation which applies to situations where risky action is taken based on incomplete information (Horváth, 2013).

Trust in philosophy is critical and is important in life, as people usually use trust to rely on others for help, advice and when making important decisions. Moreover, trust can be a moral behaviour in human society (Marshall and Elghossain, 2014).

Trust in psychology grows from birth and becomes stronger over time depending on one's relationships. For example, a child which grows up in a very loving family is likely to express love and trust toward other people. When trust is lost, regaining it is difficult. We believe someone we have high trust in is less likely to cheat, steal or lie to us. In addition, a trustworthy person is less likely to be conflicted, unstable or sad, and is sought by many people. However, many trustees have been deceived and fooled by distrusting trustworthy people (Tyler et al., 2014).

There is a difference between confidence and trust, as confidence is based on knowledge or predictability whereas trust is needed preserve interactions. In real life, trust is emotive and has various levels. Trust in relationships is also provisional and contested. People have to trust each other in certain situations. For instance, a customer demonstrates trust in a store website when they purchase an item and insert

all their payment details. This trust is based on the store's reputation. In real life trust is temporal and related to past information, reputation and the future (Haggerty, 2012).

4.3.2 Using trust to detect DoS attacks in MANET

The usage of trust is used, combined with security, in order to enhance the security level (Felici, 2013). MANET has five properties of trust. First, trust is dynamic and not static, so trust establishment is based on spatial and temporal information. Second, trust is subjective. This means a trusted node can display a varying level of trust against the same trusted node regards the different experience and that due to the dynamic topology of MANET. Third, trust is not transitive. For example, if node A trusts node B, and node B trusts node C, it does not mean that node A trusts node C. Fourth, trust in MANET is asymmetric. Usually a node with higher capabilities and more energy will not trust a node with less power. Fifth, trust is context-dependent, so nodes trust others depending on the task, such as trust in selfishness or in computational power (Cho et al., 2011).

For instance, Alice can trust Bob's abilities as a mechanic but not as a plumber. A comprehensive study of trust management in MANET provides different definitions of trust which are dependent on different fields, including economics, organisational management, psychology, autonomic computing, as well as communications and networks (Chen et al., 2014). In addition, many studies have investigated ways to detect misbehaving nodes in addition to attack and design protocols based on different directions. For example, there are many research directions and protocols based on secure routing, access control, authentication, trust evaluation, trust computation, trust distribution and general trust level identification (Cho et al., 2011).

(Blaze et al., 1996) conducted the first research into trust management for network security. They considered trust management to be a separate component of security services within a network. The effectiveness of trust management is that it is possible without any previous interactions the nodes in the network can participate with an acceptable average of trust relationships of nodes. The main objectives of this framework are to support localised control and relationships by binding public keys to allow the access control process to proceed without complex security authentication procedures. This paper's only limitation is that only localised trust

management is based on an entirely decentralised concept, which is essential to policy information (Seigneur et al., 2013).

In MANET, trust management is used for two motivations. First, trust management can help to identify and isolate misbehaving nodes, decreasing the impact of faulty nodes. Second, trust management can predict a node's future, helping to improve network performance (Govindan and Mohapatra, 2012). Trust management is classified as both a trust-establishment framework and a reputation-based framework (Li et al., 2007). The former evaluates neighbouring nodes based on direct observations, as trust between nodes is built by combining opinions from intermediate nodes (Cho et al., 2012). Multiple trust management schemes have been developed for MANET. (Marti et al., 2000) argued for the use of secure routing in particular, as one trust management scheme consists of both a watchdog and a pathrater. The watchdog is used to monitor node behaviours, whilst the pathrater collects reputations and forms reactions. It is observed that this method is based only on direct monitoring (Varshney et al., 2014).

With regard to MANET, definitions of trust can be classified into four categories: trust as a risk factor, trust as belief, trust as subjective probability, and trust as a transitivity relationship. This study defines trust as dynamic, and as oscillating over time. Many attacks can occur in trust management in MANET, including Sybil attacks, collusion attacks, and DoS. Furthermore, the study explains the three main areas of trust in MANET are trust propagation, trust aggregation, and trust predication. The two main requirements that must be considered when developing any trust management method are the detection of maliciousness and the accuracy of trust. The authors assume that the area of trust management is not yet fixed (England et al., 2012). Every node which conducts a trust calculation on another node will raise the resource cost. Unfortunately, these resources are limited in MANET. It would thus be beneficial to share trust values with nodes, which is known as trust propagation.

Trust propagation has two additional requirements. First, partial availability should be available at the time, which according to the nature of MANET means just partial information. Trust can be calculated when only some of the trust scores can be obtained. Second, minimal overhead is another requirement as resources in MANET are limited (Zouridaki et al., 2006). The disadvantage of trust propagation is that attackers can exploit the advantage of this method by consuming as many

resources as they can by flooding the network with trust recommendations. The network will then suffer from a DoS attack (Govindan and Mohapatra, 2012).

Establishing trusted communications in MANET to ensure authentication is another way to perform security in MANET. (Weimerskirch and Thonet, 2002) used human behaviour as a base to develop a novel trust model. Society in this research is considered to be an *ad hoc* network. The Secure and Objective Reputation based Incentive (SORI) is developed as another reputation based trust management scheme that employs an incentivized approach. This scheme is based on encouraging the forwarding packets process whilst discouraging selfish behaviour through the use of a reputation propagation method and quantified objective measures.

Another approach based on a reputation trust management scheme is known as Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks (CONFIDANT). This method is unique as it provides an incentivised approach for altruistic nodes, paid as a response for cooperative action. This scheme is based on detecting misbehaving nodes via direct and indirect observations, and recommendations from other nodes. CONFIDANT results suggest that 60% of the network contains misbehaving nodes. CONFIDANT is used as a benign network. CONFIDANT is constructed of four main processes: monitoring, a reputation system, a path manager and a trust manager. Monitoring is responsible for checking each forwarding packet in order to detect any deviations. The reputation system maintains the identities of the table of nodes using associated ratings. The path manager removes the path which contains the malicious node, whilst the trust manager transacts with the sent and received alarm messages. CONFIDANT uses timers which are associated with each node identity; when a timer expires, the node is considered legitimate (Buchegger and Le Boudec, 2002).

A new mechanism is proposed: COllaborative REputation (CORE). This approach combines a reputation function with a monitoring mechanism. CORE is intended to provide a decision-making process regarding the cooperation or gradual isolation of a specific node (Michiardi and Molva, 2002). An innovative characteristic of this approach is that the exchange of solely positive and reputable information can occur. The only limitation of this approach is that it can decrease the resilience of positive reports, whilst there is no facility to submit negative feedback (Thorat and Kulkarni, 2014). However, CORE differs from CONFIDANT as the latter sends the reputation values to nodes in the network, allowing fake reputation values to be spread maliciously, while the former uses the reputation values defined

by each node. In addition, the CORE scheme allows only positive reports to pass through, but CONFIDANT also allows negative ones. CORE is thus better at preventing the false reports which cause DoS attacks (He et al., 2004).

(Zhong et al., 2003) proposed a simple cheat-proof credit-based system named SPRITE. This system applies an incentive to MANET by encouraging selfish nodes to cooperate with other nodes. A node will inform the credit clearance service about received messages, or will even forward messages by uploading receipts (Buttyán and Hubaux, 2003). The intermediate nodes then gain credit if they succeed in forwarding the message to other nodes. Generally, credit systems give nodes an incentive to cooperate (Crowcroft et al., 2004). When a node relays a packet to other nodes, it will therefore receive credit it can use to send its own packet. Meanwhile malicious nodes will continue to drop packets, which will eventually deplete their credit eventually so it will not even be able to send its own traffic (Dev and Augustin, 2015). One benefit of SPRITE is that it takes both public key infrastructure and source routing into consideration. The superiority and merit of this work is highlighted by the relatively low cost overheads, as well as its ability in areas such as MANET and its constrained resources. SPRITE however is considered unreliable as the resources of nodes are low (Sedghi et al., 2013) .

(Liu et al., 2004) posited trust levels in the routing process. Source nodes use the trust level to evaluate the security of the destination point. Subsequently, trust levels can be used as a guide to the source node and selecting the most appropriate and secure route. Trust management schemes are used to detect misbehaving nodes, for example selfish and malicious nodes. Many attacks have been deterred based on the implementation of trust management strategies, such as varying types of DoS attacks, including wormhole, blackhole and grayhole attacks. MANET employs many trust management schemes based on secure routing, authentication, IDS, access control and key management.

In addition, (Sun et al., 2008) introduced a ‘trust manager’ element into their scheme. This scheme is based on determining the trust level of the node by drawing upon self-monitored information. As a result, reputation is collected via direct and either indirect observations or experience. No results have been generated from this approach, but some important questions are raised. A key question is the nature of the relationship between the number of tolerated malicious nodes and the total number of nodes in the network.

(Denko, 2005) proposed the use of reputation-based incentive mechanism for detecting and preventing DoS attacks in MANET. This method uses a clustering architecture to perform reputation data management in both distributed and localised ways. This method allowed DoS attacks to be detected using information exchange and collaborative monitoring. The reputation rate is proceeded using cluster level information and neighbourhood, but more weight is given to the node's observation. In order to reduce traffic between cooperative nodes, a load balancing mechanism is used. Simulation results reflect the success of using this method considerably. It is important to distinguish between selfish and malicious nodes. The former type refuses to cooperate with other nodes in the network to perform network services and operations, while the latter type performs attacks in order to degrade the performance of the network. Trust-based routing algorithms aim to identify malicious and selfish nodes in MANET.

Observation-based Cooperation Enforcement in Ad hoc Networks (OCEAN) is an extension of the DSR routing protocol. OCEAN uses both monitoring and reputation systems. Unlike the approaches discussed above, OCEAN relies only upon its own observation to bypass the new intrusions of false accusations from second-hand reputation exchanges. OCEAN is therefore standalone architecture. OCEAN considers two kinds of routing misbehaviour: misleading and selfish. When a node has participated in the route discovery but not packet forwarding, it is considered to be misleading because it misleads other nodes in order to route packets via itself. However, if a node does not participate in the route discovery, then it is considered to be selfish (Anantvalee and Wu, 2007). A Locally Aware Reputation System (LARS) has the same concept of OCEAN as it relies on the local information in order to handle and isolate misbehaving nodes and does not consider second hand reputation information (Hu and Burmester, 2006).

In order to deal with selfish nodes, a new mechanism is conjectured. This approach encourages nodes to cooperate in MANET by employing many components of trust, including transitivity, subjectivity and dynamicity. In order to evaluate trust, this scheme uses packet forwarding behaviours (Soltanali et al., 2007). To strengthen the power of security within MANET, a new trust model is proposed. This research focused on issues related to recommendations. Only trusted routes are used in this model when communicating between nodes. Furthermore, malicious nodes are isolated based on information from direct interactions and

recommendations. This model considers the traits of DoS attacks and attempts to detect them within the network (Balakrishnan et al., 2007).

In order to construct trusting relationships, this study uses recommendations as mentioned by (Li et al., 2009). Trust can be calculated using these recommendations, so this work will use trust for the purpose of authentication. The model is based only on monitoring packet forwarding behaviours. (Moe et al., 2008) proposed an extension of the DSR referred to as a Trust-based Secure MANET Routing (TSR). This is based on an incentive mechanism which promotes cooperation among nodes and weakens the strength of selfish nodes as far as possible. In addition, this work uses a Hidden Markov Model (HMM) in order to quantitatively measure the trustworthiness of nodes. The selfish node is described as benign as it drops packets selectively. The only limitation of this work is that it cannot detect modifications and some attacks performed by malicious nodes.

(Chang and Kuo, 2009) proposed the use of the Markov chain trust model in order to generate Trust Values (TVs) for one-hop nodes. TVs are computed based only on direct observations of node behaviours, not by measuring the decay based on the recommendations from other nodes. By using a Certificate Authority (CA) server and a backup CA with high levels of TVs, this scheme delimits a trust-based hierarchical key management approach. However, this work is limited due to the lack of consideration of trust decay, although trust is based on the recommendations of other nodes.

It is proposed that the Distributed Cooperative Trust based Intrusion Detection (DICOTIDS) architecture for MANET can protect the network from misbehaviour, such as selfish nodes. The key aspect of this framework is to use both direct and indirect observations among nodes. In addition, this framework can target false trust information propagated by malicious nodes within the network. This method uses the ‘promiscuous mode’ to observe other nodes. The main goal of DICOTIDS is to detect compromised nodes which disseminate false detection alerts in MANETs. This method is based on using trust with IDS. This approach uses a reputation mechanism to rate nodes. After detecting misbehaving nodes, a distributed IDS algorithm will broadcast IDS alert messages among nodes. All data collected from the nodes will be shared between them periodically. The reputation mechanism is used to evaluate the level of trust in a specific node. In summary, the level of trust - whether trusted, untrusted or undecided - is calculated based on the reputation value in this method (Mutlu and Yilmaz, 2011).

(Khan and Vatsa, 2011) proposed a new method to detect DDoS attacks in MANET by providing a credit-based mechanism. This method helps nodes in MANET to cooperate. The performance of this method is based on three phases: reputation and score-based cluster creation and cluster head selection, DDoS classification of attacks and their detection, and DDoS control packet requests. This method is efficient, and its only limitation is the mobility issue. This was not considered when designing the architecture, as the cluster heads are assumed to be stationary so that only the nodes of the cluster could move freely. Scalability is another issue, as in order to balance the workload on the cluster, the size of the network would increase dramatically.

Another study which uses a reputation, trust based scheme and credit to enforce nodes communications was posited in (Abbas et al., 2011). Identity based attacks such as the Whitewashing and Sybil attacks have affected the performance of this method. In order to hinder these attacks, a non-monetary and entry fee per identity is used that helps to handle these type of scenarios considerably. The limitation of this work is that newcomer nodes are not welcomed with regard to the free identities available in the network. Simulation results provide better evidence in plummeting evil nodes and evil throughput compared to the CONFIDANT scheme in the occurrence of whitewashing nodes.

Another collaborative and multidimensional trust-based outlier detection algorithm is proposed in order to secure MANET and detect misbehaving nodes. This allows nodes which have exhibited abnormal behaviour to be identified. In addition, this algorithm evaluates the trustworthiness for nodes from three perspectives: Collaboration Trust (COLT), Behavioural Trust (BET) and Reference Trust (RET). COLT is determined based on the collaboration rate, while BET is defined based on the misbehaviour rate, such as the number of flooding attacks. RET is determined based on the correctness of the opinion given to other nodes. The initial trust value is 1. A punishment factor is applied to the trust value of any misbehaving node. These factors will be updated using the weighted voting method in the local view update step. Although this algorithm records downgrade, it is considered better than other methods such as Simple trust-based Weighted Voting (SWV) and the Simple Averaging (SA) method (Li et al., 2009). The limitation of this method arises due to differing circumstances; for example, if the majority of nodes are malicious, then the local views are unreliable. Furthermore, this method is overly robust in small communication overheads (Li et al., 2012).

(Xia et al., 2013) suggested another trust model which is extended from Trust based Source Routing protocol (TSR). This method relies on the individual experience and prediction methods to indicate the safest route from source to the destination. Nodes prediction trust value is considered as the input. Untrusted nodes would be removed from the transmission in this situation. Nodes can be malicious, suspect, low trustworthy, trustworthy, and completely trustworthy.

(Vir et al., 2013) proposed the use of another trust-based routing system to update and store the trust value of nodes in MANET. This system assumes that evaluating trust will help to concisely distinguish between normal and malicious nodes. The study also provides a strong comparison between the three types of routing protocols in terms of throughput and trust-based average jitter: DSR, AODV, and DYnamic MANET On-demand (DYMO). The results showed that the AODV protocol was the strongest, as it delivered 65% of packets - more than the other protocols.

(Aravindh et al., 2013) proposed another trust management scheme to calculate trust in MANET. This research uses direct observation to calculate trust, which helps to successfully isolate malicious nodes from the network. Furthermore, this methods uses trust values to favour packet-forwarding by maintaining the trust counter of every node. If the trust-counter value decreases below a certain threshold, the corresponding intermediate node is considered malicious and is isolated from the network.

(Gunasekaran and Premalatha, 2013) suggested the use of MANET-specific Trust Enhanced Anonymous on-demand routing Protocol (TEAP). TEAP aims to control anonymity in two ways. First, by reining-in misbehaving nodes after receiving two warning alerts, which leads to compromised nodes not sending cooperative messages to other nodes. Second, if any node sends the same claim message about a certain node, then it is considered to be misbehaving. The TEAP protocol uses the concepts of anonymity and liability to detect misbehaving nodes in MANET. The results of this study reflect the efficacy and robustness of this protocol in detecting anomalies.

(Kartha and Neeba, 2014) developed another technique to establish trust in nodes. Trust is assigned to a node according to the history of communications of trustable path from source to destination as the trust values of nodes are aggregated. The simulation results prove the power of this method in decreasing both overhead and drop packets.

(Krishnan et al., 2015) estimated node trust using two agents. The first agent continuously tracks any packet dropping and link failures. The second tracks any attack or malicious activities in the network. These two agents of trust interconnect the nodes with trusted nodes that improve the network performance. The results of this method highlight the effectiveness of this model, as it gives low delays and high throughputs.

Another study restricts and punishes selfish nodes as they are not provided with packet forwarding services by the good nodes within the network (Abbas et al., 2015). Thus, good or normal nodes will increase the network throughput and decrease the misbehaving nodes activities. In this study of cooperation schemes in MANET, where Direct Interactions (DIs) might affect metrics, such as delay, routing overhead, throughput, and utility, these metrics are evaluated. With regard to the simulation results, the cooperation promotion schemes need to be evaluated utilising wider areas for constant radio ranges to diminish the effect of DIs.

A trust based routing strategy termed routing Secure-BEst FOrwarding Route Estimation (BEFORE) is proposed to guarantee the optimal route estimation in calculating the trust value and hop counts utilising the dummy packets inside the network at the 1-hop level. The problem with this method is that some 'intelligent' DoS attacks cannot be detected, such as a grayhole attack. Only genuine nodes can send a dummy packet to the destination, therefore, a grayhole node pretends to be a genuine node and drops the packet. Another limitation is redundancy and overhead as nodes send RREP to the source nodes and only one-hop nodes are considered while the others are dismissed (Shah et al., 2016).

The Trusted Secure AODV routing protocol (TSAODV) is positioned carefully. This protocol is based on calculated trust values and determines the status of the node based on different factors such as communication type. The node can be one of the following: reliable; unreliable; and mostly reliable. Different trust levels between 0 and 1 determine the node's status. If the node is either reliable or mostly reliable then it is allowed to participate in the network communications, otherwise, it is blocked from communications. The drawback of this work is the MANET, with its mobility, increases the rate of packet dropping regardless of the congestion. Therefore, if the node fails to send RREP then it can be considered mostly reliable or unreliable (Singh et al., 2016).

A further study which presents a comprehensive survey regarding the reputation based method which help to detect and even isolate misbehaving nodes from communications is carried out in (Abbas et al., 2010). Another study examining establishing trust in MANET based on different themes is illustrated in (Dalal et al., 2012). In addition, studies which look at trust-based routing protocols in MANET and trust management to encourage nodes to cooperate are illustrated respectively in (Thorat and Kulkarni, 2014 ; Gandhi and Jhaveri, 2015 ; Vijayan and Jeyanthi, 2016).

4.4 Current methods used to assign IP addresses and merge MANETs

Regarding the mobility of MANET, the chance of both MANET merge and partition occurs. Figure 4.1 shows the pre- and post-merger of two MM. Due to the dynamic topology of MANET, and the absence of central management, it is essential to assign an IP address and guarantee it is unique to avoid any IP address conflict.

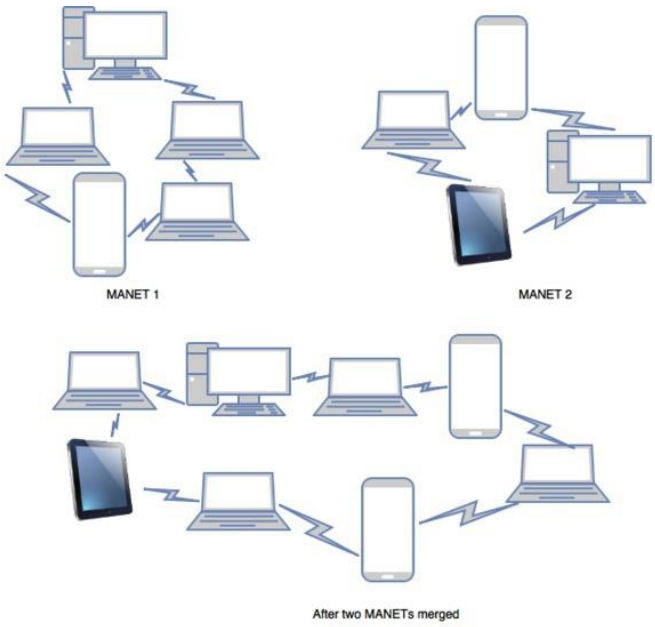

Figure 4.1. The scenario of two MANETs merge.

This section gives detailed information about the IP address, assign IP address to nodes in MANET, and how the IP address conflict problem is solved in MANET environment according to some existing studies.

It is essential to take into consideration the security aspect when assigning the IP address; for example, if a malicious node provides an incorrect vacant IP address to a new node, an IP address conflict would occur.

4.4.1 IP address

Internet Protocol (IP) addresses are designed to allow a device to communicate with other devices via the Internet. IPs facilitate the completion of many actions on the World Wide Web (WWW) and govern Internet activities. IPs thus identify both initiating devices and various Internet destinations, which enable two-way communication. In IP version 4 (IPv4), each device has a unique IP address which identifies the device on the Internet. Each IP address is composed of four numbers separated by a dot. These numbers can have between 1 and 3 digits. Each of the four numbers may range from 0 to 255. An example of an IP address could be 58.123.0.208 (Rooney, 2011).

The Dynamic Host Configuration Protocol (DHCP) is a standardised network protocol used on IP networks to distribute network configuration parameters dynamically, such as IP addresses for services and interfaces. Devices using DHCP can request IP addresses and networking parameters automatically from a DHCP server. This reduces the need of a user or a network administrator to configure these settings manually (Carrell et al., 2012).

4.4.2 Assign IP address in MANET

Assigning IP address in wired networks is easier as the DHCP helps to assign IP addresses to clients. However, this method cannot be used in MANET as it requires the central server to allocate IP addresses to nodes. MANET's non-fixed infrastructure devoid of central management cannot use this method. Assigning IP addresses in MANET is a challenge due to its dynamic topology and mobility. MANET needs an efficient and reliable host identifier for communications (Choudhury et al., 2015). In order to ensure proper routing, assigning unique IP address in MANET is a prime task.

Three types of method are used to assign IP addresses in MANET: leader-based allocation, best effort allocation, and decentralised allocation. The majority of

these methods use the Duplicate Address Detection (DAD) method to identify IP address conflicts on the network. The DAD algorithm is used when entering a new node into the network, or when MANETs merge. For instance, the new node picks up a tentative IP address and uses the DAD method to check the availability of this IP address with all existing nodes in the network. The node then sends a Duplicate Address Probe (DAP) message to nodes and waits to receive the Address Conflict Notice (ACN) message within a specific timeout period. If the ACN is not received, the node assumes that the IP address is available. There are a number of limitations to using the DAD method. First, when the packet reaches its destination there is a chance that the duplicate is being tolerated. Second, this method depends on routing protocols, which involves traffic overhead caused by the routing packets (Vaidya, 2002). Passive DAD is a modified version of the DAD method. Periodic link state routing information is used by nodes to inform other nodes about their neighbours. Unfortunately, this technique has a number of drawbacks, such as contention, absolutely costly, redundancy, and collision which is called broadcast storm problem (Weniger, 2003).

In leader-based allocation schemes, an elected leader will allow nodes to obtain valid IP addresses as needed. This method does not require the use of the DAD method during the assigning of IP addresses, partitioning or merging. Using DHCP is a method under this category. The concept of this protocol is based on client/server where a central point is important. DHCP servers are responsible for assigning IP addresses for nodes which require a vacant IP address. The node therefore broadcasts a message in order to discover the server (Droms, 1997). The Dynamic Address Configuration Protocol (DACP) is designed to encourage the dynamic address allocation process in MANET. An elected Address Authority (AA) will maintain the state information of the network. A tentative address is used to verify the IP address and ensure its uniqueness using the DAD scheme. The limitations of this protocol stem from its high overhead, as messages flood networks using both AA and the DAD method (Hsu and Tseng, 2005).

The best effort allocation approach allows a node to assign its own addresses and does not involve any other nodes within the network. Therefore, these approaches do not guarantee uniqueness of IP addresses and need the DAD mechanism to bypass IP address conflict to ensure correct communication (Munjal et al., 2013).

Decentralised allocation is the third type, as a host acquires an IP address, either itself or from a neighbour, and then applies the DAD to ensure the uniqueness of the IP address (Xiaonan and Huanyan, 2013).

4.4.3 Examples of existing method to assign IP in MANET

Based on the address management, three types of protocols are needed to configure incoming nodes: stateful protocols, stateless protocols, and hybrid protocols. Using stateful auto-configuration protocols, every node maintains a table relating to the IP addresses of other nodes, while stateless protocols require every node to administer its own IP address. In the latter case, the node creates a random address and applies a DAD algorithm to discover any conflicts (Kim and Chung, 2013). Hybrid protocols are a mixture of the other two types that can improve the reliability and scalability of auto-configuration; hence, this type of protocol has a high level of complexity (García Villalba et al., 2011).

4.4.3.1 Stateful Protocols

Dynamic Address Allocation Protocol (DAAP) is based on the idea of address assignment by a leader. The leader functionality is shared through whole network nodes. If a new node joins the network, it would be the leader until the next node joins. A unique identifier is linked with the network. In addition, the leader preserves the highest IP address within the network (Patchipulusu, 2001).

MANETconf is a stateful auto-configuration protocol used to allocate IP addresses for nodes in MANET. When using this method, each host in the network acts as an initiator to allocate IP addresses for new hosts. This method maintains both a distributed allocation table and a pending allocation table. The former is used to find un-configured addresses. The latter is a group of in-use configured IP addresses and a set of initial incomplete allocations. In addition, the pending allocation helps to bypass concurrent address allocations. The requester will ask the initiator about free and unused addresses via broadcast message. However, the initiator would flood the network simultaneously with asking messages in order to ask all hosts about the ability of the address allocation. In situations where all hosts confirm that a pending address is unique, this address will be assigned. Otherwise, the process will be repeated using a new address until a unique address is available (Nesargi and

Prakash, 2002). This method identifies both network partitions and merging, although identifying merging is more problematic. This is because using this method means two tables are maintained which transmit periodic control messages. This would raise communication overheads, latency, and affect the efficiency of communications (Sadok et al., 2014).

A decentralised address configuration method called Prime DHCP (PDHCP) is developed by (Hsu and Tseng, 2005). This means a node can obtain a unique address without using the DAD algorithm. Every node works as a DHCP proxy and uses a prime numbering address allocation algorithm in order to compute a unique address for every new node. However, this method does not consider the issue of address recovery. When the address resources for the assignment of a DHCP are required, the DHCP proxy has to ask its own ancestor node to complete the address configuration process. The address configuration cost is therefore high, and even the delay is prolonged.

According to (Mansi and Ravi, 2006) , every node in the network preserves a collection of unassigned IP addresses. When a node moves out the network, it will return its address to the corresponding collection. When the node leaves the network suddenly or fails, the address resource will be lost. For this reason, the periodic-flooding query method is used in this approach to reclaim address resources lost by failed nodes. However, the periodic flooding query will consume the network's resources.

(Zhou et al., 2010) elucidated the use of a prophet address allocation scheme in MANET. A function f (n) is used to generate a collection of random numbers to assign addresses. The first node in the network will generate a random number and define its address to the number. A random state value will be used by the node as a seed for its function f (n). When a new node needs to obtain an address, then the first node could do so with a state value as the seed for its function. In situations where a new node enters the network, this node will perform the same process to acquire an address. The address configuration latency and cost in this scheme is low. On the other hand, its main drawback is that address conflict still occurs and can be solved by using a weak or passive DAD.

(Gammar et al., 2010) suggested using an address configuration scheme in MANET. The address configuration process uses the transmission of the control packets and is controlled by a two-hop scope, decreasing both delay and the address

configuration cost. However, this method cannot reuse the address resources released by failed nodes.

(Al-Mistarihi et al., 2011) illustrated the use of the Tree based Dynamic Address Auto-configuration Protocol (T-DAAP) for MANET. This protocol arranges the network in a tree structure. In addition, nodes are divided into three groups: root, normal and leader. The root node is responsible for keeping information on all leaders in the network, so it would be easy for any leader to check the status of other leaders. The network will have just one root node, which is responsible for network merging and address reclamation. Although the normal node does not have main functions in this protocol, it acts as a relay in many situations. The leader node consists of a disjointed free address pool and is responsible for assigning IP addresses to new nodes. The disadvantage of this protocol is that the root node maintains information on all leaders, which increases the address configuration cost.

(Ghosh and Datta, 2011) developed an address configuration method whereby a new node broadcasts a discovery control packet to its neighbouring proxy nodes. When the discovery control packet is broadcasted by the new node is received by a proxy node, an offer control packet returns by the proxy node to the new node. The proxy node with the minimum address is selected by the new node as its father node. The new node then sends a select control packet to its father node. The father node requests the address resources from its ancestor nodes if it does not have address resources. The father node returns an Acknowledgment Packet (ACK) to the new node. In addition, the payload of the ACK packet would be the assigned address. If the father node does not have address resources, then the address configuration cost raises and the delay increases. Moreover, this method assumes that the first new MANET in its initial state sets its address as 0. The drawback of this method stems from a scenario whereby two new nodes join the MANET at the same time, which might cause an address conflict to occur.

(Wang and Qian, 2014) discussed distribution address configuration methods for MANET. In this method, common nodes have unique address spaces in order to assign IP addresses. In addition, an isolated node can obtain a unique address from its neighbouring common nodes without the use of the DAD algorithm. Because of this, the address configuration process is distributed around the common node. A comparison between this scheme and other existing methods suggests this method decreases the address configuration cost and the delay.

Moreover, an address allocation algorithm is proposed. This algorithm bypasses network-wide broadcasts to allocate an address to a new node. Furthermore, this method helps to allocate addresses dynamically as the network maintains an 'IP resembles topology' state. Thence, routing becomes easier and the overall overhead in communication is decreased. In addition, this algorithm is simple as the hierarchy in IP addresses is used, therefore, the algorithm is simple (Khatri et al., 2016).

4.4.3.2 Stateless Protocols

(Sun and Belding‐Royer, 2004) proposed the use of a stateless address configuration method based on DAD. The DAD packet will be broadcasted across the entire network in this scheme. The latter will therefore consume network resources and bring a high number of control packets.

Automatic IP Address Configuration (AIPAC) is a type of stateless auto-configuration protocol in MANET. This protocol aims to avoid any wastage of available resources. In this method, new nodes need a minimum of one neighbouring node in order to be configured. The new node might be a new un-configured node or an already configured node. After the new node enters the network, it selects a random 4 byte Host Identifier (HID) and sends GetConfig messages periodically until it receives a reply from neighbouring nodes. When the neighbour node is un-configured, the node with the highest HID will begin the network initialisation process. The neighbouring node will select a net ID for the new network and an IP address for it and the second node. The node with the highest HID value will send the initialise message to the second node. Alternatively, in situations where the neighbouring node is already configured, it would act as an initiator for the un-configured node. The initiator therefore selects a random address and broadcasts the search IP message to all configured nodes within the network. Each node which receives this message will check whether or not this IP address is vacant. In a scenario when there is IP conflict, it will respond to the initiator with a used IP message. The initiator will then choose another random IP address, and the initialising process will be repeated. When the search IP timer expires, the initiator will resend the search IP address. If no reply is received, the selected IP address is vacant. Next the initiator sends the net ID and selected IP into the requester node

(Fazio et al., 2006). The main limitation of this method is that it is not scalable and complex to implement (Munjal et al., 2013).

A dynamic and distributed method which uses Conflict-Free Auto-configuration Addresses (CFAA) in MANET is presented by (Indrasinghe et al., 2006 ; Indrasinghe et al., 2007). This novel method generates IP addresses automatically and ensures they can be reused. Two MANET scenarios are considered in this method: partitioning and merging. This method uses the existing address space with regard to the child-parent relationships of hosts to implement the allocation of reusable addresses. If the root host is unavailable, then the address is reused by re-allocating the root address.

(Indrasinghe et al., 2008) evaluated this work and compare this method with other existing MANET auto-configuration methods. The study also evaluates a CFAA scheme for new host configurations and even the merging of MANETs with respect to network merging and address assignment (Indrasinghe et al., 2009). The same study also discusses different kinds of broadcasting methods and cluster formation in message broadcasting. In addition, a novel solution for both MANET merging and the more complicated case when the MANET ID is part of the IP address is the same for the merging MANETs. Granting a unique name for every MANET could allow its own group members to be identified from among other hosts from various networks, and so circumvent the difficulty posed by IP address duplication after a merger of MANETs that had the same MANET ID part of the IP address. Every host in MANET is able to generate a range of addresses, and the ranges of any two host's addresses will be disjointed. Each host thus generates numbers unique for that host. The number of unique addresses which are generated by every hosts according to a selected Base Value. Hosts are numbered depending on the order of their arrival to the network. If the host departs from the network, the number is reused (Amgahd and Yadav, 2016). Another study discusses the difficulties of secure message transmission and assigning IP addresses to new nodes which are willing to join the network. Symmetric and asymmetric keys and timestamps are used to authenticate the message transmission. In addition, every node is regarded as a proxy server which could allocate the IP to any new node. In addition, every node has a unique tuple of node ID, MANET ID, and its own IP address for merging and partition scenarios in MANET. This method is secure, however, the overhead of using symmetric and asymmetric keys is high (Choudhury et al., 2015).

4.4.3.3 Hybrid protocols

(Weniger, 2005) presented Passive Auto-Configuration for Mobile Ad hoc Networks (PACMAN). This method is efficient, is distributed address auto-configuration and supports many situations such as partitioning and merging. The protocol overhead is low as it uses cross-layer information derived from on-going routing protocol traffic. Moreover, PACMAN assigns IP addresses in a way which enables their compression, and significantly decreases the routing protocol overhead.

Nominate the trust worthy nodes to assign IP address in MANET is conducted in (Hu and Mitchell, 2005). This method is based on MANETconf assumptions. In this method, every node has a threshold trust value to calculate the trust value and decide whether the node is trusted or malicious. The node whose trust value is greater than or equal to a threshold value is deemed as trustworthy. The trustable node is used as the initiator to assign an IP address to the requester node. A DAD algorithm is used in this method to check any conflict. However, the authors made some unrealistic assumptions which rendered their model unsuited for MANET. In addition, there is no consideration for security during the IP address configuration process. Overheard is another drawback of this method regards the usage of DAD method. This method does not handle specific scenarios in MANET such as during the merging and partition processes of MM.

The Scalable Hierarchical Distributive Auto Configuration Protocol (SHDACP) is designed to configure and manage the IP addresses of large MANET. In this method some nodes are termed cluster heads, which are responsible for configuring nodes within the network. The main idea of this protocol is to divide the address space into three fields: partition number, node id and cluster number. This method supports the merging scenario. Using this method gives better results than approaches such as MANETconf and AIPAC protocols (Munjal et al., 2013).

(Singh et al., 2014b) presented the election algorithm, which uses a node as a cluster head based on its weight. The weight is calculated based on different factors such as battery lifetime, neighbouring node numbers and the transmission level. Heavy nodes will be elected as the cluster head. The network in this method is divided into sub-networks as clusters in order to improve the address auto-configuration in MANET. The cluster head is the coordinator of the cluster. Moreover, the method supports both partition and merging methods. It should be noted that the simulation results reflect the power of this method in raising the packet

delivery ratio and minimizing the packet delay ratio. Basically, prior works focus on preserving a stable link between cluster heads and other members. In addition, the velocity of cluster heads are also measured (Chatterjee et al., 2000 ; Chatterjee et al., 2002). A survey about existing methods to assign an IP address in MANET is featured in (Abdelmalek et al., 2009). Many studies have investigated address auto-configuration and presented many such protocols. For example, (Wangi et al., 2008 ; García Villalba et al., 2011 ; Zhou and Mutka, 2012) offer a comprehensive summary of existing auto-configuration addresses in wireless *ad hoc* networks.

4.5 Chapter summary

This chapter provides an overview of all studies related to the proposed method used in this thesis. Identify the advantages and disadvantages of the existing methods in order to design a new method and bypass the limitations of the existing studies. Many topics are considered, such as existing methods capable of detecting DoS attacks in MANET, using trust to detect misbehaving nodes in MANET, merging MANETs, and assigning IP addresses in MANET. These studies are interconnected, and understanding them is important in order to understand existing methods and their performance, and how to differentiate them from the proposed method. Moreover, commercial software has been explained and some examples have been mentioned. Figure 4.2 illustrates the scope of studies that are discussed in this chapter.

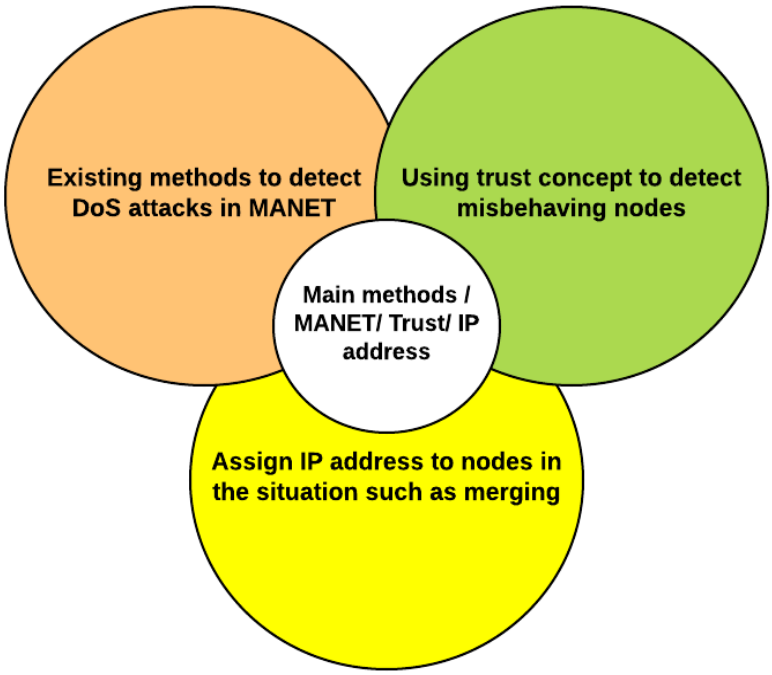

Figure 4.2. Scope of the study.

In the next chapter, the methodology, design and analysis, in order to present the proposed method to detect DoS attacks in both Single MANET (SM) and Multi-MANETs (MM) environments will be explained in detail.

Chapter 5: Design and Analysis of Monitoring, Detection and Rehabilitation Method - MrDR

In the previous chapter, the existing methods used to detect DoS attacks are illustrated including their advantages and disadvantages. Thus, there is a pressing need to design a new method to detect DoS attacks in MANET that considers the advantages of the existing methods and avoids the disadvantages of the existing methods. This chapter outlines in detail the proposed method which is used in this research to detect DoS attacks in both Single MANET (SM) and Multi MANET (MM). This approach is called Monitoring, Detection and Rehabilitation (MrDR). Its name is derived from the stages used in this method to detect DoS attacks in MANET. Due to the mobility of MANET, network merging can occur. Under these circumstances, many issues need to be considered, such as assigning an IP address, as well as avoiding an IP address conflict and consider security aspect in the situation of merging. In addition, the method design and analysis of both SM and MM will be explained in this chapter.

5.1 The concept of trust in the MrDR method

In real life situations, individuals are obliged to place their trust in organisations and, indeed, trust one another in order to meet their everyday needs. For instance, when paying their bills online, people regard organisations such as the city council and electricity companies as trustworthy and reputable. Therefore, a strong association exists between trust and reputation. Mainly, trust stems from implicit and explicit trust of social networks. Direct trust statement to the users refers to the explicit trust. However, the potential trust to users is called implicit trust. In a real social network, explicit trust is not reliable as some people might use false information, so explicit trust is not reliable in this situation (Carminati et al., 2013).

Similarly, it is necessary to trust nodes in MANET in order to complete transmissions, without any guarantee being provided. Many factors need to be taken into consideration when establishing trust between nodes in MANET. These include an assessment of their trustworthiness in relation to ability, integrity, and cooperation with others. Consequently, the reputation of every node is built using a behavioural assessment with other nodes. For instance, if the node drops packet multiple times, then the node will be suspected to be malicious by other nodes. Each node builds trust based on different trust values that are calculated by its immediate nodes opinion: all of which are temporal actions.

In the proposed method, the trust value of each node will be calculated based on the three stages of MrDR. In addition, trust in MANET is temporal and needs to be re-calculated continually for all nodes within the network. Trust in MrDR also cannot be transitive. For example, if node X trusts node Y, and node Y trusts node Z, it does not necessarily follow that node X trusts node Z. This could be regarded as the dynamic topology of nodes in MANET and their mobility. Moreover, the reputation of each node will be built based on a behavioural assessment. According to the dynamic topology of MANET, many factors are measured in each node in order to calculate the total trust status value. In this method, the trust value has only two values: 1= trusted or 0 = untrusted. Furthermore, a trusted node is reliable as it performs and accomplishes all missions such as packet forwarding and does not perform any malicious or selfish activities such as drop packet. In addition, the trust value for each node in this method is utilised in order to evaluate other nodes. Therefore, it helps to distinguish between trusted and misbehaving nodes, whether they are malicious or selfish that may lead to DoS attacks. Misbehaving nodes degrade the performance of the network considerably and can cause attacks such as DoS. Every node will evaluate and monitor other immediate nodes, as an agent. Thus, a centralised administrative concept will be applied in a decentralised environment, as is the case with a MANET. Due to the dynamic topology of MANET, there is a high likelihood that MANETs may merge. Cooperation between nodes is essential in order to improve the network performance. The trust value will identify misbehaving nodes and isolate them temporally from communications when the trust value equals zero or until the node becomes trusted. The mobility of nodes in MANET proves that the trust value of nodes cannot be stable. Additionally, the

default value of each node is trusted until the assessment and calculation of the trust value is complete.

A trusted node has accurate information about other nodes. On the other hand, an untrusted node contains false information about its immediate nodes. In the proposed method, every node could be described as an inspector that observes the behaviour of other nodes. This allows the network policies to independently reduce individual node's computational load. In addition, this method assumes that a promiscuous mode is used between nodes. Promiscuous modes are a security policy that enables nodes to listen to immediate nodes activities in order to monitor the entire network traffic (Perry et al., 2010). This means that every node monitors their neighbour's activities within the network with the purpose of monitoring the overall network's activities. Misbehaving nodes, which cause DoS attacks, are detected and isolated from communications temporally until their trust mode has been changed from 0 to 1. Nodes can be blacklisted for a specific time in order to rehab them and may only be used when they become trusted nodes. All nodes that misbehave maliciously or selfishly on three successive occasions will be sent to the blacklist for a temporal time period. This means that the calculation of the trust value will be longer, which will be explained later in this chapter, to save the network energy. As nodes in MANET can join or leave the network frequently, nodes cannot be considered permanently trusted or untrusted especially in MANET with its dynamic topology.

There are differences between malicious and selfish nodes. While both are misbehaving nodes, they differ in terms of their impact on performance and effects. Malicious nodes modify or drop a packet, as they do not transmit it to the intended destination. Therefore, this node drastically harms and degrades the network's performance. However, selfish nodes save battery power and do not transmit the packet to the intended destination. Hence, this node resembles a non-cooperative node, which does not harm the network directly compared to a malicious node. Malicious nodes cause damage and clearly lead to network outages due to their activities such as drop and modify packets.

5.2 MrDR design

The MrDR method has three main stages, which are used to calculate the total trust status value for each node. Its acronym is derived from these three stages: Monitoring; Detection; and Rehabilitation, as illustrated in Figure 5.1. It is paramount that these stages correlate in order to calculate the Total Trust Status Value (TTSV) for each of the nodes in the network. Obviously, the good or trusted nodes will withstand scrutiny as they will behave normally.

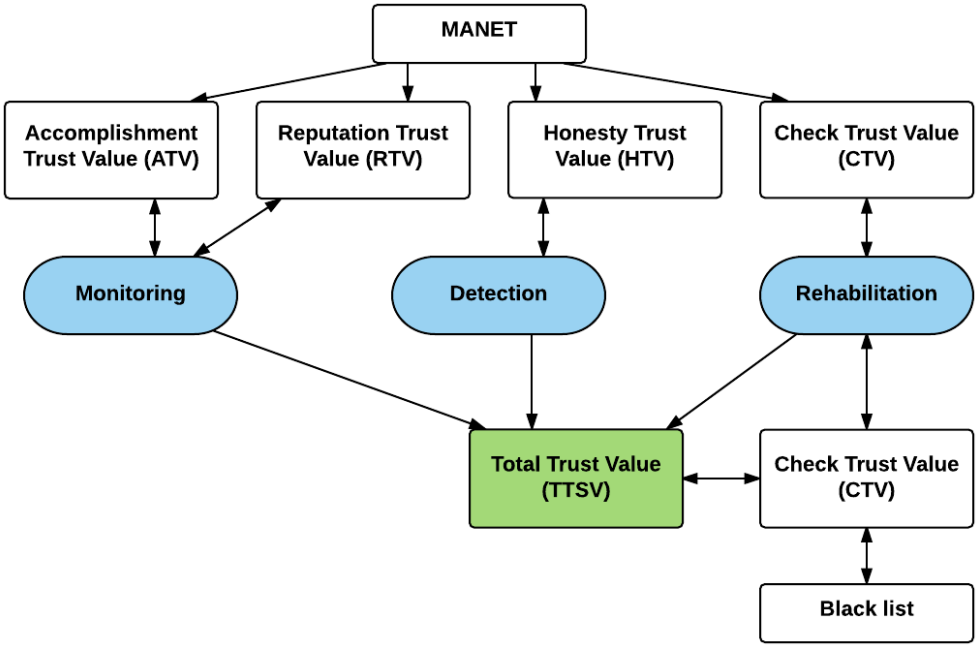

Figure 5.1. MrDR architecture.

5.3 MrDR stages

The three stages of the proposed method work collectively and interoperably, to measure the trust value for each node, whether trusted or untrusted. These stages will be explained in detail in the following subsection. It is important to mention that the first two stages are responsible to caculate the trust values, but rehabilitation is to caculate the trust values of nodes each specific time depends on the experiment duration.

5.3.1 Monitoring stage

The literal meaning of monitoring is noticing or even observing a particular object or person (Press, 2016c). In the proposed method, this stage involves monitoring the entire network by nodes within the network to detect any

misbehaving behaviours as early as possible. At this stage, two checks will be carried out and their values will be measured as follows.

5.3.1.1 Accomplishment Trust Value (ATV)

Accomplishment literally means the completion of an action or a mission. Trust between hosts in the network enables nodes to communicate with each other and enhance the network performance. For a more in-depth discussion about trust network see (Liu et al., 2012 ; Vasanth et al., 2014). However, in the context of the MrDR method, it indicates that a node has completed its assumed and expected tasks by sending data which is confirming that it has already received data from the node that sent it.

The ATV comprises two parts: ATV1 and ATV2. ATV1 determines whether the node sends the required packet to the intended destination or not. Figure 5.2 illustrates the ATV components. If the node sends the packet to the correct destination, then the ATV1=0.5; whereas if the node fails to send this packet, then the ATV1 = 0. In addition, if the node sends a confirmation message to indicate that it has already received the packet, then the ATV2 equals 0.5. However, if the node fails to send this confirmation message, then the ATV2 = 0. The overall ATV value may be calculated as follows:

$$ATV = ATV1 + ATV2 \qquad 5.1$$

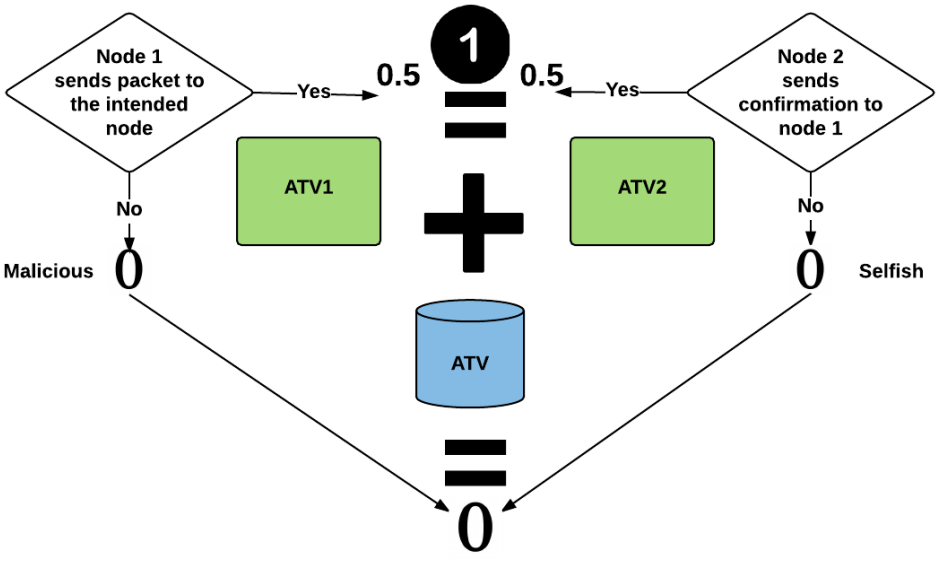

Figure 5.2. ATV components.

5.3.1.2 Reputation Trust Value (RTV)

Reputation may be defined as the views and opinions people hold in relation to a specific individual, organisation or even an object. In addition, reputation is connected to the node's identity. It is usually based on previous behaviour, word of mouth or personal experiences in particular situations (Press, 2016e).

In MrDR, it is assumed that the punishment resulting from packet dropping is less punitive than packet fabrication. This is because packet dropping does not always occur for misbehaving nodes, whether as a result of maliciousness or selfishness. It could be due to power failure or network congestion, broken links, corruption of the medium, or lack of power resources which relate to the MANET environment. However, if the node drops packet sequentially then the node is obviously malicious. Equally important, a node has a good reputation if it does not modify, drop, or mis-route packets such as DoS attacks. As previously mentioned, due to the specific nature of MANET, the RTV value of the node when it drops the packet for the first time is 0.5. Furthermore, when the node subsequently undertakes this action for the second time, the RTV is equal to 0.25. Finally, when the node drops the packet for the third time, the RTV is equal to 0 and the node is deemed to be malicious. However, when the node misroutes or modifies packet, or launches a DoS attack, the RTV is directly equal to 0. Alternatively, when the node does not perform any of these misbehaving actions, the RTV is equal to 1. Figure 5.3 shows the RTV value decision-making process based on the behaviour of the node.

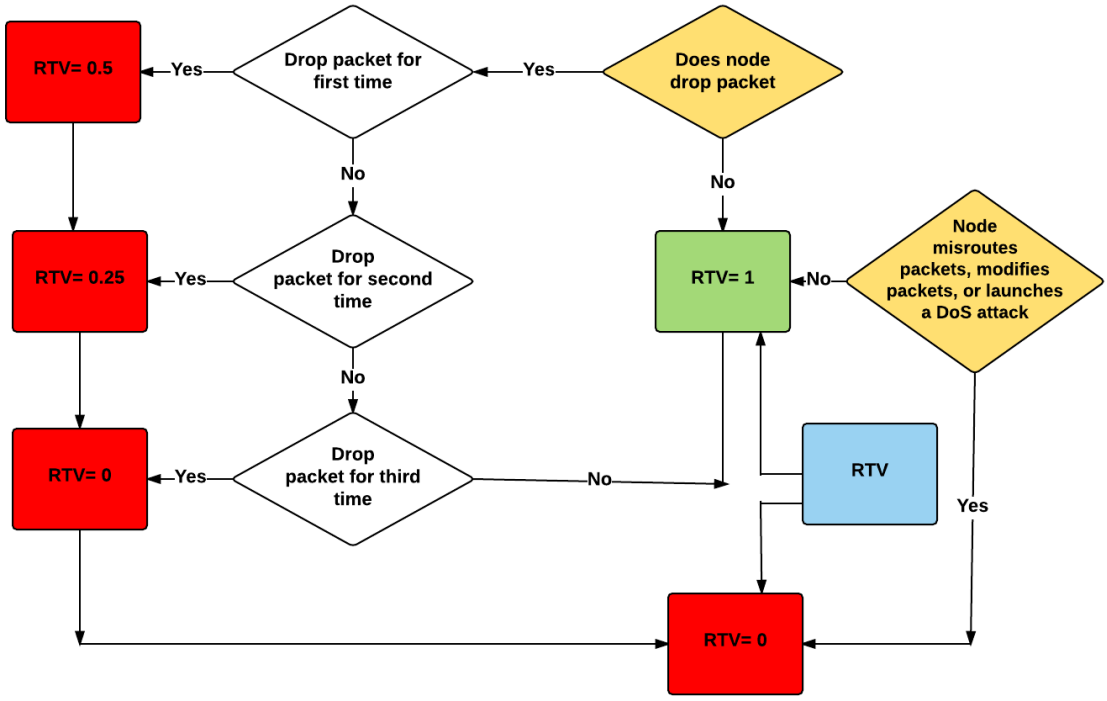

Figure 5.3. RTV calculations.

5.3.2 Detection stage

Detection literally means that someone or something has been discovered or observed (Press, 2016a). The objective of this stage is to detect misbehaving nodes, be they either malicious or selfish. The calculation of the Honesty Trust Value (HTV) at this stage is to assess the trustworthiness of each node within the network. In this situation, where the node exchanges accurate information about trust values and that information matches with information from the majority of the nodes, then the HTV is equal to 1. However, when the information is different or in conflict it means the information from this node has been modified, and the HTV is equal to 0. Figure 5.4 outlines the HTV calculation process for each node.

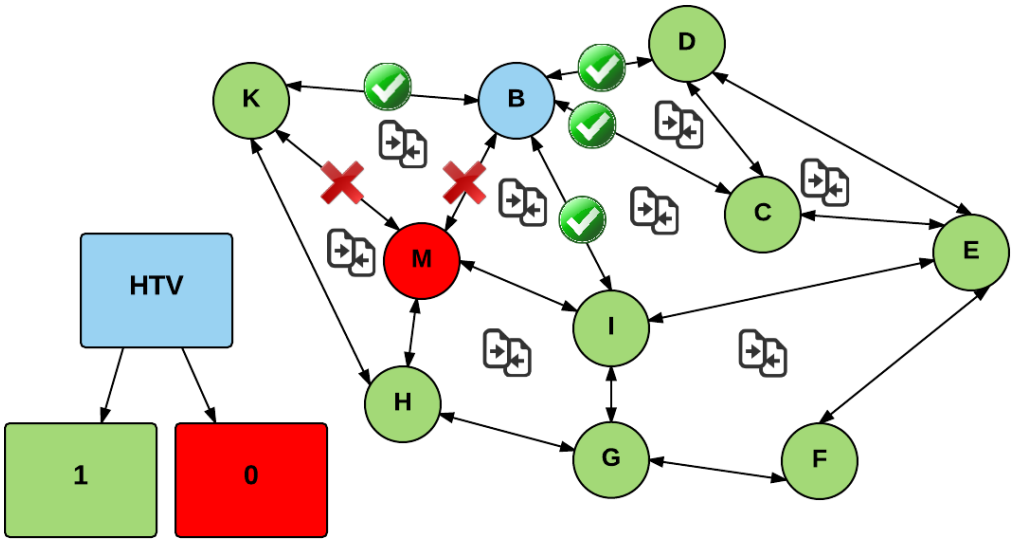

Figure 5.4. HTV calculation process.

Based on the data presented in Figure 5.4, it is apparent that node B attempts to check and compare how the information matches, as well as its symmetry to its immediate nodes such as K, M, I, C and D. It is assumed that node M is a malicious node and that it sends false information to node B. Thus, node B compares the information which originates from node M with information sent from other immediate nodes such as K, I, C and D. Accordingly, if node B considers that node M provides incorrect information, then its HTV is equal to 0, whereas the HTV values for nodes K, I, C and D are equal to 1.

Subsequently, from stages 1 and 2, the Total Trust Status Value (TTSV) is calculated as follows:

$$\boldsymbol{TTSV} = \begin{cases} \mathbf{0}, \boldsymbol{ATV} = \mathbf{0.5}\ \boldsymbol{or}\ \mathbf{0}\ , \boldsymbol{RTV} = \mathbf{0.5}\ \boldsymbol{or}\ \mathbf{0.25}\ \boldsymbol{or}\ \mathbf{0}\ , \boldsymbol{HTV} = \mathbf{0} \\ \mathbf{1}, \boldsymbol{ATV} = \mathbf{1}\ , \boldsymbol{RTV} = \mathbf{1}, \boldsymbol{HTV} = \mathbf{1} \end{cases} \qquad \mathbf{5.2}$$

TTSV is such a binary mode and has only two values: 1 is trusted and 0 is untrusted. A node can either be trusted or not in MANET. It is meaningless to provide a trust value to nodes that are partially trusted or suspicious as the node may eventually be untrusted and can rapidly degrade the network's performance. Untrusted nodes in MrDR will be isolated from the communications temporally until their trust values are altered from 0 to 1. In addition, calculating the TTSV, for each node within the network, will have to be conducted on every specific occasion, as the

number of times required to calculate the trust value for each node depends on the experiment's duration as shown below in Equation 5.3 below.

$$\boldsymbol{CTV = \frac{ETT}{3}} \qquad \textbf{5.3}$$

These values are the optimal figures to reduce network load but any regular checking period may be applied. It is important to note that the Check Trust Value (CTV) indicates the number of times taken to calculate the TTSV for nodes, and where ETT means Equation Total Time. For example, if the ETT for an experiment is six, then:

$$\boldsymbol{CTV = \frac{6}{3} = 2}$$

For example, when the ETT is six minutes, every two minutes the nodes' TTSV will be checked for. In the next chapter, the detection of DoS attacks will be completed for both SM and MM and it will be explained how the trust values would be calculated in each experiment.

5.3.3 Rehabilitation (or resetting trust value)

The goal of this stage is to rehabilitate misbehaving nodes and to reuse them in future transmissions. Rehabilitation literally means the gradual process of returning to a good condition, status or way of living (Press, 2016d). Due to the nature of MANET, nodes cannot hold the same status for an indefinite period of time, thus the status of all nodes is considered to be temporary. In empirical terms, for instance, a thief is a criminal, but he or she does not continuously carry out criminal activities. Criminal behaviour only occurs at specific times and, in some instances, the thief stops or repents at a later date. This analogy can be used to reflect the status of nodes, which cannot always remain stable. Hence, regular checks will be conducted on all trust values at specific periods of time and for every node in the network based on Equation 5.3. This is considered such as a resetting of trust value every specific time more than a stage. Rehabilitation is repeated a number of times (n), depending on the rate at which the nodes misbehave. For example, if node A is considered to be malicious on three successive occasions, then the rehabilitation time will be longer based on Equation 5.4 below:

$$CTV = \frac{ETT}{2} \qquad 5.4$$

For example, if node A is malicious on three successive occasions, then the node's rehabilitation will be longer in order to reduce energy consumption. Thus, if the total time of the experiment is six minutes, then the TTSV of that node will be checked, by its immediate nodes, every three rather than every two minutes. The next subsection will illustrate that every node calculates these trust values, as shown in Table 5.1, through its immediate nodes. However, this only exchange only occurs between immediate nodes (see Table 5.2). Hence, it would reduce the nodes' energy, if it is definitely malicious.

5.4 An example of how the MrDR method performs

As below indicated in Figure 5.5, node A monitors its immediate neighbours (D, E, F, G, B, and H) and acts as an inspector that assesses them based on specific observations in order to calculate the trust value of each node. Table 5.1 demonstrates the information that node A collects from these observations and on which the calculations are based.

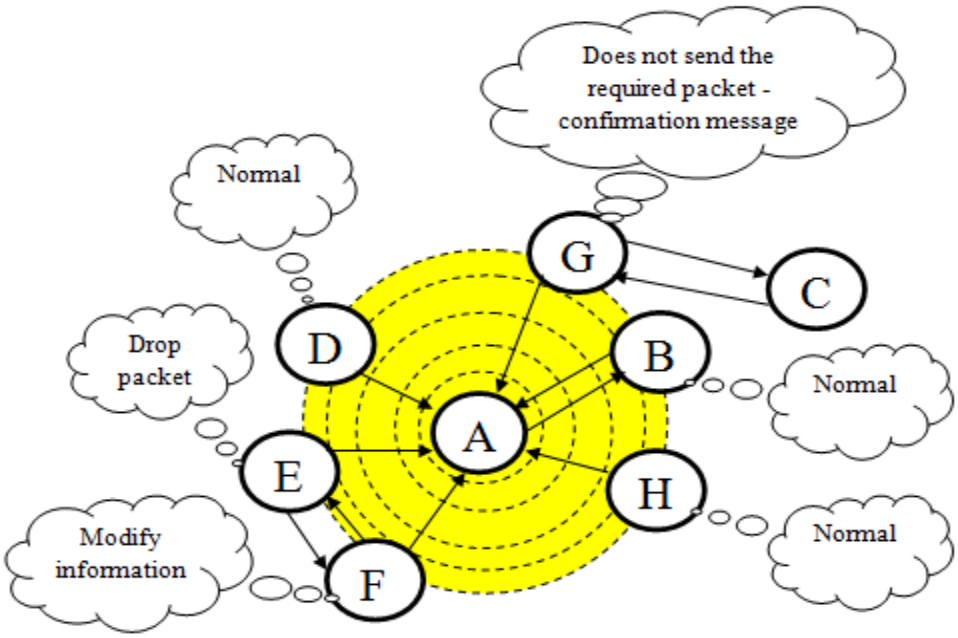

Figure 5.5. The observation of other nodes.

Table 5.1. All trust information in each node.

Node	ATV		RTV	HTV	TTSV	Node type
	ATV1	ATV2				
D	0.5	0.5	1	1	1	N
E	0.5	0.5	0	1	0	*
F	0.5	0.5	1	0	0	M
G	0.5	0	1	1	0	S
B	0.5	0.5	1	1	1	N
H	0.5	0.5	1	1	1	N

As shown in Table 5.1 above, N means normal, and * depends on the number of times that the RTV is given. The latter means that the RTV, as illustrated, cannot be 0 at all times for maliciousness or selfishness to occur. Due to the nature of MANET, the RTV can equal 0 as the packet drop might deem that the route has broken or that the destination node has left the entire network. Thus, when the RTV equals 0 on three successive time periods then it will undoubtedly be considered to be a malicious node. In addition, M indicates that a node is malicious, while S signifies it is selfish. To decrease the network overhead and message redundancy node A exchanges two types of information: TTSV and node type with all its immediate nodes. This is appropriate and efficient for power and resources which are constrained in networks such as MANETs. Details of the information exchanged between immediate nodes are shown in Table 5.2.

Table 5.2. Information exchange between the nodes.

Node	TTSV	Number of packet drops (RTS)	Node type
D	1		N
E	0	First time	*
F	0		M
G	0		S
B	1		N
H	1		N

As outlined in Table 5.2 above, node D is normal, and therefore its TTSV is equal to 1 and it is a trusted node. However, node E is untrusted, and the RTV value needs to be checked again as it might equal 0 due to normal issues in MANET such as packet dropping and routing issues. In addition, node F is a malicious node and it is untrusted, thus its TTSV is equal to 0. Node G is a selfish node as its ATV2 is equal to 0, therefore its TTSV is indeed equivalent to 0. Nodes B and H are trusted nodes and their TTSVs are equal to 1. This assessment is carried out on every node in the network to prevent misbehaving nodes from launching DoS attacks, which could degrade the network performance collectively. Moreover, this method gives natural traceability, which derives from the occurrence of any differences in exchange information amongst nodes.

Nodes in MANET are not stable and move frequently, thus TTSV is calculated based on Equation 5.2, while Equation 5.4 depends on trust values. Similarly, rehabilitation is also important in terms of trust status, as changes can emerge due to the dynamic topology of MANET. Rehabilitation encourages misbehaving nodes to cooperate in future transmissions and does not isolate them permanently from communications. This essentially improves the network's performance significantly as additional trusted nodes cooperate. Figure 5.6 illustrates the MrDR procedure to calculate TTSV for each node within the network.

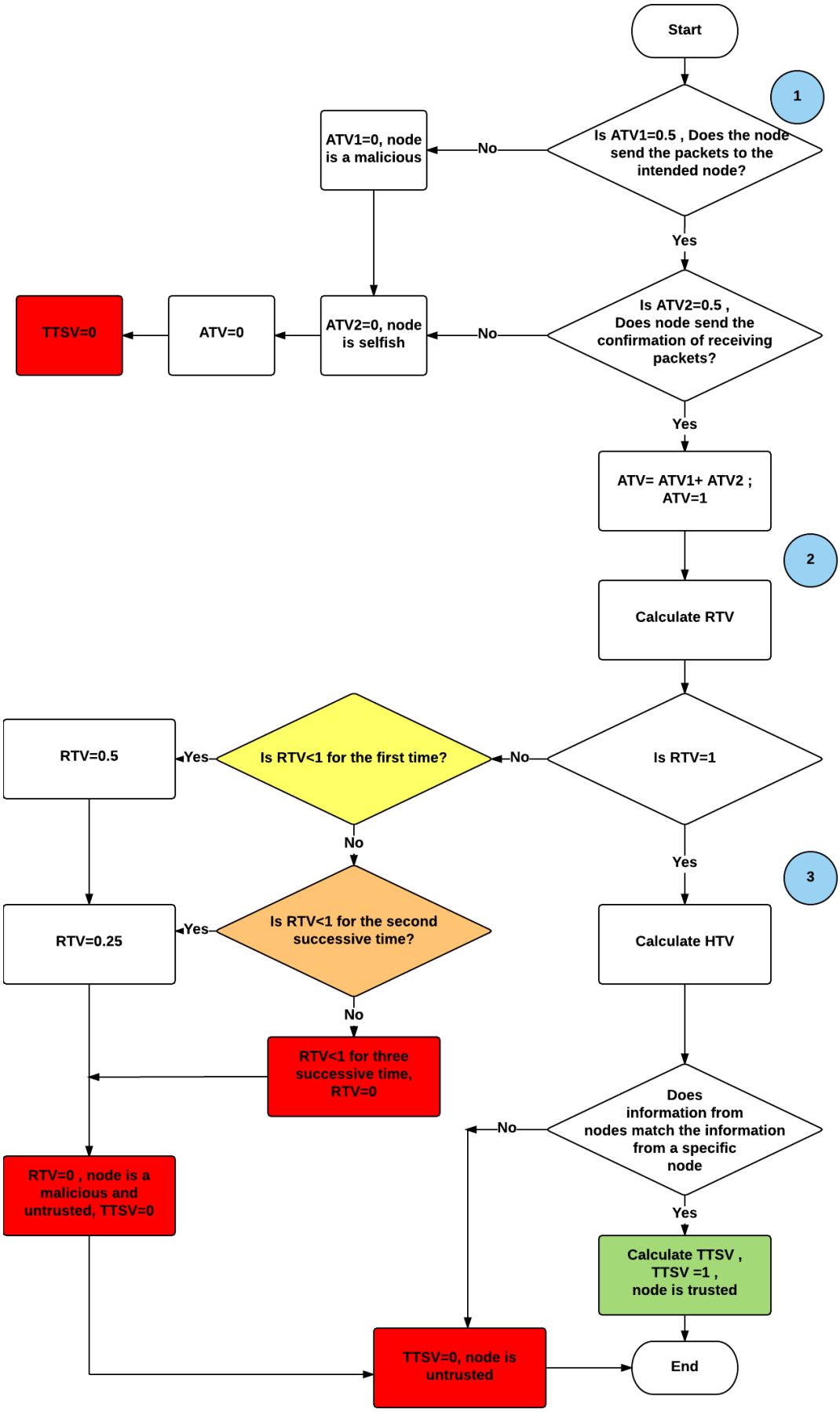

Figure 5.6. MrDR procedure to calculate TTSV.

5.5 Using the MrDR method on Multiple MANETs (MM)

MANET, with its dynamic topology, non-fixed infrastructure and volatile nodes connected via a wireless communication encourages changes as nodes can frequently join and leave. Thus, the topology of the network can change, and there is a possibility that MANETs can both merge and partition. The existing studies as seen in Chapter 4, focus on handling IP address in the merging process and do not discuss specifically the security concerns in the precise issue of detecting DoS attacks. The proposed method in the first study considered the security aspect when MANETs merge. It is essential to detect attacks every time, for example, in the merging process. It should be noted that the proposed method is the first study to address the detection of DoS attacks when two or more MANETs merge.

In the context of MM mergers, many issues need to be considered in relation to the IP address. These include: the assignment of an IP addresses to the node of the MANET that joins the network; the avoidance of IP address conflict; and reclamation of the IP address when the node leaves the network. It is important to mention that IPv4 is considered in this thesis.

5.5.1 Requirements of the IP address auto-configuration system

Some requirements must be met when assigning an IP address in MANET. First, no conflict should arise in the IP address between nodes. If two nodes within the network have duplicate addresses, this could cause the malfunctioning of the network. Second, when a node leaves the network gracefully or abruptly, its IP address can be reused by another new node. Leaving abruptly leads to IP address leakage (because there are some IP addresses that are neither assigned to any node, nor available for assignment). Third, all nodes in the network must be reachable at all times as they must update their vacant IP addresses and help to allocate an IP address to the new host. Finally, it is assumed that nodes in MANETs are configured *a priori*, before they become part of the network.

5.5.2 Proposed IP auto-configuration system to a new node

In the previous chapter, the existing method for assigning IP addresses in the network are illustrated with their advantages and limitations. In general, this process

does not guarantee the uniqueness. Additionally, energy consumption is the greatest drawbacks of this method (Hsu and Tseng, 2005 ; Al-Mistarihi et al., 2011 ; Zhou et al., 2010). However, the existing examinations do not meet the project requirements, so a new method for assigning the IP address is proposed in this section.

The proposed method for assigning IP address helps nodes within the network to cooperate and assign IP address for new nodes or for any node that needs an IP address in specific situations such as MANETs merges. According to Figure 5.7, the following steps will need to be carried out in order to assign an IP address to the new node:

1. Node F is a new node which attempts to join the network.
2. Node F broadcasts Request IP Address (REQIP) to all its immediate nodes or one-hop nodes (A, B, C) (see 1 in Figure 5.7).
3. The three nodes A, B and C receive this request. If any of these nodes have a vacant IP address, it will send a Reply IP Table (REPT) which contains just one vacant IP address. While some nodes may have more than one vacant IP address, only one will be sent.

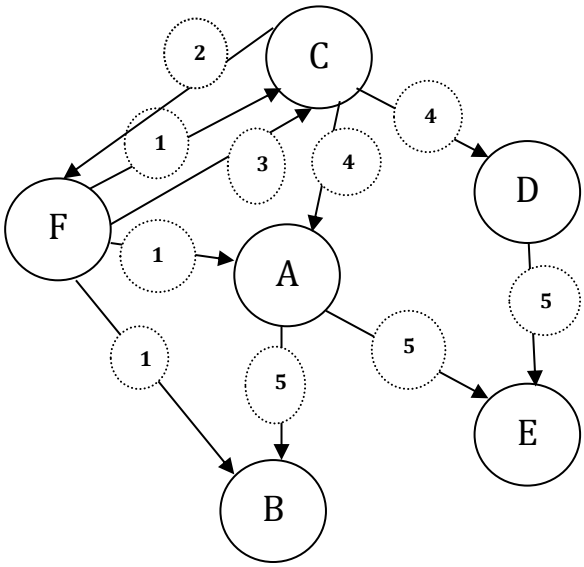

Figure 5.7. IP address configuration.

4. The REPT is sent as a table, as shown in Table 5.3.

Table 5.3. Information included in the REPT.

Node name	Vacant IP addresses
C	196.168.1.2

5. The first node that sends a reply is considered and the others are discarded.

6. It is assumed that node C is the first node to reply with a vacant IP address to node F (see 2 in Figure 5.7).

7. Node F allocates the IP address and broadcasts confirmation of the allocation to node C (see 3 in Figure 5.7).

8. Node C broadcasts this allocation to all its immediate nodes A and D (see 4 in Figure 5.7). They also broadcast this to their immediate nodes (see 5 in Figure 5.7) and so on, in order to update their vacant IP address lists.

9. In the case where, at the beginning of this process node F sends the REQIP and does not receive any reply, there are two possible derivations:

    1. Nodes C, A and B do not have any vacant IP addresses. Subsequently, node F has a timer set at approximately 20 seconds. If the timer expires, then this process will be repeated once. If there is still no reply, then nodes C, A and B will broadcast this request to all their immediate nodes, namely D and E. This would be until the reply message arrives from a node that has a vacant IP address with the time interval.

    2. Where nodes C, A and B are no longer connected to this network, after the timer expires, this process is also repeated once. If there is still no answer, the process is repeated for the last time (timer = 20 sec). If at this stage there is no reply, then that means that nodes have departed from the network. Node F updates its routing table and broadcasts the request to its new immediate nodes.

In addition, when a node departs from the network, the IP address reclamation is applied. In a graceful manner, prior to its departure, the host that is leaving needs to broadcast its IP address and leaving notification to its immediate nodes so that they can update their vacant IP addresses. Conversely, in a graceless manner, the immediate nodes will discover that they have not received any reply

from the leaving node, and this IP address will then be added to their vacant IP address lists.

It is important to mention that in the situation where no nodes has a vacant IP address in the whole network, then one of the immediate nodes should produce a random IP address using (Indrasinghe et al., 2009) method.

5.6 Merging MM based on Merging Using MrDR (MUMrDR) (Centralised trust)

It could be that two MANETs might have the same ID. Figure 5.8 depicts where two standalone MANETs are about to merge. A standalone MANET is where that network is not connected to any other, which includes any external network, such as the Internet. In Chapter 4, the literature that primarily focuses on auto-configuring IP addresses in situation such as merging and partition scenario are discussed. Nodes participate in this process regardless of if the nodes are trusted or not (Ghosh and Datta, 2011 ; Gammar et al., 2010). However, the proposed method specifically uses the centralised trust concept in order to reduce redundancy and consider security aspects, as one trusted node from each network helps to complete this process.

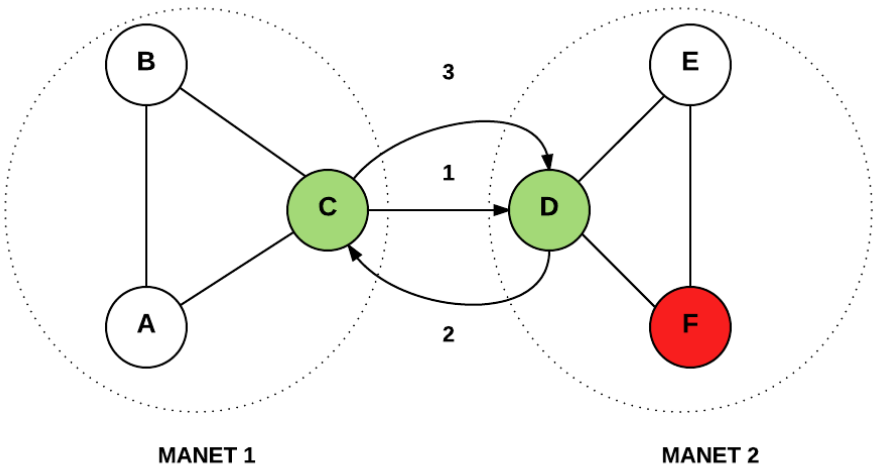

Figure 5.8. Procedure for merging two MANETs.

In Figure 5.8, nodes C and D are trusted nodes and are called connected nodes, as their main responsibility is to help the two MANETs to merge smoothly.

The type of connected nodes is selected prior to the merging since trusted nodes nominate a trusted node which has been given high votes by other nodes in each network. For example, MANET1 assumes that nodes A and B vote that node C is the most effective node to be a manager; therefore, node C will become a connected node in this network. Nodes C and D also have some checking responsibilities. First, there must not be any IP address conflict amongst nodes. Second, any either malicious or selfish nodes need to undergo a rehabilitation process. For example, in Figure 5.8, node F is an untrusted node, so it is now the responsibility of node C, which is considered to be a manager, to check the status of node F and apply rehabilitation to it. Third, managers C and D nodes have the responsibility to allocate the IP addresses to all nodes in their domain, should any IP conflict arise. In addition, managers are trusted, otherwise they cannot complete their duties to accomplish the merging process. Consequently, another trusted node will instead be nominated to complete the merging process. For instance, if node D is untrusted, node C will communicate with other nodes in MANET 2, such as node E. Finally, if the node leaves the network, then its IP address will be reused. Thus, the immediate node will maintain this vacant IP address until it is needed.

To begin the merging process, first node C sends a MREQ (Merge Request) to node D. Node D replies with a Merge Check 1 (MCHK1) to node C. This reply contains all the nodes in the current MANET, their IP addresses and their trust values, as shown in Table 5.4 below.

Table 5.4. Information included in the MCHK1.

MANET ID	Node name	IP address	Trust value
MAC address +timestamp (indicates the time of boot up) + number of nodes	D	192.168.1.2	1
MAC address +timestamp (indicates the time of boot up) + number of nodes	E	192.168.1.3	1
MAC address +timestamp (indicates the time of boot up) + number of nodes	F	192.168.2.1	0

Node C receives this information and passes it in a Merge Check 2 (MCHK2) to node D, as shown in Table 5.5.

Table 5.5. Information included in the MCHK2.

MANET ID	Node name	IP address	Trust value
MAC address +timestamp (indicates the time of boot up) + number of nodes	C	192.168.1.7	1
MAC address +timestamp (indicates the time of boot up) + number of nodes	A	192.168.1.1	1
MAC address +timestamp (indicates the time of boot up) + number of nodes	B	192.168.2.9	0

Nodes C and D check if their networks contain some misbehaving nodes, either malicious or selfish, and whether their trust values equal 0. Any misbehaving nodes found will be marked as suspicious. In addition, manager nodes check the IP addresses to establish if there are any conflicts, and if they arise, they resign the IP addresses.

In a situation where there is no IP conflict, then node C sends node D an Acceptance of merger (ACCM). Then node D replies to node C with a Confirmation of Merger (ConfM) and the two networks become one large network, as demonstrated in Figure 5.9.

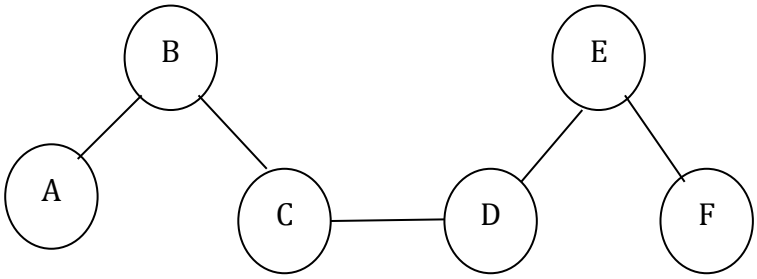

Figure 5.9. Node configuration following the merger.

If there is an IP conflict, then the IP address will be configured, as shown in Subsection 5.5.2.

A MANET ID is used to differentiate the nodes that belong to different networks. As the MANETs merge, their two IDs become one combined ID. The new identity of the merged MANETs is shown as follows:

$$\mathbf{MMID} = \boldsymbol{MANET\ ID\ 1} \cup \boldsymbol{MANET\ ID\ 2} \cup \boldsymbol{timestamp} \cup \boldsymbol{whole\ Nodes\ No} \qquad \mathbf{5.5}$$

As node F is a malicious node, it will need to be checked again for specific time interval, depending on the duration of the experiment and it is explained earlier in this chapter. If the status of it is still malicious, then it will be given another two chances (Rehabilitation). If the trust value of node F changes, then it will go from 0 to 1. Otherwise, it will be sent to the blacklist and isolated from the network for a longer time period as it is shown in Equation 5.4 until the node becomes trusted.

Merging using the MrDR method (MUMrDR) is employed in this situation to help the two MANETs to combine. In addition, one trusted node in each network helps to complete the process and to avoid any misbehaving activities.

5.7 Merging MM based on MUMrDR (Decentralised trust)

Based on the existing literature on Chapter 4 , there is no study uses the trust value to detect DoS attacks in MM merging. Therefore, this is the first study discusses this situation.

Figure 5.10 demonstrates that as the two MANETs are about to merge, a bridge will be built between each node to bring them closer to one another. The red lines above show the virtual format of that bridge. This bridge helps to exchange information from each node in MANET 1 to the corresponding node in MANET 2, which are the nearest nodes to one another. Each node will pass a table which includes: MANET ID, node name, IP address, node trust value, and the vacant IP addresses.

.

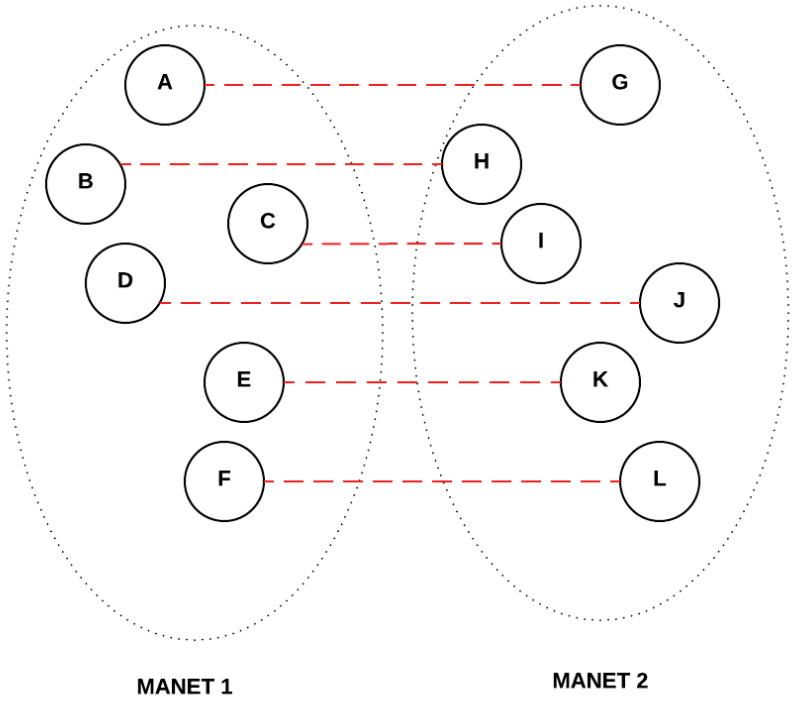

Figure 5.10. Two MANETs at the start of the merging process.

In the case where there are more nodes in MANET 1 than in MANET 2, two nodes from MANET 1 can communicate with a corresponding node in MANET 2. In Figure 5.11, node A will pass its table to node G in another network (see 1). Node G will check the table and compare the values with its immediate nodes (see 2). If the information is the same, then node A is trusted. Otherwise, the node is untrusted. The same process with be carried out with all other nodes, namely: B and H; C and I; D and J; E and K; and F and L.

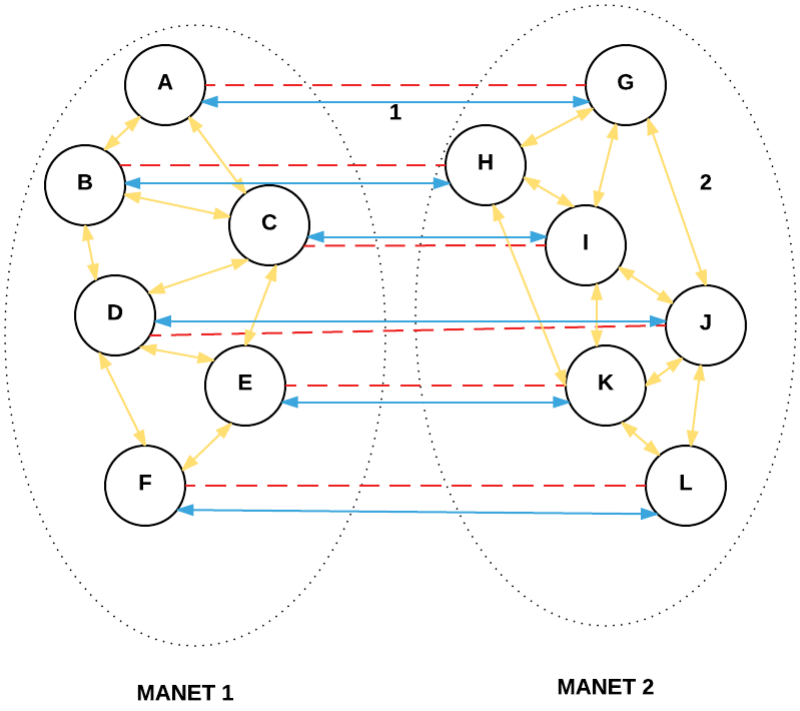

Figure 5.11. Negotiations between nodes.

During the negotiation process between nodes in both MANETs, any IP address conflict will be detected. For instance, if node H has the same IP address as node B, then an alarm message will be sent to both nodes via their immediate nodes. Therefore, the first node to receive a vacant IP address will change its IP to the new one. Assuming the nodes have negotiated, node B receives a vacant IP address from node D. When node B changes its IP address, it then informs node H of this via the IP change complete message. Then nodes B and H will send that information to all their immediate nodes. Figure 5.12 illustrates the process between nodes B and H. The red arrows show the alarm messages, which have been sent to both nodes B and H from their immediate nodes. The alarm indicates that there are IP conflict issues between nodes B and H. The yellow arrow from nodes B to H is to inform node H of the IP address change in node B. Therefore, node H does not need to change its IP address. The blue arrows show the announcement of the IP configuration of node B to all immediate nodes.

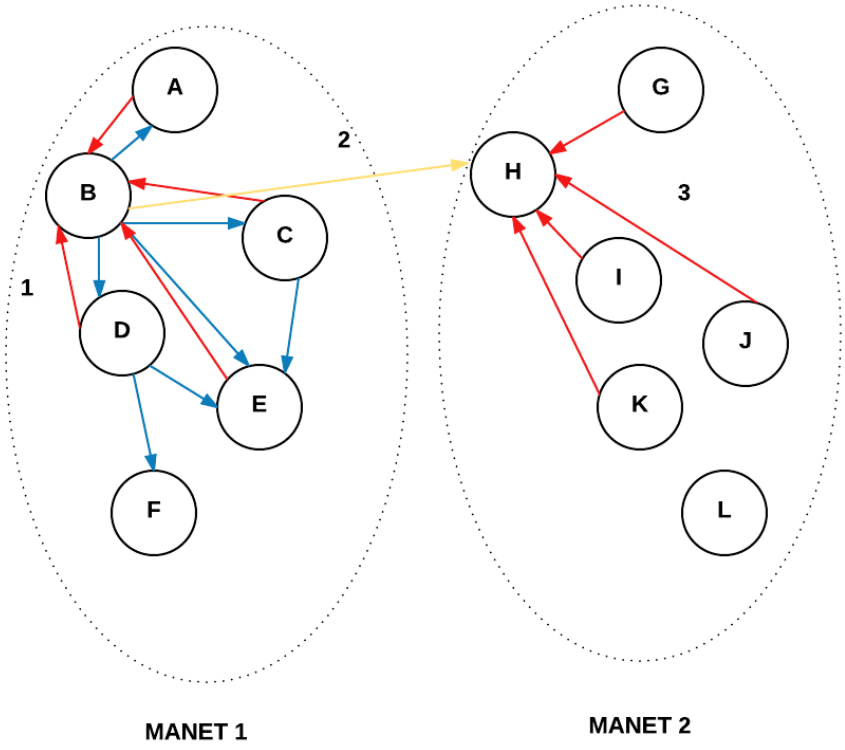

Figure 5.12. Negotiations between nodes.

No IP address conflict arises as the two MANETs merge together to become one large MANET. Moreover, the MANET ID is explained earlier in this chapter in section 5.6. In addition, Figure 5.13 shows the large MANET resulting from the merger of the two MANETs.

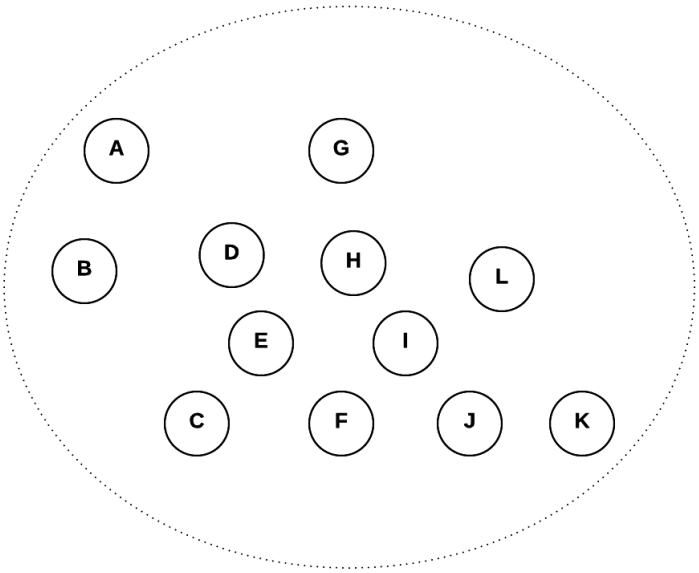

Figure 5.13. Large MANET following the merger of two MANETs.

However, if using either a centralised or decentralised trust concept to accomplish the merging process, both need to be managed, and that decision should be based on a number of criteria. The following section will explain this in detail.

5.8 Selection of a merging method (an identifier protocol)

Usually the larger MANET adopts the smaller one. The decision to use centralised or decentralised concepts when merging two MANETs is determined by different factors. There should be a concept identifier protocol in place to decide whether a centralised or decentralised concept is employed to accomplish the merging process. It is as follows:

1. If the number of nodes in MANET 1 is greater than 50 per cent of the number of nodes in MANET 2, then the centralised method is used.
2. If the number of nodes in both MANETs is equal or approximate then the decentralised concept is used.

This protocol is used to decide whether the centralised or decentralised method will be employed, based on the quality of the nodes in each MANET. The steps below explain how this protocol operates:

1. In Figure 5.14, nodes in MANET 1 have to nominate a trusted node. It has the responsibility for negotiating with another network. For instance, each node will send the trust value to its immediate node. Assuming that node C is trusted, it is nominated to negotiate with the second network.

2. The same process in the previous point will be repeated in MANET 2, where it is assumed that node D is nominated by the nodes in MANET 2.
3. Now nodes C and D will exchange their node numbers. Node C will send information that MANET 1 has seven nodes. Node D will respond by indicating that MANET 2 has three nodes. Nodes C and D will send a message to begin the centralised trust concept in order to complete the merger process.

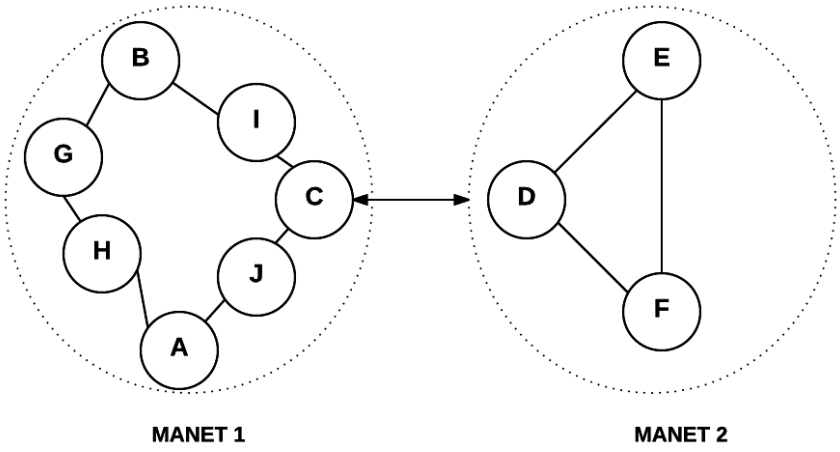

Figure 5.14. Negotiations between nodes in both MANETs.

This protocol helps to determine the concept used to merge, whether centralised or decentralised, depending on the node's numbers in both MANETs. In order to ensure that the merging process is applied successfully, the security aspect should be considered. This protocol will help to determine the optimal merging concept depends on the factors which are explained above.

5.9 Chapter summary

This chapter presents and explains a novel method (MrDR) to detect DoS attacks in both SM and MM. In SM, the proposed method detects these attacks based on the calculation of the trust values of each node. Three stages are applied in MrDR in order to calculate the TTSV of each node. A node can be either trusted (TTSV = 1) or untrusted (TTSV = 0). Rehabilitation encourages misbehaving nodes to be trusted in the future. If their TTSV changes from 0 to 1, then the node can communicate in transmission. Moreover, assigning an IP address to a new node

joining the network is discussed. In addition, as the topology changes in MANET, there is a likelihood that merging and partitioning can occur. MUMrDR is used to detect DoS attacks based on trust values in the case of merging MANETs. Two trust concepts are discussed, namely centralised and decentralised. A protocol is employed to decide which one should be used to successfully complete the merging process. Each independently configured MANET in a cluster can merge or partition. The selection of the merging type is dependent on the quality of each node. In the next chapter, three types of investigations will be undertaken. First, four experiments with different DoS attacks will be carried out to outline and evaluate the performance of the proposed method on SM. Second, the centralised trust concept and MUMrDR will be used to complete the merging process on MM (two independently configured MANETs). In this situation, one type of DoS attack will be detected in this experiment. Third, the decentralised trust concept and MUMrDR are used to detect different DoS attacks on MM (four independently configured MANETs).

Chapter 6: implemented a Simulation of MrDR method

This chapter deals with the implementation procedures to test and evaluate the proposed method in both SM and MM. Thus, the protocols and actions are transformed into procedures and events to express the scenario. Many programs and tools are used to simulate the network architecture and scenarios (Parker et al., 2010). In this research, Network Simulator (NS2) is used in this task, in order to simulate the method in different scenarios. In addition, MrDR will be applied in this chapter on three scenarios: SM; MM (two MANETs); and MM (Four MANETs). Different DoS attacks are detected using MrDR and the results are dependent on the attack type, as will be shown in Chapter seven.

6.1 Introduction to NS2

First, simulation refers to a real-world system which is imitated via computational re-enactment of its behaviours based on rules in a mathematical format. Simulation is used in order to allow safer and cheaper testing, optimise system performance, and evaluate the advantages and disadvantages of the method. Because the nature of computer communications and network models are complex, the development of special computer programs for a specific simulation issue is a possibility, but totally inefficient and time consuming. With the improvement in the application of modelling packages and simulations, they have become time-saving in the area of coding and more customary which enables programmers to focus on the modelling problem rather than the programming details. Many network simulators are available to use such as Cnet, OMNET++, NetSim, OPNET, QualNet, GloMoSim, NS2, and NS3 (Guizani et al., 2010). In this study, NS2 is used for two main reasons. First, the majority of studies online use this tool to simulate their protocols which demonstrates its good reputation in the research community. Second, much documentation is available online which alleviates the difficulty of the

learning process and coding. However, selection criteria for the network simulation includes many factors; for example, software license costs. NS2 is free and one of the most powerful tools which can be used in network research and development.

There are certain advantages of using NS2 to simulate networks and protocols. First, it is cost-free and does not require extra equipment. Usually it is run on a Linux platform or used with the Cygwin program on a Windows platform. Second, complicated scenarios can be simulated and tested easily. Third, it is a popular simulator as results can be obtained quickly and many ideas can be tested within a smaller timeframe. In addition, NS2 is considered as a standard experimental environment in research community. The use of the simulator provides an opportunity to investigate and understand the dynamics of networks. NS2 provides substantial support, in order to simulate many protocols, such as FTP, TCP, UDP, DSR, and HTTP. Besides, NS2 is used to simulate both wired and wireless networks. TCL is the main scripting language, which is Object-oriented support (otcl). NS2 uses two languages: TCL script and C++. The reason for using two languages is that TCL simulates some slightly varying parameters or configurations, such as quick explore of scenario numbers and iteration time (Quintero et al., 2013).

Furthermore, the simulator has various types of tasks to undertake. First, it needs a programming language to manipulate bytes efficiently or even packet headers which run over large data where the run-time speed is more essential and turn-around time is of low importance. Thus, C++ is fast to run but slow to change which makes it more suitable for detailed protocol implementation. Second, a great part of the network includes exploring a number of scenarios quickly as run-time speed has less importance. However, C++ simulates protocol requirements such as packet processing, algorithm implementation, run simulation, rerun, recompile, and run time speed (Issariyakul and Hossain, 2011). That OTcl runs more slowly but can be changed quickly makes it appropriate for system configuration (SHI et al., 2008).

6.2 Experiment design and simulation parameters

Design of experiments (DOE or DOX) or experimental design refers to the design of any task which aims to explain or describe the variation of information under specific conditions, and hypothesised to reflect the variation (Antony, 2014). In this section three main experiments will be conducted to test the proposed method on both SM and MM. The first experiment will test the proposed method on SM to

detect four types of DoS attacks separately: wormhole attacks; blackhole attacks; grayhole attacks; and jellyfish attacks. The reason for choosing these attacks is that they are the most popular DoS attacks which occur in the MANET environment, with the majority of studies raising the topic of their high occurrence (Jhaveri et al., 2012a ; Jain and Tokekar, 2011).

Some types of DoS attacks will not function successfully in MANET, such as Transfer Control Protocol Synchronize (TCP SYN) flood attacks. The reason behind this is that it is a multilayer attack that can occur in any layer. The attack exploits the TCP's three way handshake in the transport layer between client and server. However, the TCP SYN attack relies on multiple spoofed addresses to leave the TCP connections uncompleted; this is achieved through non-application of the third part of the handshake. These multiple spoofed addresses will be outside the network's normal IP addresses, so will be easily detected. Delays might occur due to this attack in MANET, which may slightly affect network performance (Geetha and Sreenath, 2015).

Besides, the second experiment will test the proposed method on MM when two MANETs merge and detect a grayhole attack. The concept of centralised trust will be used in this situation to help the MM to merge. For example, checking IP address conflicts and assigning IP address to any node which requires one. The reason for choosing this attack is that it is a challenge to detect it, as it does not behave maliciously all the time and can turn toward normality on occasion.

The third experiment will also test the proposed method on MM and in this situation on four MANETs. The four aforementioned attacks in experiment one will be used in this experiment. Further, the decentralised trust concept will be used to help these MANETs merge smoothly.

6.3 Test the proposed method against different DoS attacks on SM

Table 6.1 presents the simulation parameters that are used in the next four experiments, to detect different DoS attack scenarios, such as blackhole attack, wormhole attack, grayhole attack and jellyfish attack. Network Simulator (NS2.35) is utilised to run these experiments under LINUX (UBUNTU 12.04).

Table 6.1. Simulation parameters used in the experiments.

Simulation parameters	
Processor	Intel(R) Core (TM) Duo CPU P8700 @ 2.53GHz
RAM	4.00 GB
System type	64-bit
Operating system	UBUNTU 12.04
Routing protocol	AODV
Simulation time	6 min
No of nodes	71
Traffic type	CBR
Packet size	512 bytes
MAC type	Mac/802_11

Figure 6.1 shows the network architecture that is used to test the attacks. Moreover, every attack is applied as a separate experiment. The main architecture of the network for the four experiments is the same, as it includes 71 nodes, including one source node (node 8) and one destination node (node 7). In the future, the number of nodes could be incrementally increased and the network density considered. The timeline of the next four experiments is shown later in this chapter in Figure 6.3 which illustrates the experiments scenario and identifies the process of detecting the misbehaving nodes.

It is important to mention that the real-time schedule is used in the simulation which helps to synchronise the execution of events with real-time.

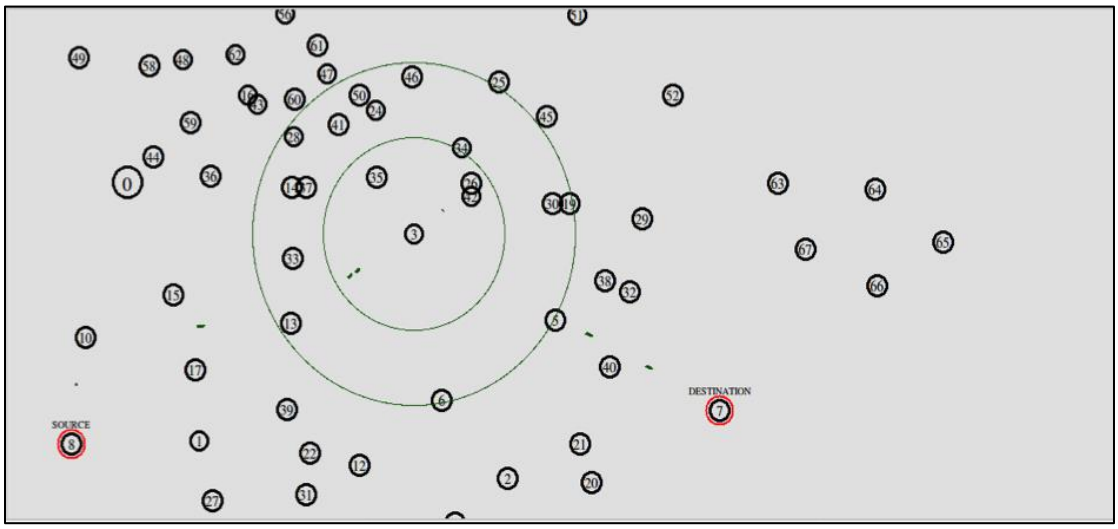

Figure 6.1. Network architecture for experiments.

The TTSV presented in Chapter 5 in Equation 5.2, will be calculated and checked in this experiment every two minutes, with the total period of each experiment set to approximately six minutes. The duration of the experiment could be longer but six minutes is used in these experiments to compare the performance of the network in the following scenarios: before the attack occurs; when the attack occurs; and after detecting the attack using the proposed method. In addition, the trust value will be tested three times in order to evaluate the effectiveness of the proposed method. Using the MrDR method, the network is able to update the TTSV of nodes and detect misbehaving activities as anomalies, such as occurring DoS attacks. Three factors are considered and measured in these experiments: network throughput; packet delivery ratio; and packet delay ratio. The comparison between these factors will evaluate the effectiveness of the proposed method in detecting DoS attacks.

Furthermore, the network overhead will be measured during a grayhole attack experiment. Overhead refers to any combination of extra or indirect computation time, bandwidth**,** memory, or other resources required to achieve a specific goal (Singh et al., 2015). This is important as it evaluates whether the proposed method would impact energy costs in relation to the power constraints of this network environment. As previously mentioned, the reason for choosing the grayhole attack is to test the impact on using the proposed method on the network overhead is that grayhole attacks are a challenge to detect as they can frequently turn between normality and maliciousness.

6.3.1 Attack scenarios

In this age of wireless devices, MANET has become an essential means by which to establish communication between nodes. However, security robustness is an essential service for both wired and wireless network communication. Due to the nature of the MANET environment, such as dynamic topology and the absence of a central administration point, it is prone to many attacks. In the first experiment, four DoS attacks are tested using the proposed method to detect them. This section gives an overview of attack scenarios and the design of each experiment to evaluate the proposed method on SM.

6.3.2 Wormhole attacks

In the case of a wormhole attack, the attacker receives the packet from one point in the network, which is referred to as the origin point, and tunnels itself to another point in the same network. This is referred to as the destination point. Subsequently, the attacker replies locally to the network from that point. The tunnel between the two attackers is a high-speed, off-channel link called the wormhole link that colludes to launch the attack in the network. After establishing the wormhole link, the attackers record the wireless data, overhear and forward them to each other. In addition, the adversary node replays the packet via the wormhole link at the other end of the network. Valid network messages are replayed at improper places. The wormhole attackers could make nodes that are far apart believe that they are really immediate neighbours, and force all communications between the affected nodes to go through them (Patel et al., 2015a).

Unfortunately, certain security mechanisms, such as encryption and authentication, are useless in preventing the latter mode of the wormhole attack. These security methods are applicable in the wired network. However, in the case of MANET, these methods are not applicable. Nodes in MANET perform basic network functions such as packet forwarding and routing. In addition, encryption and authentication increase the network overhead that is not appropriate in MANET with its constrained power. Applying security services in the MANET environment is challenging, as it is more vulnerable for eavesdropping and intrusion. Another mode of wormhole attack is the participation mode. The latter mode is more difficult than the hidden mode, owing to the fact it is harder to detect (Rajakumar et al., 2014). In the hidden mode, the intruder does not require cryptographic keys in order to launch

the wormhole attack. However, in participation mode the attacker launches a strong attack utilising valid cryptographic keys. Thus, the intruder does not make virtual links between the legitimate nodes. In fact, malicious nodes in this mode participate in the routing similar to legitimate nodes and use the wormhole tunnel to deliver the packets with a smaller number of hops. In the hidden mode, the intruder could drop data packet after inclusion in the route between the source node and the destination node (Nagrath and Gupta, 2011). Figure 6.2 shows the architecture of this attack. Two malicious nodes, X and Y launch wormhole attacks. These malicious nodes falsify the route length and encapsulate data packets. Assuming that node S wants to deliver packets to node D and initiates the route discovery process, node X receives the route discovery request from node S and encloses the route request, then tunnels it to node Y via route [X→F→E→C→Y].

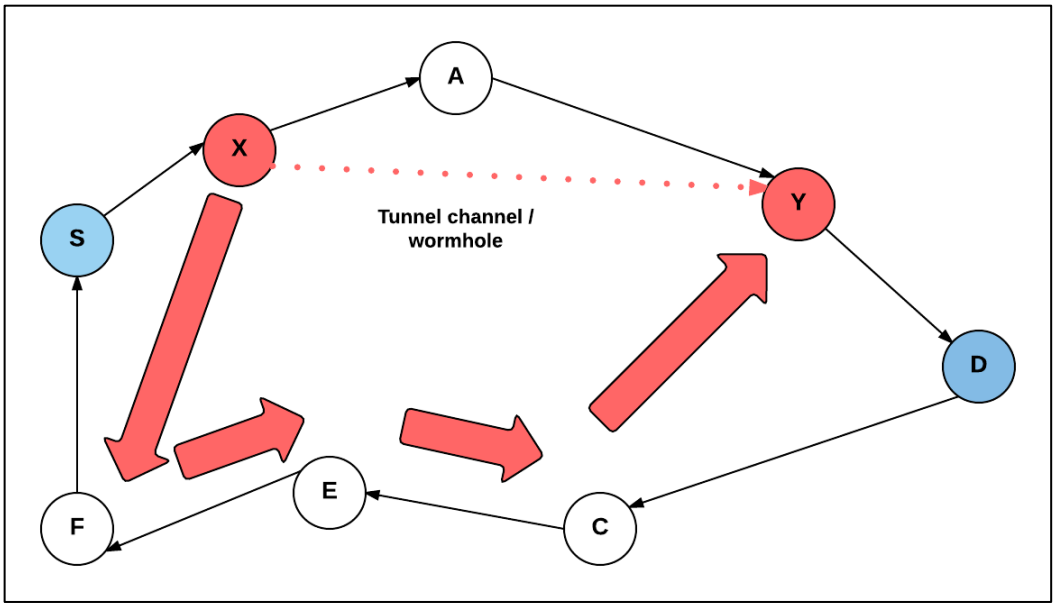

Figure 6.2. Wormhole attack architecture.

When the encapsulated route is received by node Y, which is requested for D, node Y will pretend that it had only one path of travel [S→X→>Y→D]. Besides, neither X nor Y update the packet header. Thus, node D finds two path routes from S of unequal lengths, as the first one is of four and the second one is of three. When node Y tunnels back the route to reply to node X, node S falsely considers the path to D through X is better than the another path to D via F. Subsequently, tunnelling prevents honest intermediate nodes from increasing the metric used to measure the existing path lengths correctly.

A wormhole attack is quite severe. An attack is possible even if the attacker has not disclosed any hosts, or even in a situation where all communications have been applied with confidentiality and authenticity (Hu et al., 2003). Geographical packet leashes, temporal packet leashes, directional antennas, neighbour node analysis and digital signatures are the most popular methods applied to detect wormhole attacks in MANET (Sorathiya and Rathod, 2015). In this chapter, the trust concept of MrDR method will be used to resist this versatile attack.

6.3.2.1 Experiment scenario

The total time length of all experiments is six minutes. At the beginning of minute two, or in other words the normal network mode, no wormhole attack occurs and the network is normal. Thus, the TTSV will be checked for each node to detect any malicious attacks and the network performance is measured. The timeline in Figure 6.3 shows the experiment scenario in terms of minutes to detect the DoS attacks used in this section on SM for each DoS attack.

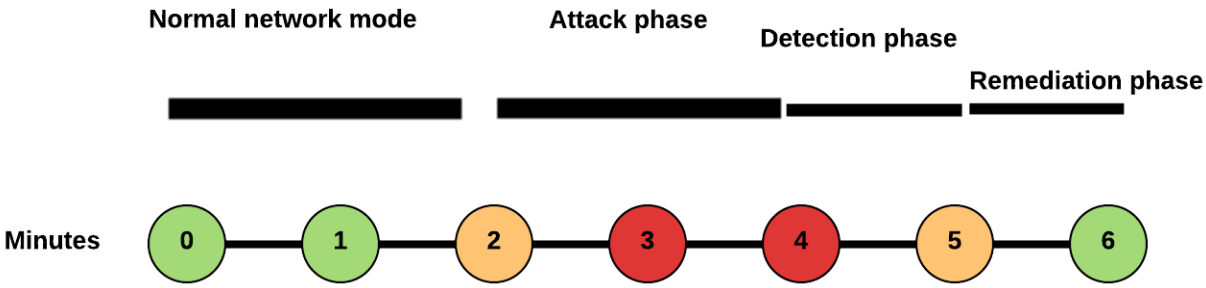

Figure 6.3. The timeline of the experiment scenario.

At the end of minute two, node 12 launches a wormhole attack. In addition, after ten seconds of the occurrence of the first wormhole node, node 16 also commences this attack. Moreover, nodes 18 and 25 follow the previous wormhole nodes and launch this attack in the beginning of minute 3, as it is shown in Figure 6.4.

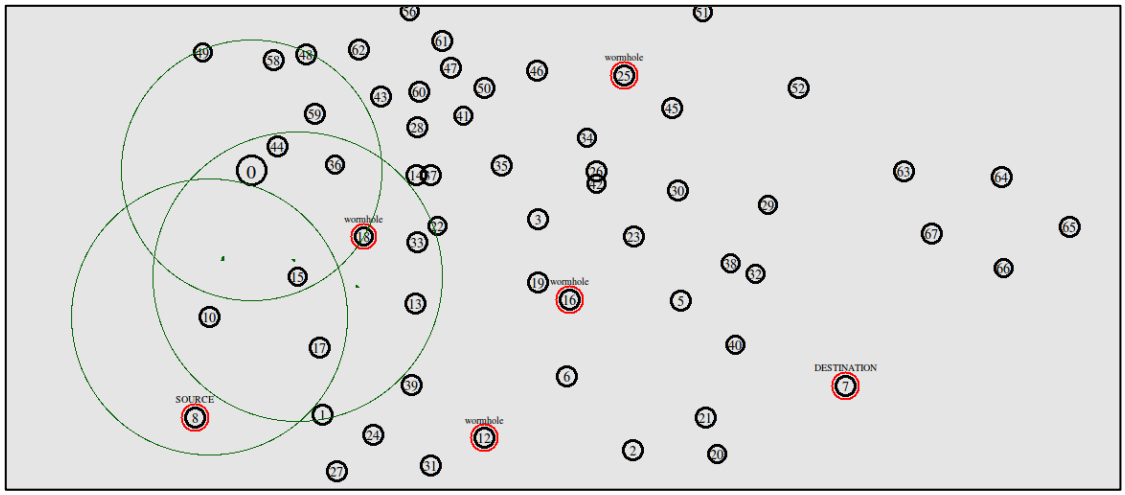

Figure 6.4. Network architecture after wormhole attack occurs in four nodes.

Figure 6.5 (A, B, C, and D) shows the gradual removal of the wormhole attacks from the communications within the network. At the beginning of minute four, node 18 is detected followed by node 16 approximately 10 seconds later. Furthermore, node 12 is detected followed by node 25. Thus, by the end of minute four, all wormhole nodes have been temporally isolated from communications.

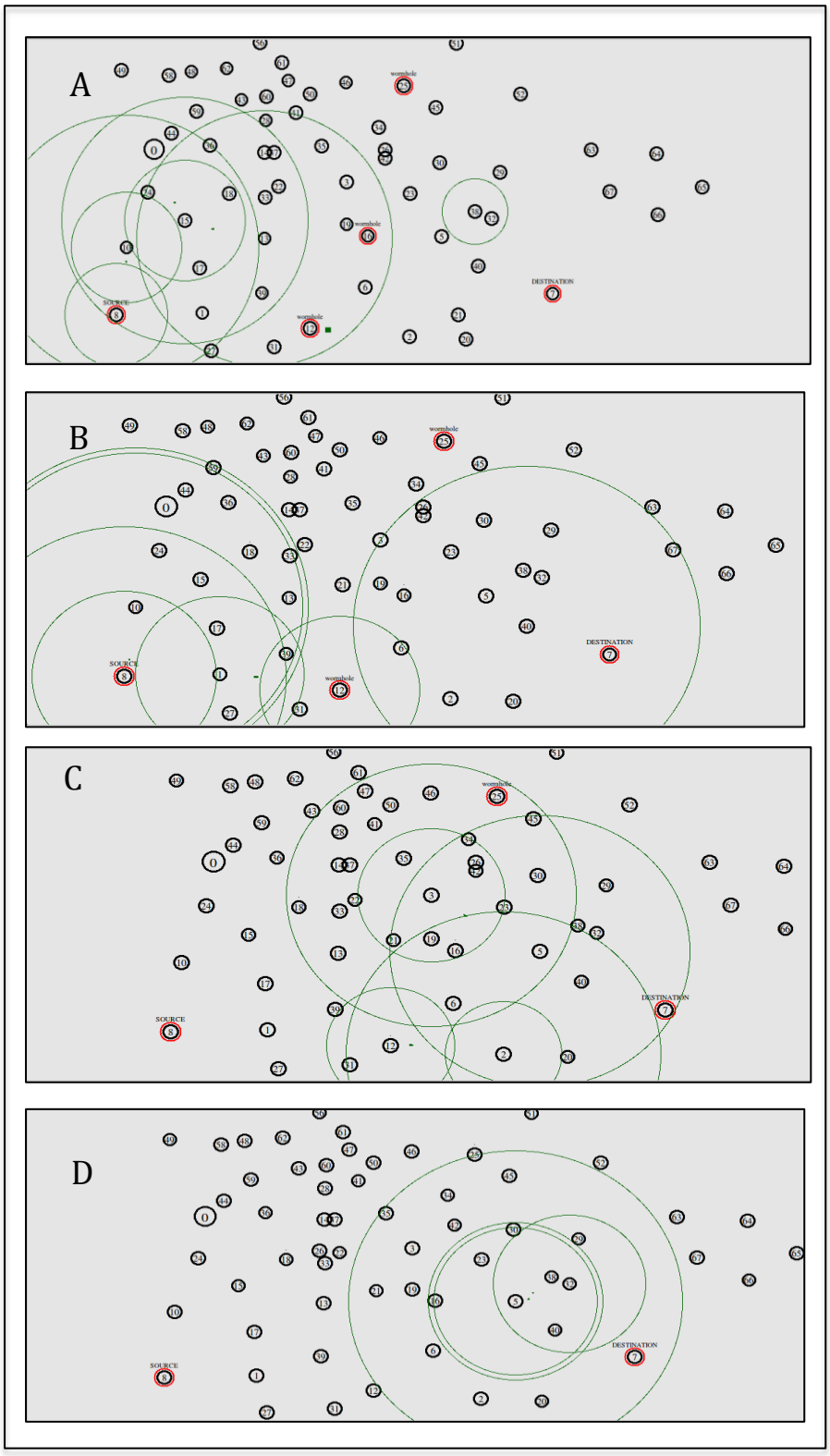

Figure 6.5. The gradual removing of the wormhole attacks.

In the remediation phase or rehabilitation, the proposed method ensures that only trusted nodes perform tasks and rehabilitate misbehaving nodes. Thus, if the misbehaving nodes become trusted, then they can participate in the network activities. However, if the TTSV for the node is equal to zero on three successive

occasions, it will be isolated from the network for longer. Thence, the calculation of the TTSV will be longer as is explained in Chapter 5 (Equation 5.4). Subsequently, this would save the network resources as MANET has constrained energy.

The algorithm to detect this attack is implemented using NS2. The pseudo code of the algorithm which gives a representation of the actual code to calculate the TTSV of nodes using tcl and cc files is shown in the Appendix A.

6.3.3 Blackhole attacks

This attack aims to detect the AODV protocol. AODV is a state-of-the-art routing protocol that follows a purely reactive strategy. It establishes a route on-demand at the start of a communication session and utilities it until it breaks, after which a new route setup is initiated. Specifically, AODV uses Route Request (RREQ) and Route Reply (RREP) control messages in its Route Discovery stage. It uses the Route Error (RERR) control message in the Route Maintenance stage. However, a blackhole attack exploits the AODV protocol to launch a DoS attack. Figure 6.6 represents the architecture of this attack (Pokhariyal and Kumar, 2014).

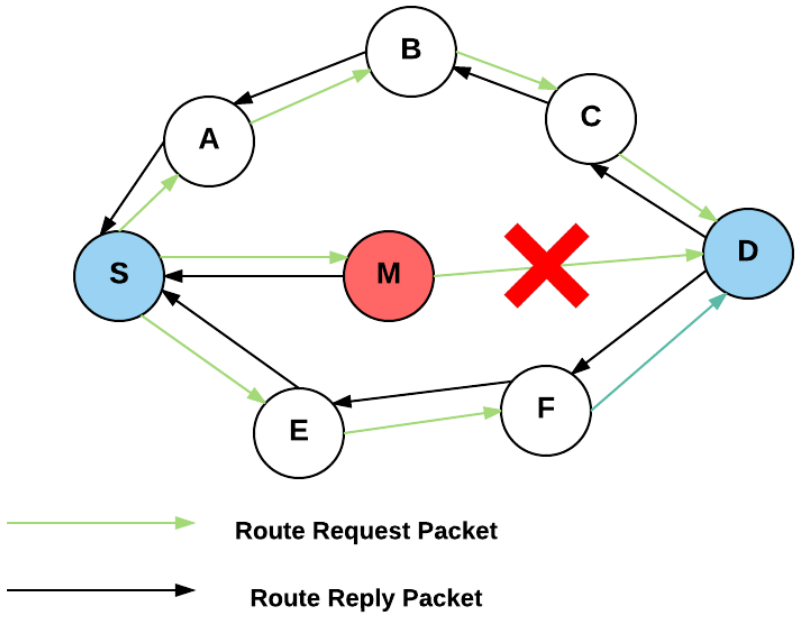

Figure 6.6. Blackhole attack architecture.

Assuming that node S wants to communicate with node D, node S launches or broadcasts route discovery request or RREQ to its neighbours. Any intermediate

node or the destination node D which has a fresh route will reply to node S with RREP. In a situation that has no intermediate nodes in the network, but has a fresh route to node D, they forward RREQ towards node D. Node M is a malicious node that does not forward RREQ forward. Instead, it replies falsely to node S, claiming it has a valid route to node D. Therefore, the RREP from node M arrives to node S faster than other neighbours of S. Thus, node S will send packet to node D via node M, as node M announced it has the shortest route to node D. Unfortunately, node M would now absorb drop all packets that are sent to node D from node S, and as a result, node D will receive nothing (Jhaveri et al., 2012b).

6.3.3.1 Experiment scenario

Based on the timeline in Figure 6.3, at the beginning of minute three or in the attack phase, blackhole nodes start to appear gradually, first node 16, then after five seconds, node 11. After ten more seconds, node 18 is also a blackhole node. Figure 6.7 shows the progressive occurrence of this blackhole attack in the network.

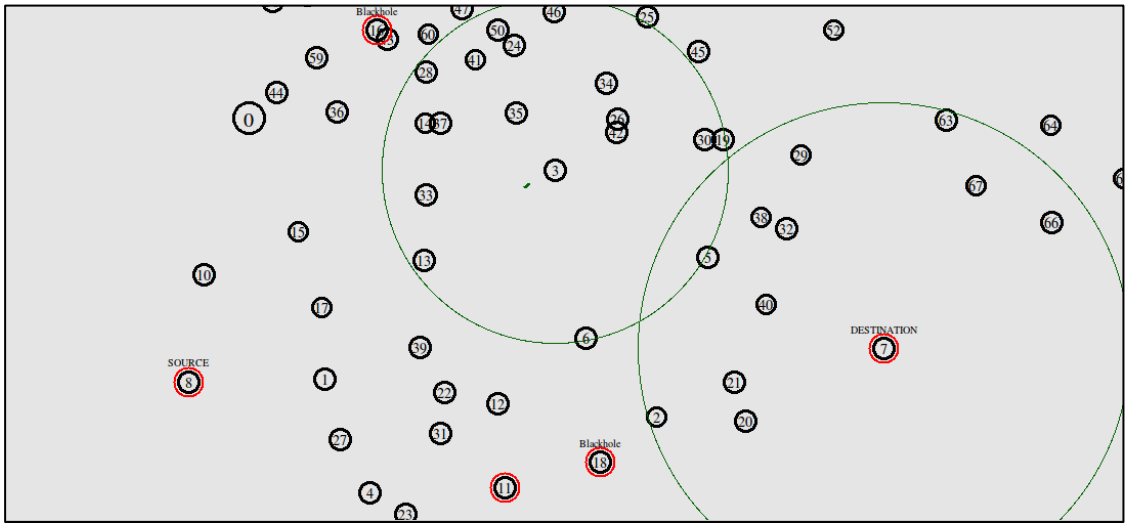

Figure 6.7. Blackhole attacks in the network.

Subsequently, at the end of minute four or in the detection phase, the MrDR method starts to detect a DoS attack, which is the blackhole type in this experiment. First, node 16 is detected, then after 10 seconds, node 18 is also detected. Furthermore, at the beginning of minute five, node 11 is also isolated from network transmission temporally. Figure 6.8 (A, B, and C) illustrates the gradual detection of blackhole nodes using the proposed method. Each misbehaving node that has a TTSV equal to 0 is untrusted and should be isolated from communications until its

TTSV is restored to 1 and it becomes a trusted node. First, node 16 which is untrusted is isolated from communication, followed by node 18 and node 11 respectively as they are also untrusted. Again, in the remediation phase it will be ensured that nodes are trusted in order to use them in future communications.

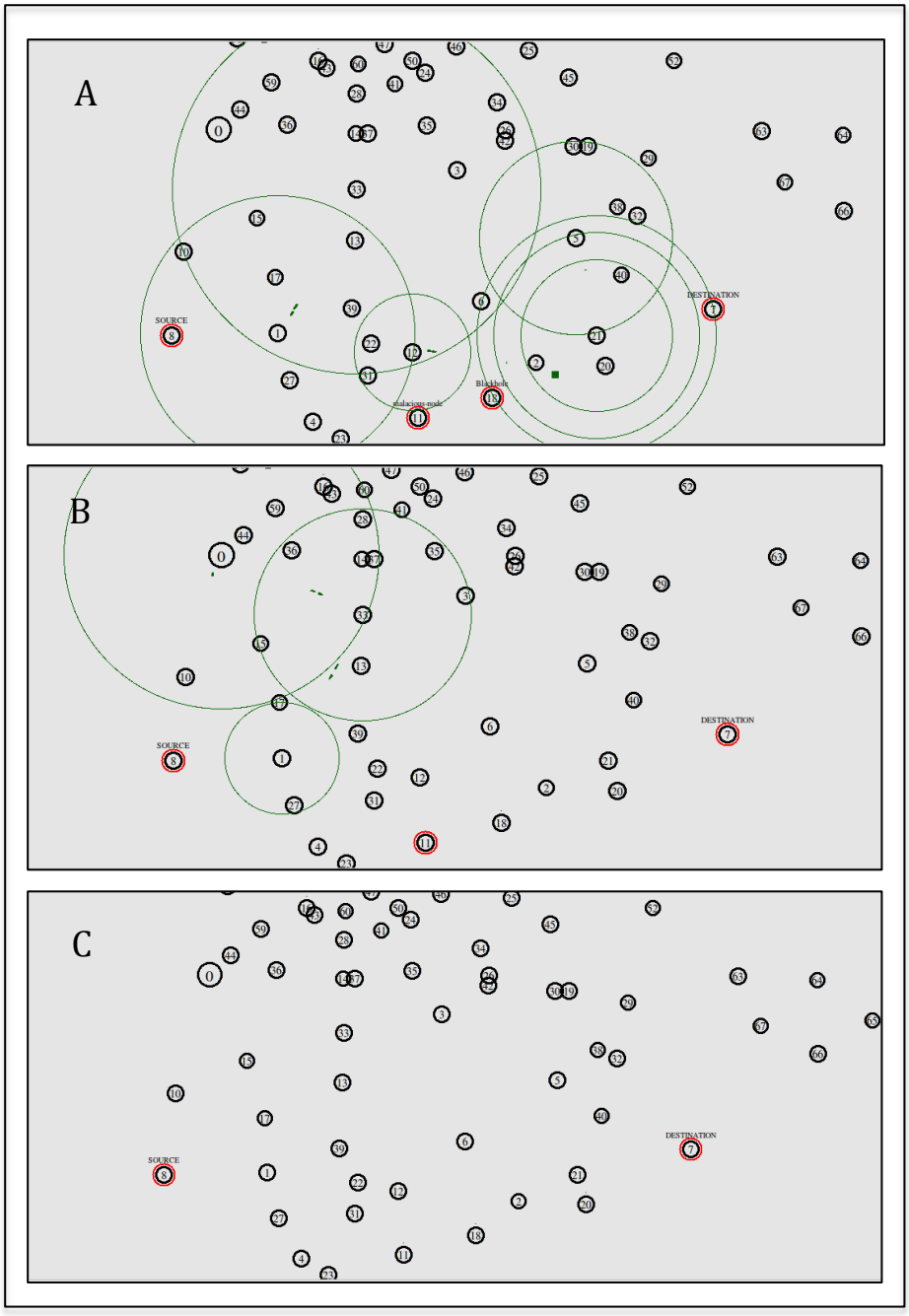

Figure 6.8. Detect blackhole attacks gradually.

6.3.4 Grayhole attacks

Grayhole attack is an extension of blackhole attacks as the misbehaving nodes are unpredictable. In addition, grayhole attacks disturb route discovery which

considerably degrades the network performance. At the beginning of the discovery process, the malicious nodes appear to be honest nodes. After a while, however, the malicious nodes start to drop some or all of the packets. However, a grayhole attack does forward nodes. Thus, grayhole attacks are more harmful than blackhole attacks. The latter drops packets certainly but the former may switch to normal status after dropping some packets. Thus, the detection of this type of attack is highly problematic because nodes intermittently switch their states from malicious to honest and vice versa (Kaur and Sidhu, 2014).

A grayhole attack drops and transmits packets selectively after advertising itself as owning the shortest path to the destination, as a response to a route request message from the source node. However, malicious nodes could perform numerous attacks by subverting the AODV protocol as it does not have any security mechanism. For instance, routing message integrity and data origin authentication at every receiving node are important. A compromised node might impersonate the sender of routing packets or even change the sequence number in RREQ /RREP messages. Further, routing information can be modified which leads to inconsistency in the network. Moreover, routing tables could contain incorrect information regarding the network topology. Therefore, changes in sequence number can result in routing loops. Figure 6.9 presents the architecture of the grayhole attack in MANET. In this figure, node M is a malicious node which behaves maliciously and drops packets which are sent from source node S to the destination node D. Sometimes, node M acts normally, so therefore behaves maliciously for a certain time period and then acts as a normal node for a specific time.

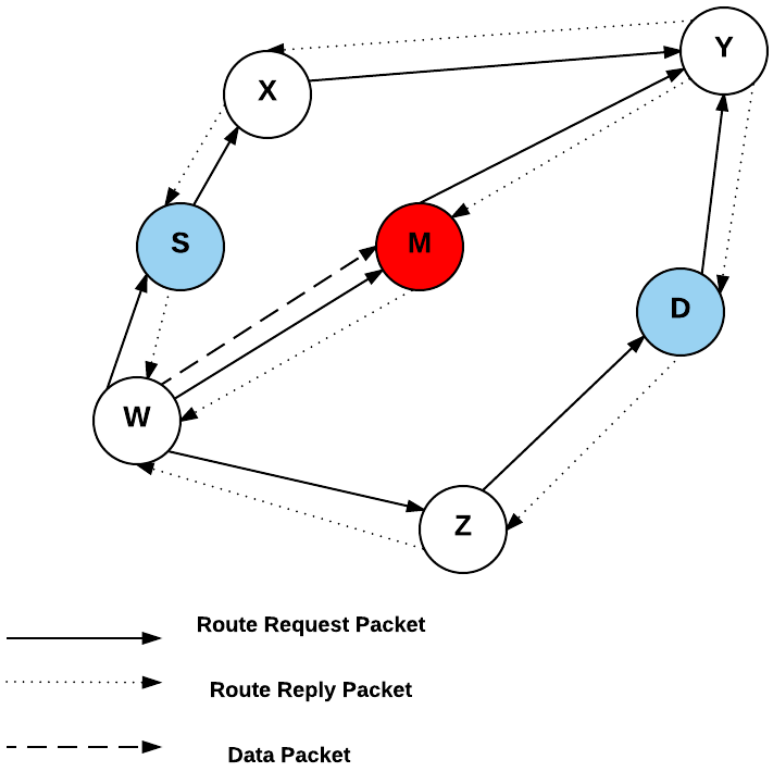

Figure 6.9. Grayhole attack topology.

Many approaches have been proposed to detect this attack, such as creating a proof algorithm, check-up algorithm and diagnosis algorithm. The main drawback of the latter approaches is that they could not detect all malicious nodes within the network, especially due to the sporadic malicious behaviour (Jhaveri et al., 2012a). In addition, trust-based approaches use passive acknowledgement such as Simple Trust AODV to detect malicious nodes (ST-AODV). This model enables AODV to cope with the existence of malicious nodes in the network (Jhumka et al., 2008). There are limitations to this work, as there is no packet authentication, so attacks can be launched easily by malicious nodes. In this experiment, MrDR method will be used to detect grayhole attacks in SM.

6.3.4.1 Experiment scenario

At the beginning of minute three or in the attack mode in Figure 6.3, grayhole nodes occur gradually. First, node 10 and node 18 are grayhole nodes, as illustrated in Figure 6.10 (A). After ten seconds, they are followed by node 16 and five seconds later, they are followed by node 25 as it is shown in Figure 6.10 (B).

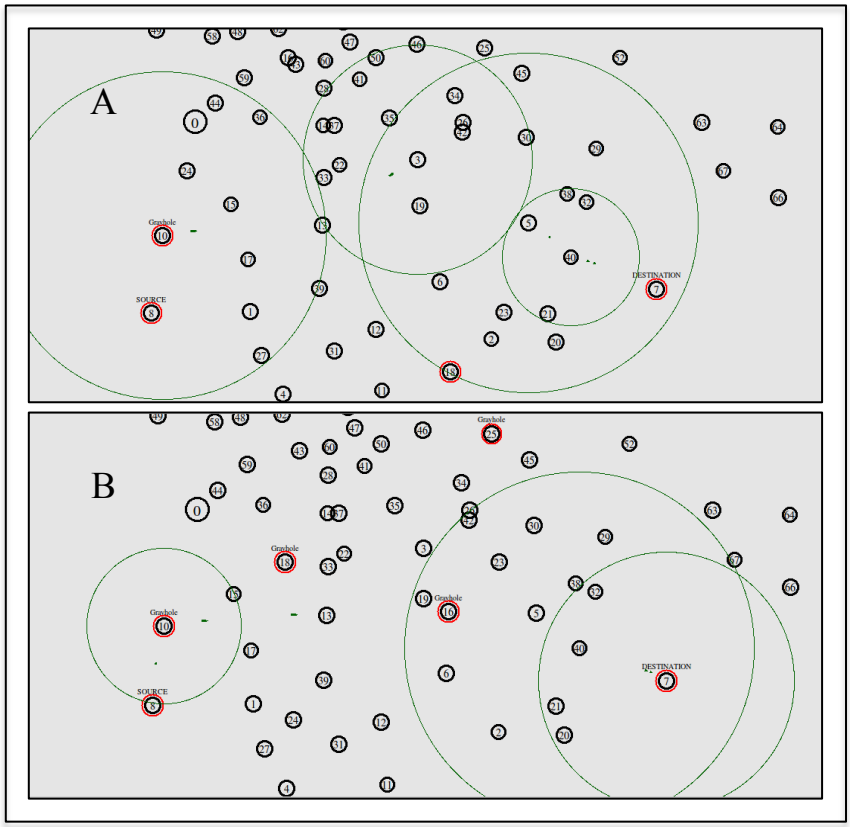

Figure 6.10. Grayhole attacks occur gradually.

At the end of minute four or the detection phase, grayhole attacks are detected progressively as node 10 and node 18 are isolated from the communications. At the beginning of minute five, node 16 and node 25 are also detected using MrDR method and isolated from transmissions, until their trust values change from 0 to 1. Figure 6.11(A and B) illustrates this detection. First, node 10 and node 18 are detected and isolation from communications followed by node 16 and node 25.

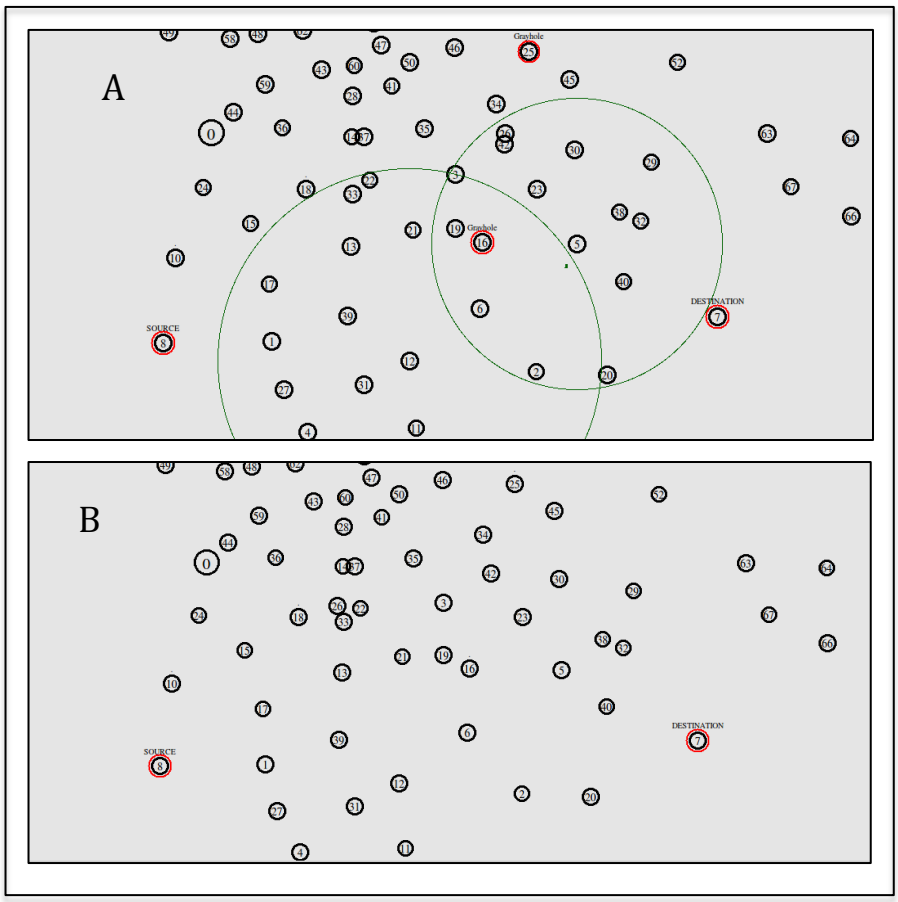

Figure 6.11. Grayhole attacks detection gradually.

6.3.5 Jellyfish attack

The jellyfish attack is one type of DoS attack that usually occurs at the transport layer of the MANET stack. During this attack, a malicious node can remain active in packet forwarding and even route discovering to inhibit it from diagnosis and detection. However, the malicious node may affect the traffic by itself via dropping packets periodically, reordering packets, or other such jitters. Thus, jellyfish attacks are considered harmful to TCP traffic as cooperative nodes can rarely differentiate the attack from the normal network congestion (Laxmi et al., 2014). Figure 6.12 illustrates the jellyfish attack architecture in the situation of a reorder buffer. Jellyfish node or node M records the buffer, as the packets are sent via the buffer (Laxmi et al., 2015). At the destination point, if the packets do not arrive in the actual order, then duplicate acknowledgement will be sent to the sender. At the sender side, when three duplicate acknowledgements are received, re-transmission of the packets begins without waiting for re-transmission timeout. In

addition, even when the packet reaches the destination, the sender still believes the packet to be lost and might re-transmit the packet (Kaur et al., 2015).

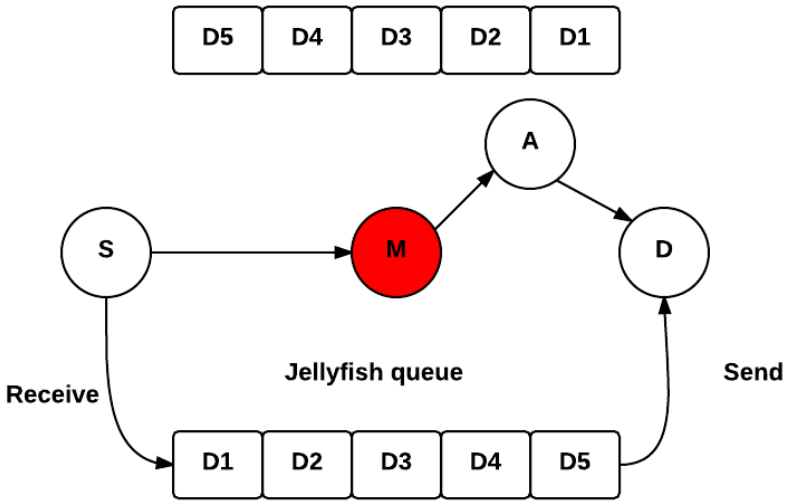

Figure 6.12. Jellyfish attack architecture.

6.3.5.1 *Experiment scenario*

According to Figure 6.3 at the beginning of the experiment, the network is in the normal network mode as no attack appears. At the beginning of minute three or the attack phase, jellyfish nodes start to launch an attack, with node 13, and then node 11. Approximately ten seconds later, node 15 launches an attack and is followed by node 20 after another 10 seconds. Figure 6.13(A and B) shows this sequence.

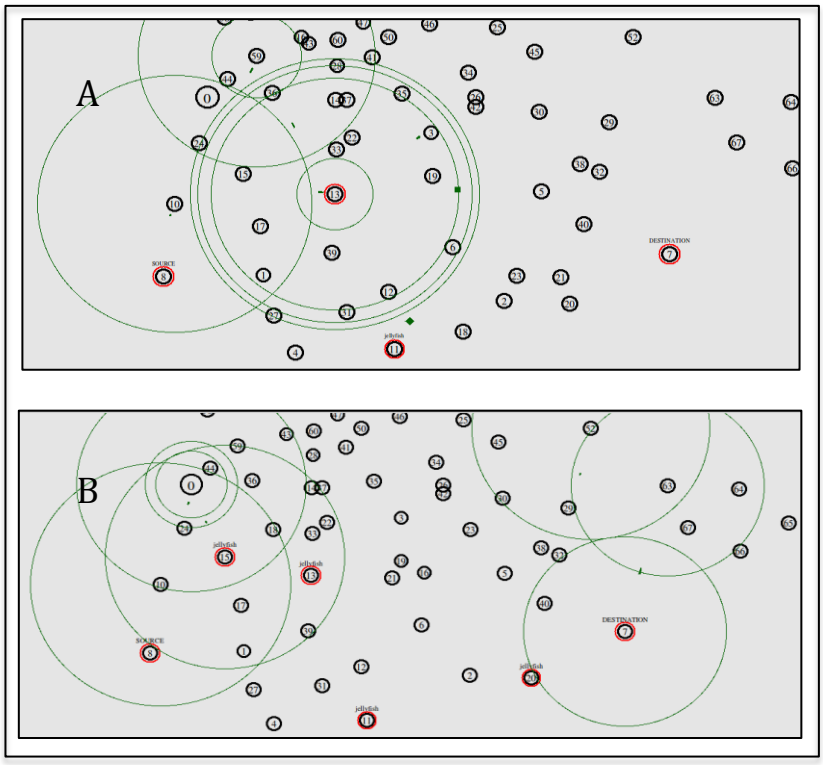

Figure 6.13. Jellyfish attacks occur gradually.

At the beginning of minute five or the detection phase according to Figure 6.3 , the jellyfish attacks have been detected, with node 13 first, followed by node 11, as illustrated in Figure 6.14 (A and B). This is followed by node 15 and node 20.

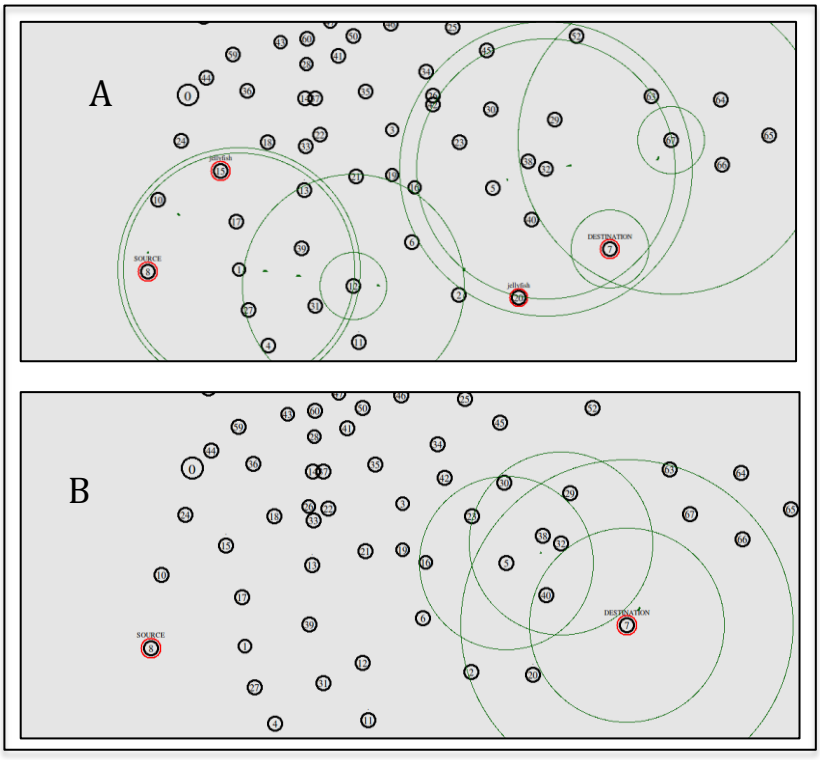

Figure 6.14. Detect jellyfish attacks completely.

6.4 Testing the proposed method against grayhole attacks on MM (Two MANETs)

MANET, with high mobility and frequent topology changes, increases the chance of one or more MANETs merging and partitioning. In this study, the focus will be on MANETs merging. Due to the vulnerabilities of MANET, such as limited protection mechanisms and a lack of central authority, many attacks can occur at any time, such as in the merging process.

The proposed method will be tested on the situation when two MANETs are about to merge. This scenario is critical as when MANETs merge many issues need to be considered to complete the merging process as quickly as possible; for example, IP address conflicts, MANET ID, and bypassing any misbehaving activities which can hinder the merging process such as the occurrence of a DoS attack which can give incorrect information and paralyse the process. Therefore, if the merging process is not handled effectively and misbehaving nodes are not detected, the effects will be serious, such as traffic delays or IP conflicts. In this experiment, the centralised trust concept, which is discussed in detail in the previous Chapter, will be used to help the MM to merge safely and successfully.

6.4.1 Experiment Design and scenario

An experimental investigation is conducted when two MANETs merge, in order to explore the efficacy of the MUMrDR method in detecting DoS attacks in MM. In this experiment, a grayhole attack is used as an example of DoS attack to evaluate and test the performance of the proposed method in this scenario. Network Simulator (NS2.35) is used to perform this experiment under LINUX (UBUNTU 12.04). This section illustrates the simulation parameters and the experiment scenario. A summary of both the simulation parameters and the computer specifications, which are used in this experiment, are illustrated in Table 6.2.

Table 6.2. Simulation parameters.

Simulation Parameters	
Processor	Intel(R) Core (TM) Duo CPU P8700 @ 2.53GHz
RAM	4.00 GB
System type	64-bit
Operating system	UBUNTU 12.04
Routing protocol	AODV
Simulation time	6 minutes
No of nodes	101
Traffic type	CBR
Packet size	512 bytes
MAC type	Mac/802_11

Two standalone MANETs are used in this experiment. The first MANET, MANET 1, consists arbitrarily of 71 nodes. Figure 6.15 shows the MANET 1 architecture.

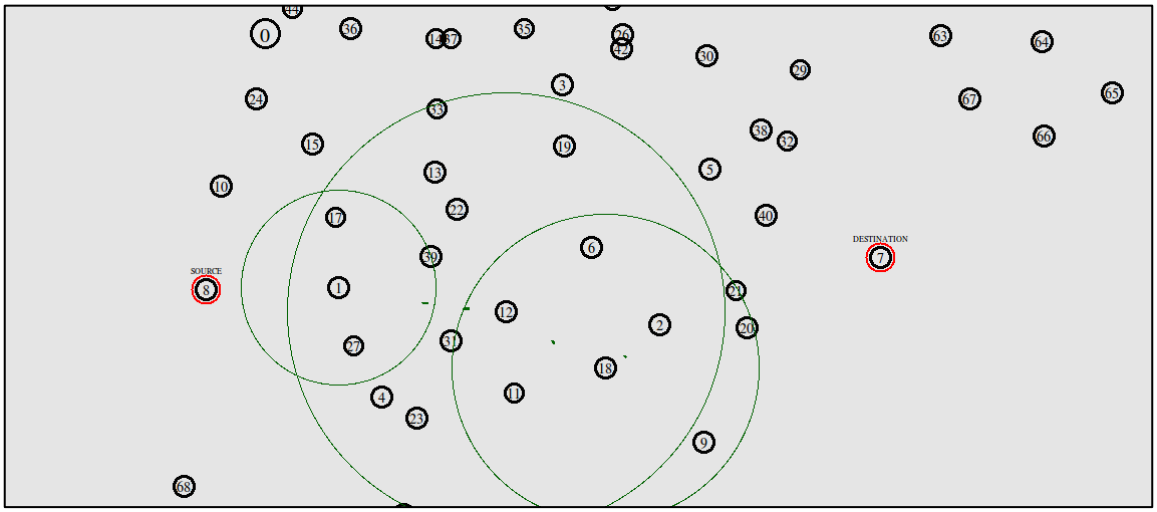

Figure 6.15. MANET 1 architecture.

In this scenario, the source node is node 8 and the destination node is node 7. The proposed method checks the TTSV for every node, three times pre-merging and

three times post-merging. The reason why the TTSV is tested three times before and after merging is to test the performance of the proposed method in different scenarios before the attack occurs; when the attack occurs; and finally after removing the attack and isolating the misbehaving nodes using the proposed method. Further, refer to Figure 6.16 in the attack phase, two grayhole nodes appear gradually, in node 10 and node 18, as shown in Figure 6.17(A). In addition, at the beginning of minute three, two extra grayhole attacks subsequently exist in nodes 16 and 25, as presented in Figure 6.17 (B).

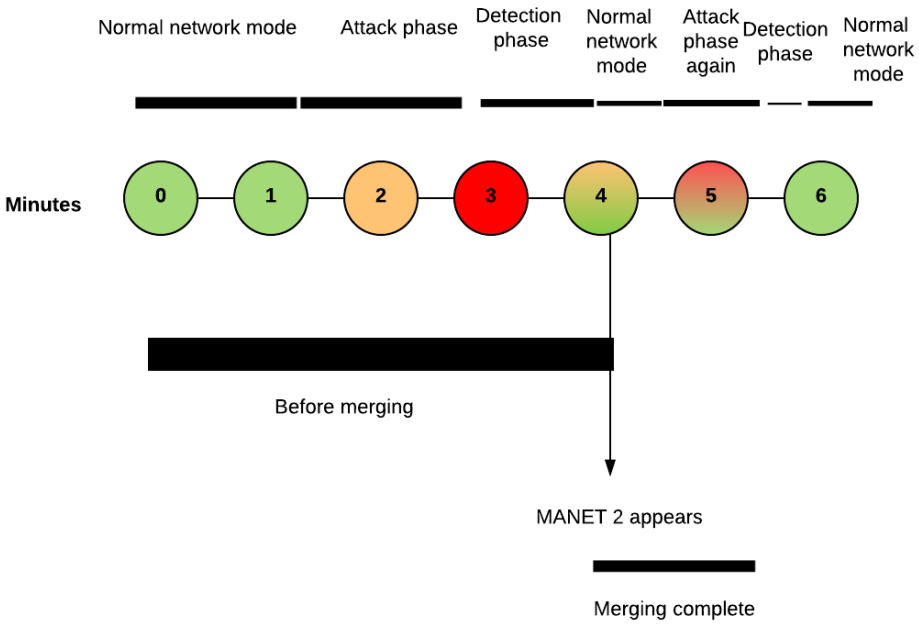

Figure 6.16. Timeline of the experiment scenario.

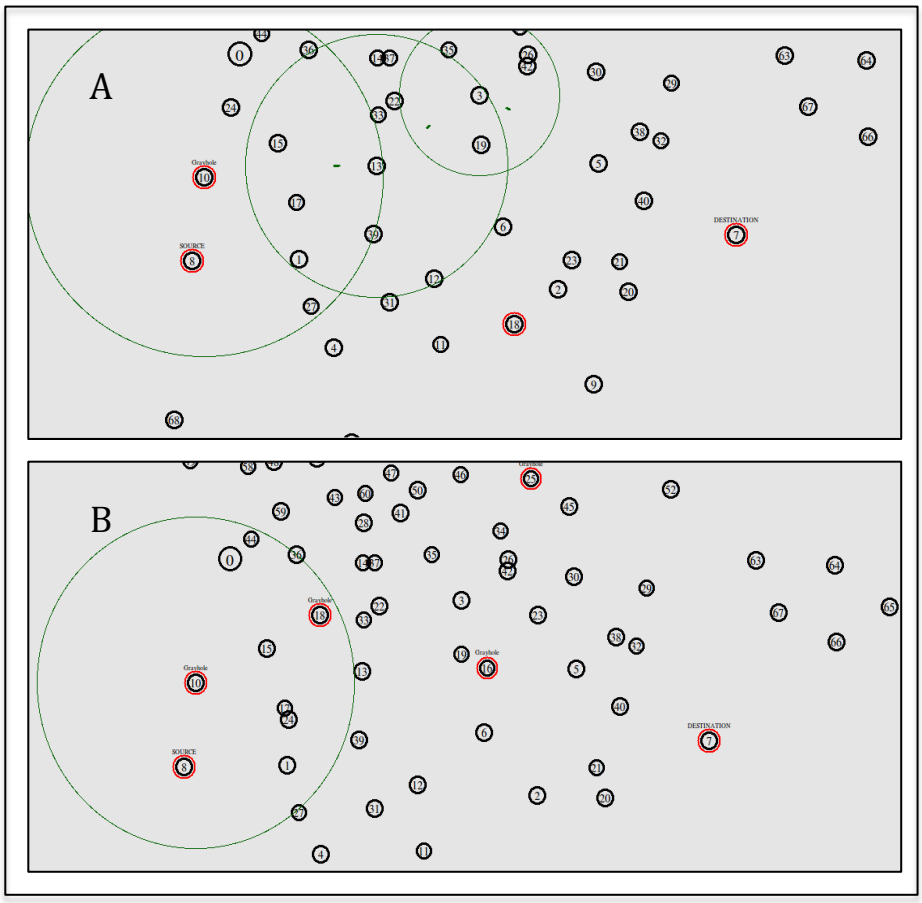

Figure 6.17. Network architecture following grayhole attacks.

At the end of minute four, the grayhole attack nodes are detected progressively, using the proposed method, as node 10 and node 18 are isolated from the communications. Further, a new MANET, which is named MANET 2 appears and will start to merge with MANET 1. Figure 6.18 (A and B) presents the gradual detection of the grayhole attacks and the occurrence of the new MANET. MANET 2 is composed of 30 nodes, so after merging with MANET 1, the total nodes will be 101 nodes.

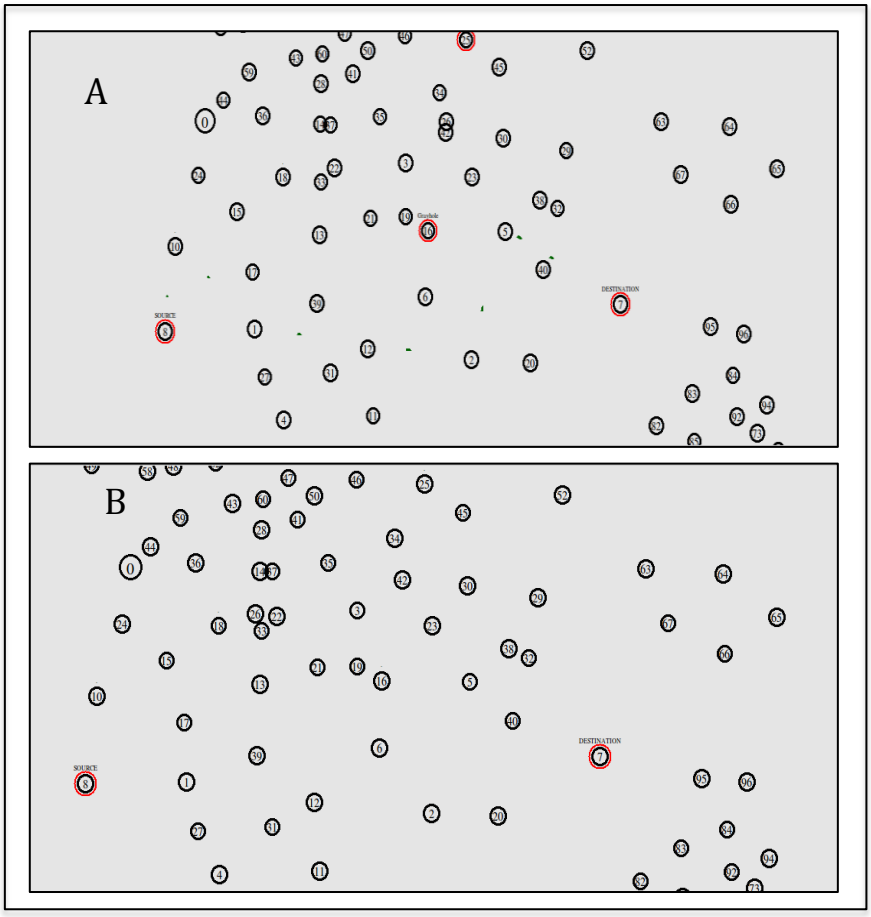

Figure 6.18. Detection of grayhole attacks gradually.

MANET 1 and MANET 2 start their negotiations, based on the centralised trust method, as one trusted node from each MANET helps to complete the process and accomplish the merging between the two networks. In this experiment, node 5 from MANET 1 and node 85 from MANET 2 are the connected nodes that have the responsibility to finalise the merging operation and check the IP address for conflict for each node. In addition, at the end of minute five as it is illustated in Figure 6.16 , the two MANETs start to merge, as shown in Figure 6.19 (A and B).

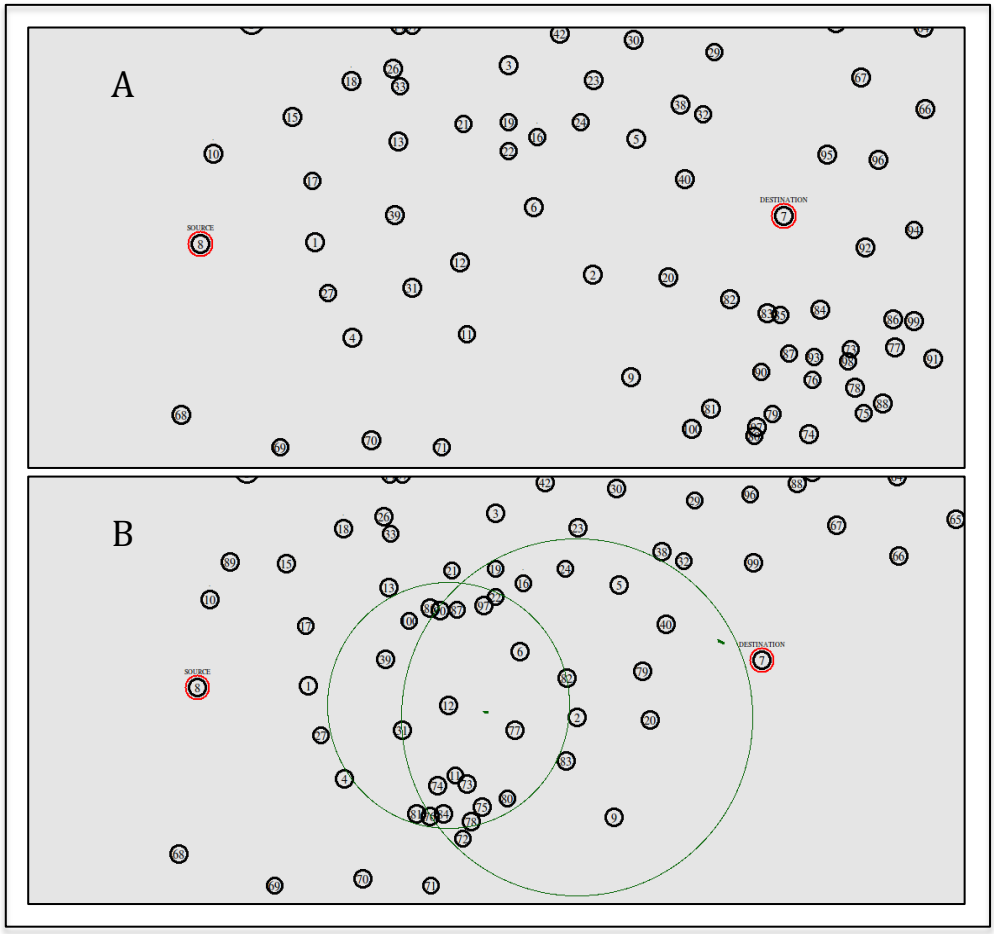

Figure 6.19. Two MANETs merging.

At the beginning of minute six at it is appeared in Figure 6.16, the two MANETs merge and two grayhole nodes occur whilst merging, at node 13 and node 39, as shown in Figure 6.20.

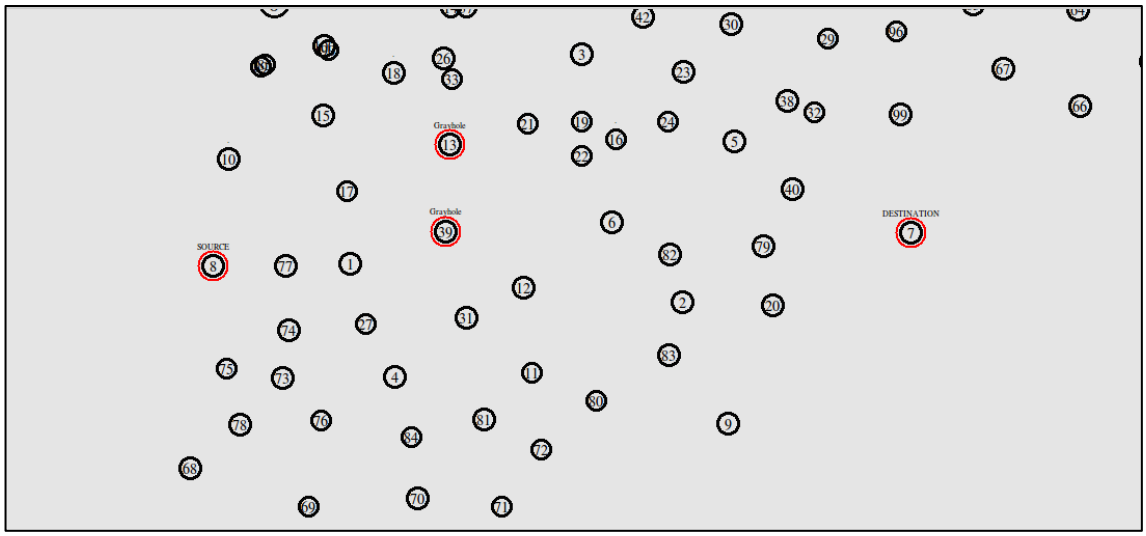

Figure 6.20. Grayhole attacks after merging.

At the middle of minute six, the proposed method detects the DoS attacks and isolates the grayhole nodes from the communication, temporally, as shown in Figure 6.21.

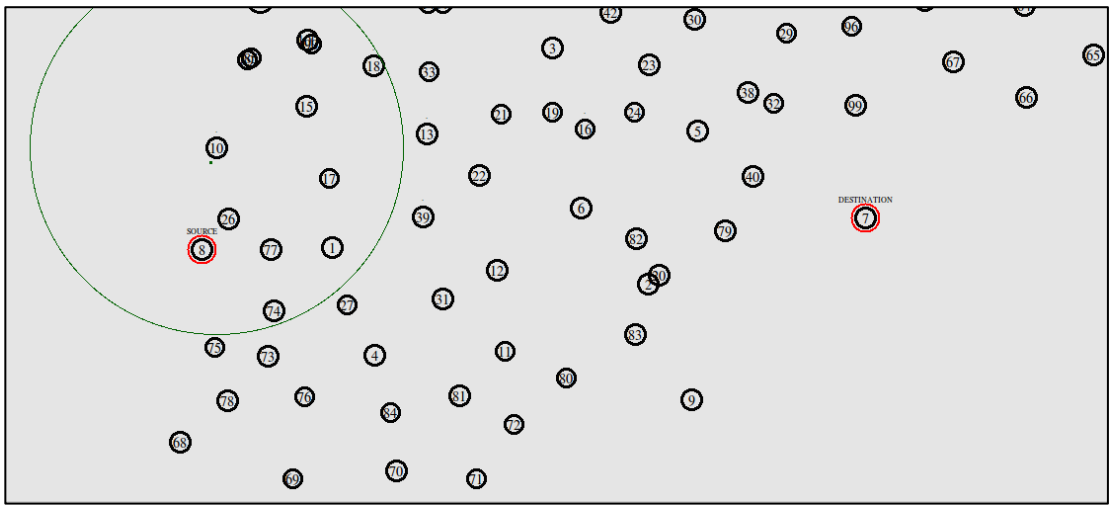

Figure 6.21. Detect grayhole attacks completely.

The proposed method then detects the grayhole nodes before and after the merging process. The TTSV measures the trust value of each three times before and after the merging process. Untrusted nodes are temporally isolated from the transmissions until their trust value changes from 0 to 1. Any node which is untrusted three successive times is isolated for longer until its TTSV changes from 0 to 1, meaning from an untrusted to a trusted node. Therefore, the TTSV will be checked in this experiment every three minutes, based on Equation 5.4 in Chapter 5. The usage of the proposed method helps to detect the grayhole nodes systematically, even in the situation of merging. Therefore, the power and effects of DoS attacks are diminished by using the proposed method which increases network performance considerably.

6.5 Testing the proposed method against different DoS attacks on MM (Four MANETs)

There is a pressing need to detect any malicious activities all the time, in order to protect the network. In this experiment the proposed method will test its efficacy to detect four types of DoS attacks: wormhole attack, blackhole attack, grayhole attack, and jellyfish attack. Drawing upon the decentralised trust concept,

which is explained in detail in Chapter 5, the four configured standalone MANETs will be merged together to make a single large MANET.

6.5.1 Experimental design and scenario

In this experiment, four types of DoS attacks are used, as demonstrated above, in order to test the performance of the proposed method in a situation where many MANETs are merged, as well as determine how to detect DoS attacks in this situation. As demonstrated in the previous section (6.1), this experiment uses the same network simulator. The simulation parameters and the computer specifications, which are utilised in this experiment are shown in Table 6.3.

Table 6.3. Simulation parameters for four MANETs merge.

Simulation Parameters	
Processor	Intel(R) Core (TM) Duo CPU P8700 @ 2.53GHz
RAM	4.00 GB
System type	64-bit
Operating system	UBUNTU 12.04
Routing protocol	AODV
Simulation time	6 minutes
No of nodes	50
Traffic type	CBR
Packet size	512 bytes
MAC type	Mac/802_11

Each network has a different number of nodes. MANET 1 in top left has eleven nodes. MANET 2 in the top right includes fourteen nodes. MANET 3 in bottom left has twelve nodes. MANET 4 in the bottom right has thirteen nodes. Figure 6.22 shows the architecture of these MANETs.

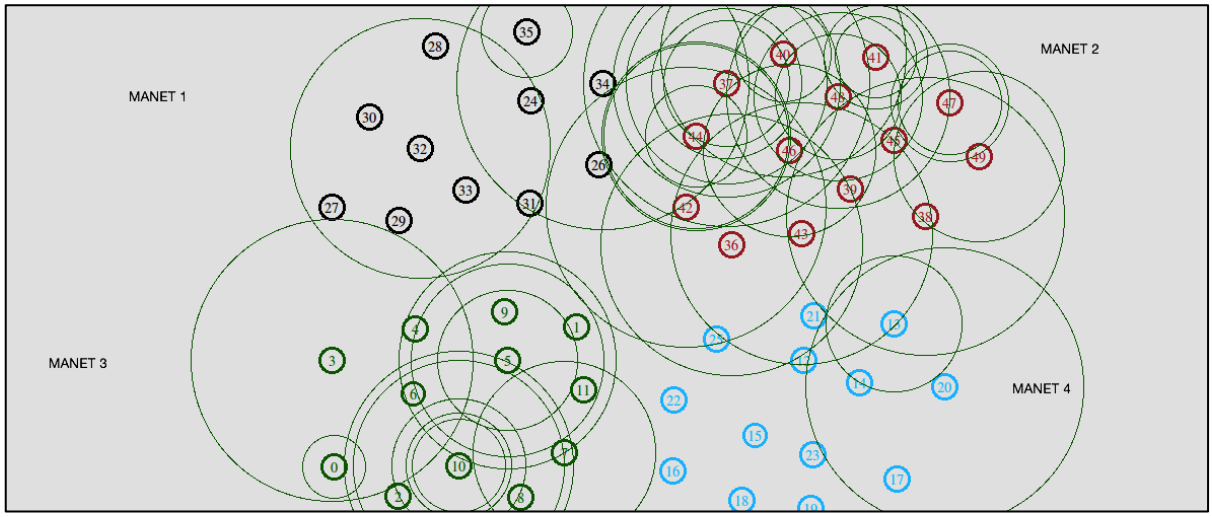

Figure 6.22. Four MANETs architecture.

The duration of this experiment is six minutes and the complete timeline of this experiment is shown in Figure 6.23.

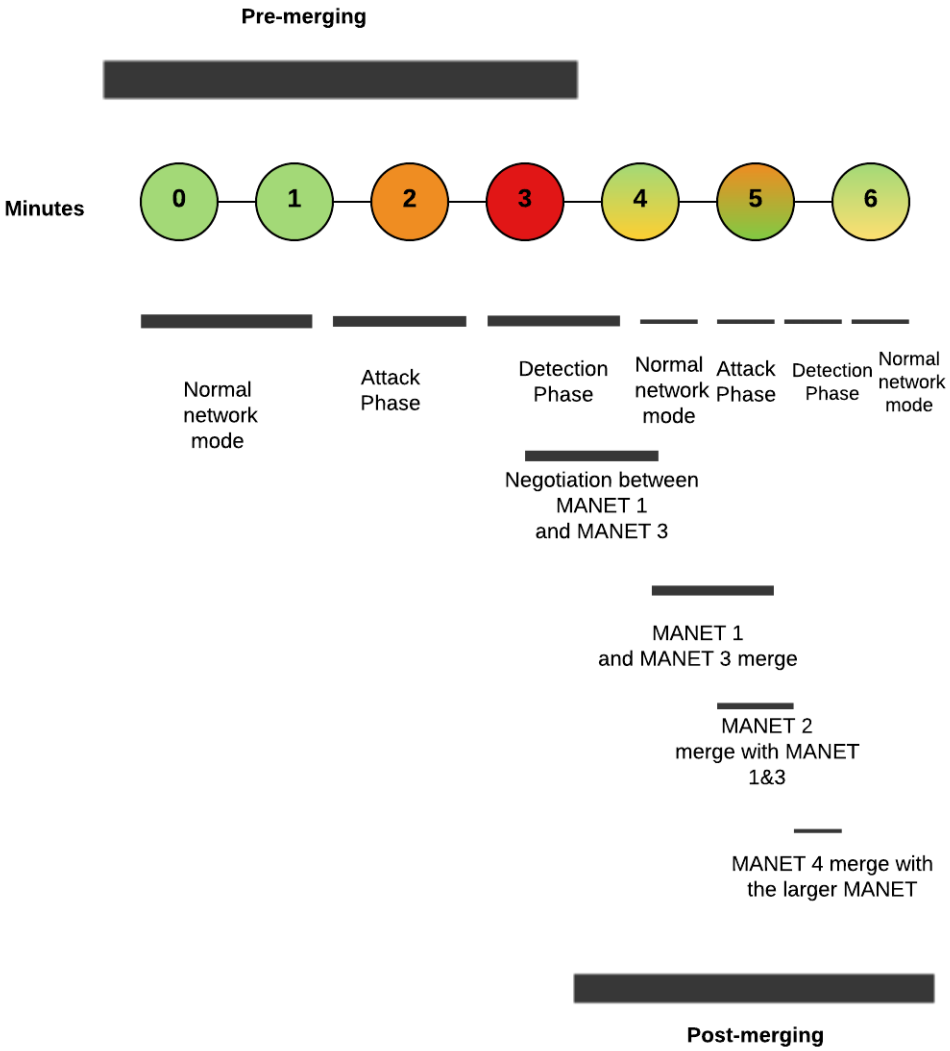

Figure 6.23. The timeline of the experiment.

At the beginning or in the normal network mode as it is illustrated in Figure 6.23, around the first 30 seconds of this experiment, the four MANETs do not start the merging negotiations, and they are separated.

At the end of minute two or in the attack phase depends on Figure 6.23, different DoS attacks occur in each MANET. Grayhole attacks appear in both

MANET 3 and MANET 4. After ten seconds of the occurrence of jellyfish attack in MANET 1, a wormhole attack occurs in MANET 2 as shown in Figure 6.24.

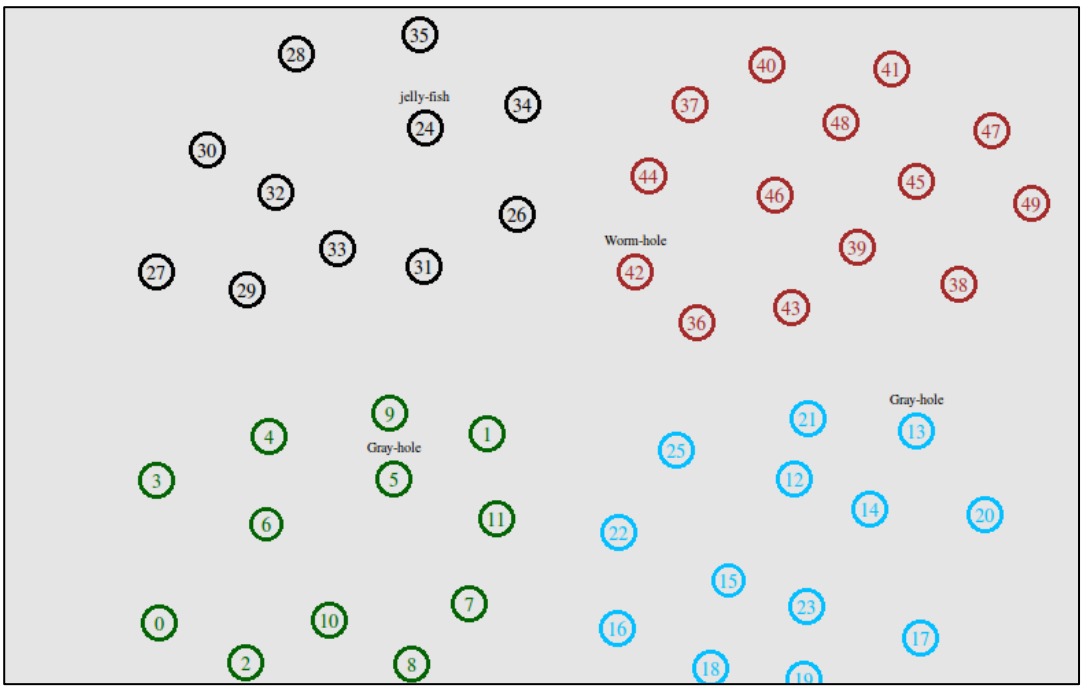

Figure 6.24. Different DoS attacks occur in different MANET.

Using the proposed method in each MANET helps to detect the DoS attacks gradually from all MANETs by the beginning of minute three based on Figure 6.23. Figure 6.25 shows the detection of all DoS attacks in each MANET.

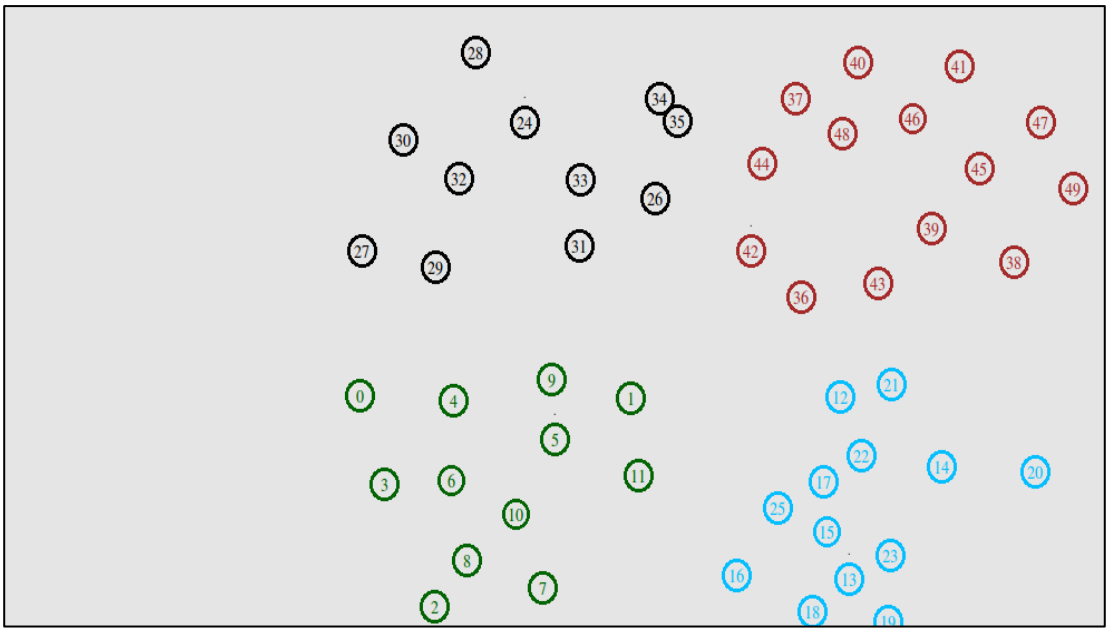

Figure 6.25. Removing DoS attacks completely from all MANETs.

At the middle of minute three, as shown in Figure 6.26 (A and B), node number 35 joins MANET 2.

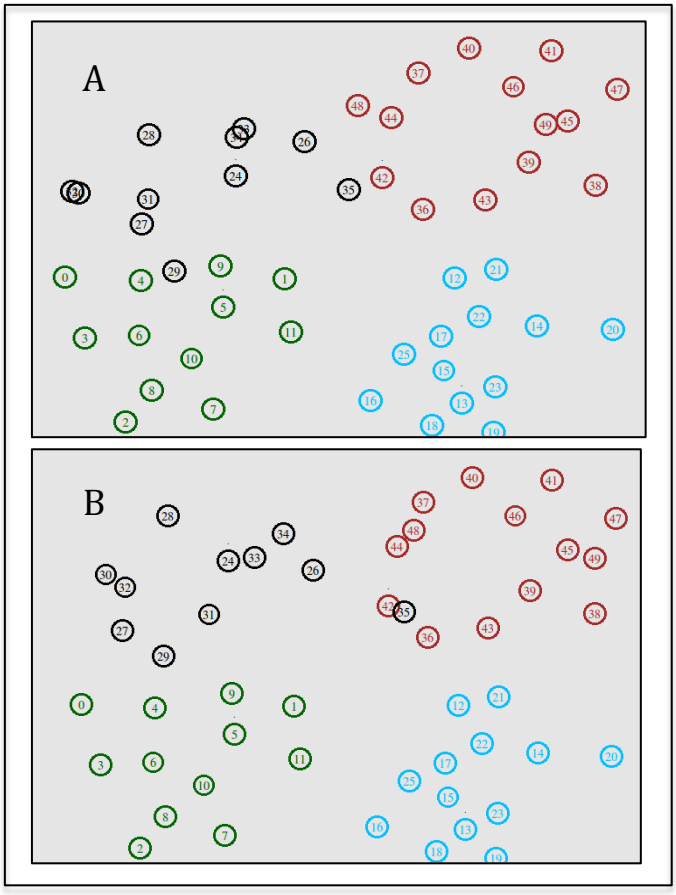

Figure 6.26. Node 35 joins MANET 2.

At the end of minute three (Figure 6.23), MANET 1 and MANET 3 start to merge, negations between them are based on decentralised trust concept. This is shown in Figure 6.27 (A and B).

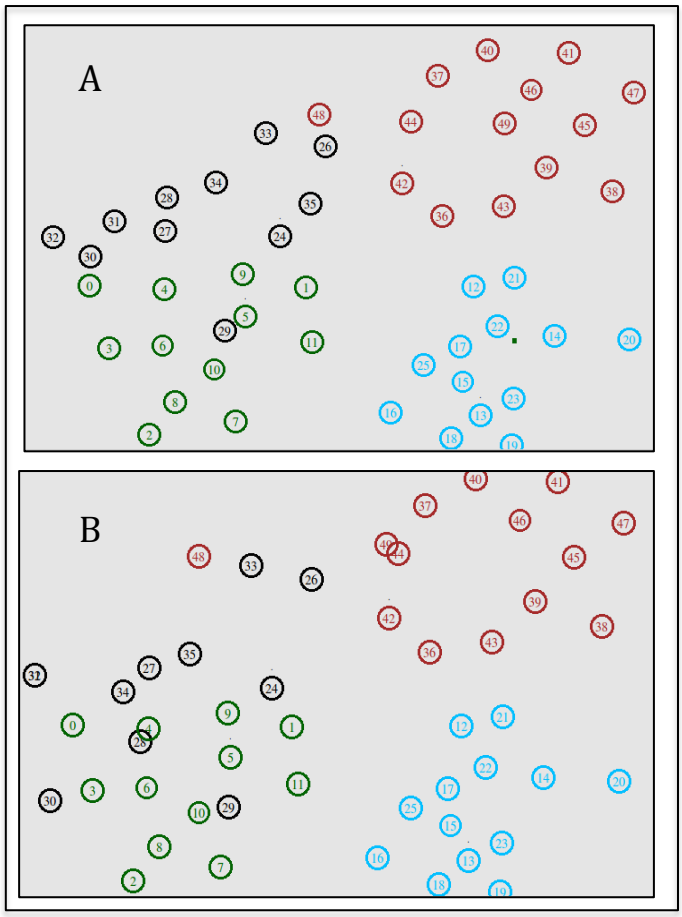

Figure 6.27. MANET 1 and MANET 3 merge.

As explained in Chapter 5, the decentralised trust concept means that all nodes from each MANET cooperate to complete the merging process. Thus, the decentralised trust concept enables all nodes either trusted or untrusted to participate in the merging process unless they give incorrect information and are nominated as malicious or selfish nodes. Thence, this type of untrusted nodes would be isolated from communication until their trust values change to 1 or the merging process is complete. This concept allows all nodes to participate in the merging process as some types of DoS attacks, such as grayhole attacks, do not behave maliciously all the time. They can convert to the normal mode sometimes. For example, a thief does not behave badly all the time; their behaviour can appear normal in the daytime and convert to criminal behaviour at night. Moreover, this thief could be a person who has a job and performs duties and tasks. The same concept is used here in the decentralised trust concept, as nodes which give correct information can cooperate and assign IP addresses to other nodes.

At the middle of minute four, MANET 2 starts merging with MANET 1 and MANET 3, as they become one big MANET. Figure 6.28 (A and B) shows this merging progressively.

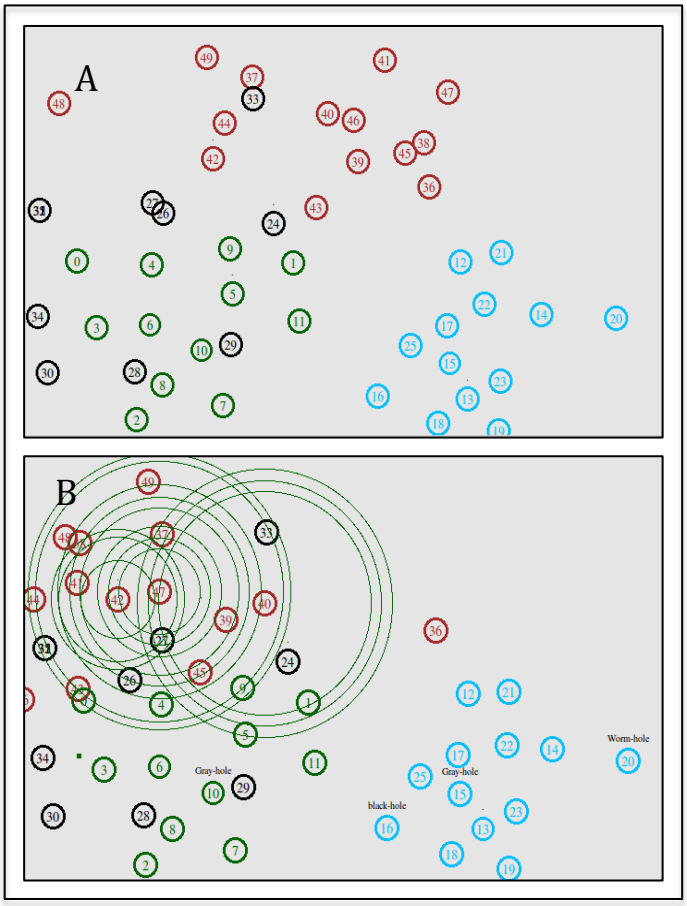

Figure 6.28. MANET 2 merges with merged MANET (MANET 1+ MANET3).

At the beginning of minute five or in the attack phase regards Figure 6.23, MANET 1, MANET 2 and MANET 3 become one big MANET and many DoS attacks appear in the big MANET and in MANET 4, as illustrated in Figure 6.28. MANET 4 starts negotiations based on decentralised trust concepts to merge with the big MANET. Thus, nodes from the big MANET will communicate with nodes in MANET 4 in order to complete the merging process and ensure that nodes merge without any IP address conflict. In addition, DoS attacks, such as grayhole attack and wormhole attack occur during the merging process, as show in Figure 6.29 (A and B). In this situation, all nodes from both of the networks will cooperate to complete the merging process and isolate misbehaving nodes which give incorrect information from communication until either their TTSV changes from 0 to 1 or the merging process is complete.

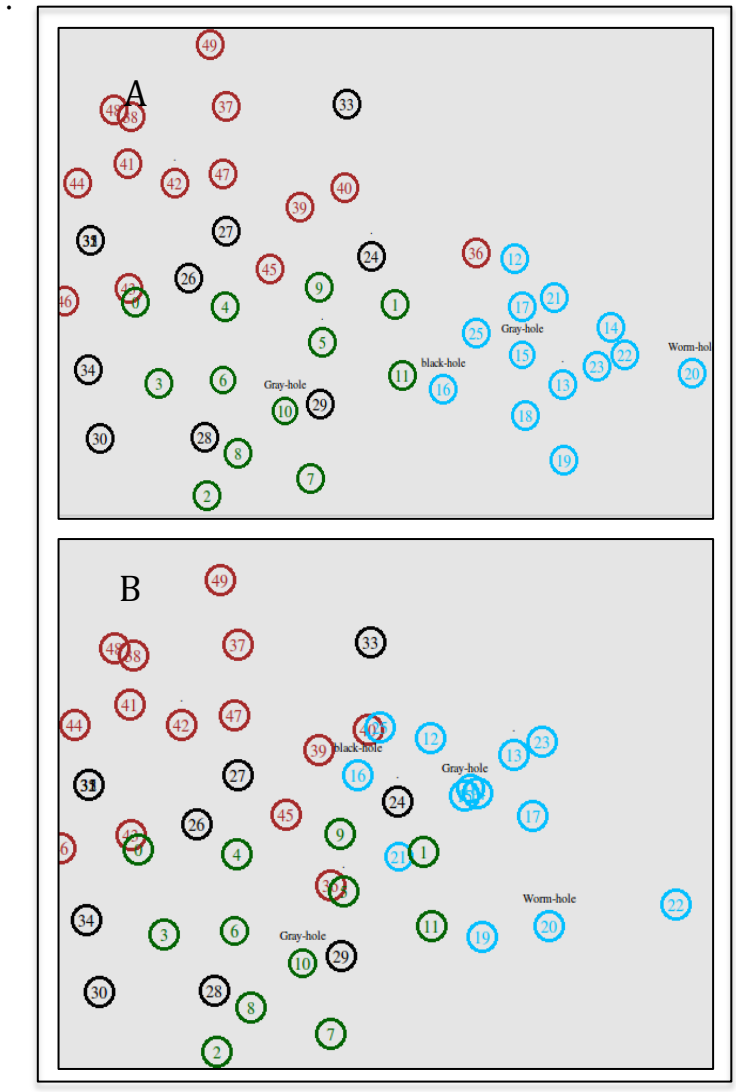

Figure 6.29. MANET 4 starts merging process with the big MANET.

At the middle of minute five or the detection phase as it is presented in Figure 6.23, the detection of DoS attacks is performed, based on the proposed method as it is shown in Figure 6.30.

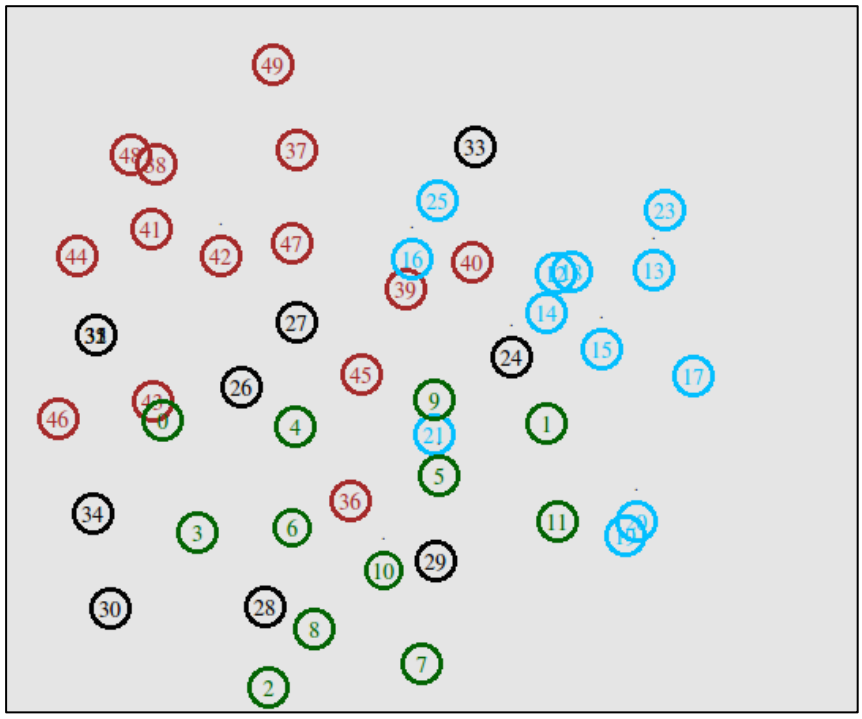

Figure 6.30. Merging nearly complete and the DoS attacks are detected.

At the beginning of minute six or in the normal network mode as it is displayed in Figure 6.23, the merging process is complete and the four MANETs become one big MANET, as shown in Figure 6.31.

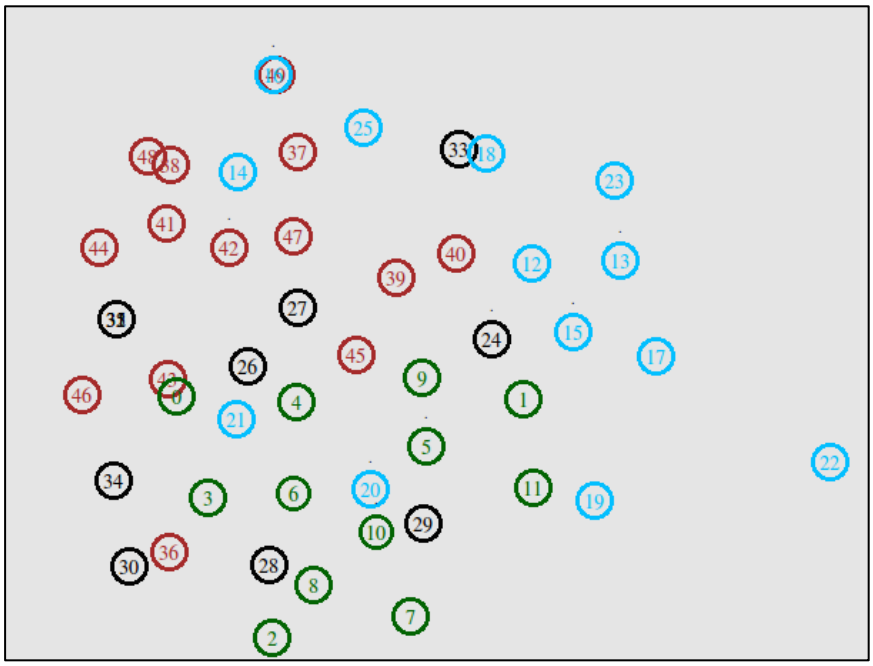

Figure 6.31. Merging complete.

6.6 Chapter summary

This chapter presents the simulation of the proposed method to detect different types of DoS attacks, in both SM and MM. The implementation of this simulation helps to test the effectiveness of the proposed method. First, in SM, the MrDR is applied to detect different types of DoS attacks separately; blackhole attack, wormhole attack, grayhole attack, and jellyfish attack. The purpose of testing the proposed method under various DoS attacks is to evaluate the performance of MrDR against different scenarios. Second, the MUMrDR is used to detect grayhole attacks, when two MANETs are merging. In this experiment, a centralised trust concept is used to accomplish the process. Third, decentralised trust concept in this experiment helps four configured MANETs to merge and detect many types of DoS attacks. NS2 is used to simulate all these experiments. In the next chapter, the results and evaluation will be done for these experiments, in order to assess the performance of the proposed method under multiple situations and experiments.

Chapter 7: Results and Evaluation

This chapter presents the findings obtained from the research by setting out the results of different experiments on both SM and MM. First, the proposed method detects different DoS attacks on SM. In the previous chapter, four types of DoS attacks were tested on SM: wormhole attack; blackhole attack; grayhole attack; and jellyfish attack. In addition, MUMrDR is used to detect different DoS attacks, even on MM. Two main experiments are performed on MM: two MANETs and four MANETs.

This chapter will illustrate the findings and evaluate the results against existing approaches on SM. On MM, there is no existing work that deals with this situation. Subsequently, this chapter will explore and clarify the results of the experiments explained in detail with their scenarios in the previous chapter.

7.1 Evaluation overview

Evaluation is the process of judging something's value, importance, quality or a report which contains this information (Press, 2016b). Many evaluation schemes have been proposed in order to evaluate the efficiency of new methods or systems, such as Common Criteria (CC), Evaluation Assurance Level (EAL), Security Functional Requirement (SFR), and Security Function Policy (SFP) (Merkow and Breithaupt, 2004). CC is the set of recognised technical configurations and standards, which nationally and internationally enable security evaluations of information technology (IT) products and technologies. These are the individual set of configurations or common criteria for technical standards that improve a technology or specific product, which qualifies for such a protection profile (Wallace, 2003). However, CC has not been used in this study to evaluate the security in MANET as the CC is used only in federal government sectors and critical infrastructure instead

of personal networks and non-fixed infrastructure such as using MANET in conferences or cafes.

Evaluation of a system or method is important in order to measure the quality and power of the new method. In addition, it provides a comparative analysis between the proposed method and existing methods, in order to prioritise the best method that is available in an environment such as MANET. It means that a method which results in increasing the network throughput and packets delivery ratio, can defend against misbehaving activities such as DoS attacks.

It is important to bear in mind that in order to evaluate the effectiveness of the proposed method, it needs to be tested and simulated, to measure different factors and network performances, using this method. Network Simulator (NS2) is used in this study for reasons which are explained in the previous chapter to simulate the proposed method and express how the MrDR method could deter DoS attacks in both SM and MM.

7.2 MrDR results against different DoS attacks on SM

As explained in the previous chapter, different DoS attacks detect SM. As the total duration of the experiments is six minutes; the TTSV of each node will be calculated every two minutes based on Equation 5.3 in Chapter 5. For each DoS attack, the network performance will be measured in three ways: network throughput; packet delivery ratio; and packet delay ratio. Subsequently, the network performance for each attack will be measured every two minutes. The reason for this measurement is to compare the performance of the network in three situations: before the occurrence of the attack; after the attack occurs, and after detecting the attack using the proposed method.

7.2.1 Testing the MrDR method against wormhole attack

In this subsection, the results of network performance are explored when a wormhole attack is launched by malicious nodes. The detailed scenario of the experiment is explained in the previous chapter. The comparison of the network performance aspects will show the efficacy of the proposed method in detecting this attack and enhance the network performance considerably.

7.2.1.1 Network performance before the occurrence of a wormhole attack

Figure 7.1 shows the network performance before the appearance of wormhole attacks. The packet delivery ratio and network throughput rise steadily, as there are no attacks that deteriorate the performance of the network. In addition, the packet delay ratio decreases, compared with the packet delivery ratio and the network throughput. That is to say, in the normal situation as no attack appears, the network performance is in the expected form and performs its tasks normally. Thence, packet delivery ratio and network throughput are high whereas the packet delay ratio is low.

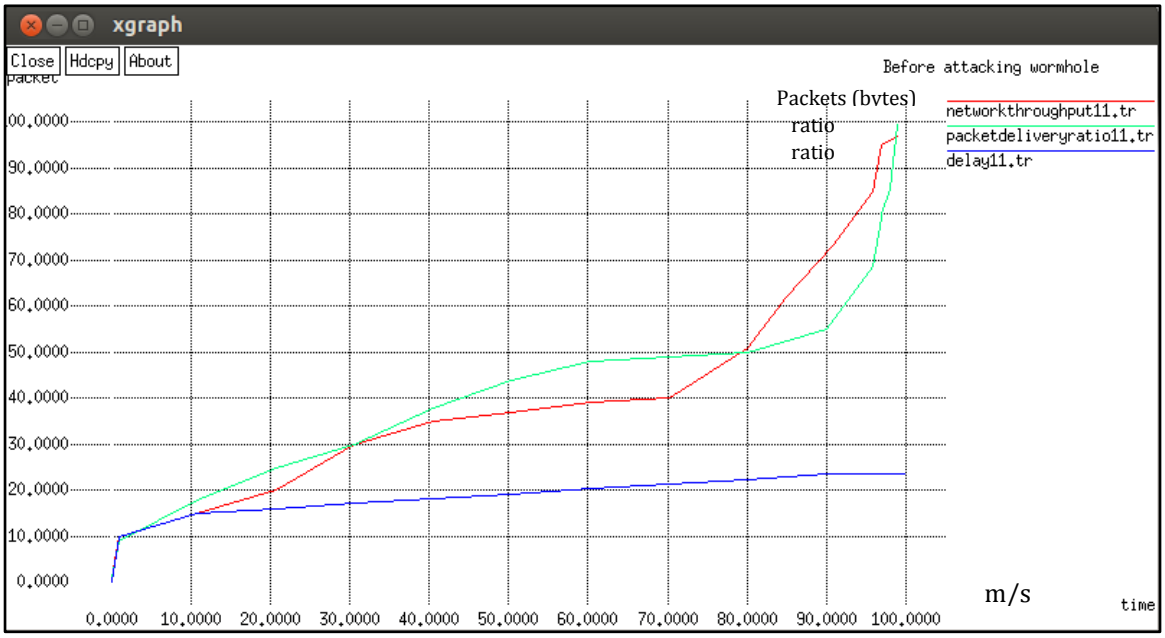

Figure 7.1. Network performance before wormhole attack occurs.

7.2.1.2 Network performance when the wormhole attack occurs

From the data in Figure 7.2, it is shown that the network performance when the wormhole attack is launched is affected as the network performance in network throughput and packet delivery ratio drop dramatically. More precisely, the packet delay ratio increases, due to the wormhole attacks.

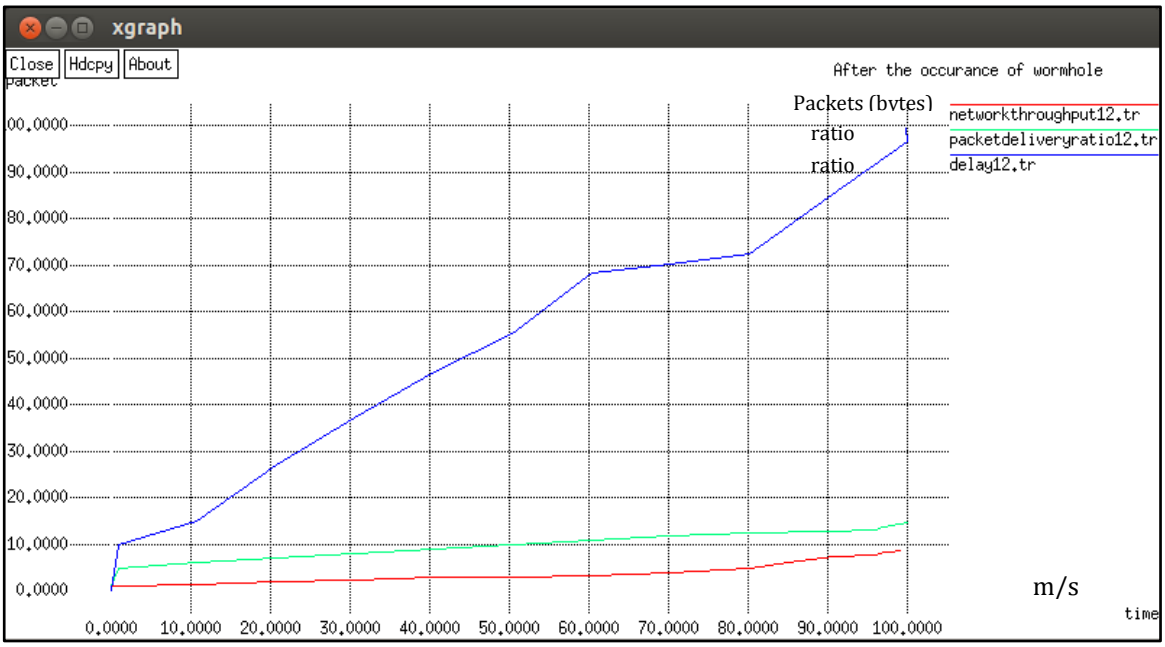

Figure 7.2. Network performance when wormhole attack occurs.

7.2.1.3 Network performance after detecting wormhole attack using MrDR method

In Figure 7.3, it is shown from that there is a clear trend in the decrease in packet delay ratio after removing the wormhole attacks and isolating the wormhole nodes using the proposed method. The packet delivery ratio and network throughput increase considerably. Removing wormhole attacks means that the malicious nodes are temporarily discarded from communications, until its trust value is restored and it becomes a trusted node.

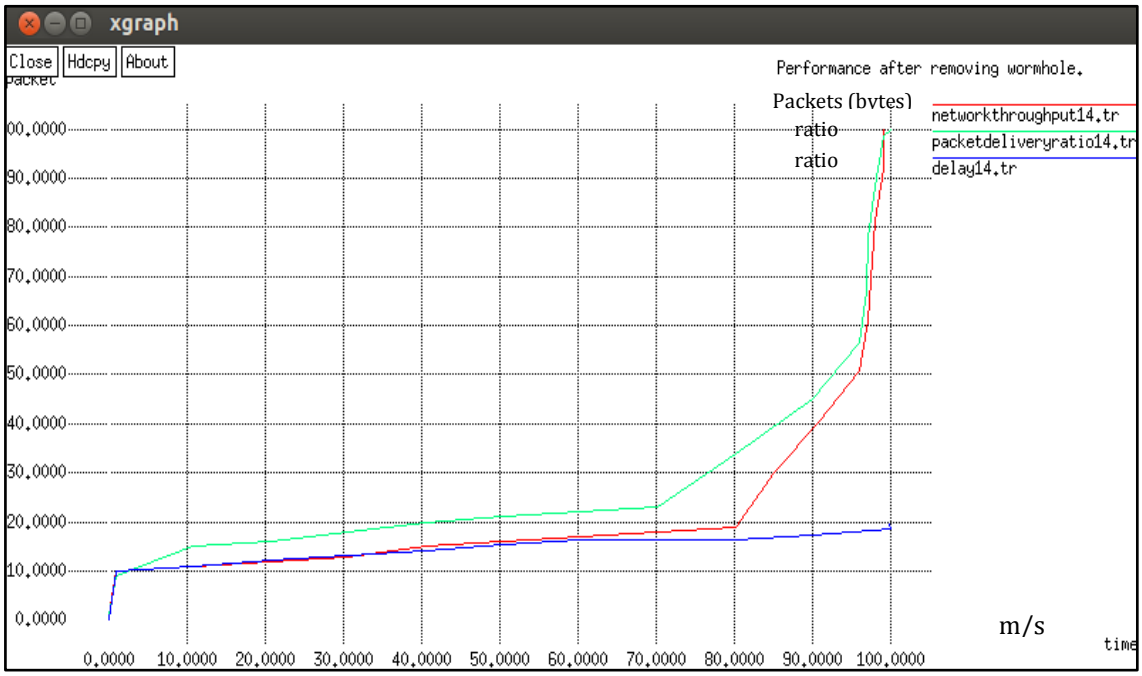

Figure 7.3. Network performance after removing wormhole attacks.

7.2.2 Testing the MrDR method against blackhole attack

The proposed method is tested also against the blackhole attack, as explained in the previous chapter. This subsection defines the results of the network performance in three situations, as with the previous attack.

7.2.2.1 Network performance before the occurrence of a blackhole attack

The network performance before the occurance of blackhole attack is positive and normal as the packet delay ratio is low, whereas packet delivery ratio and the network throughput are high. Normal means that as there is no attack occurs, the nodes will perform their duties normally such as send packets to the intended nodes. Figure 7.4 shows the network performance at the end of minute two as no attack has yet occurred.

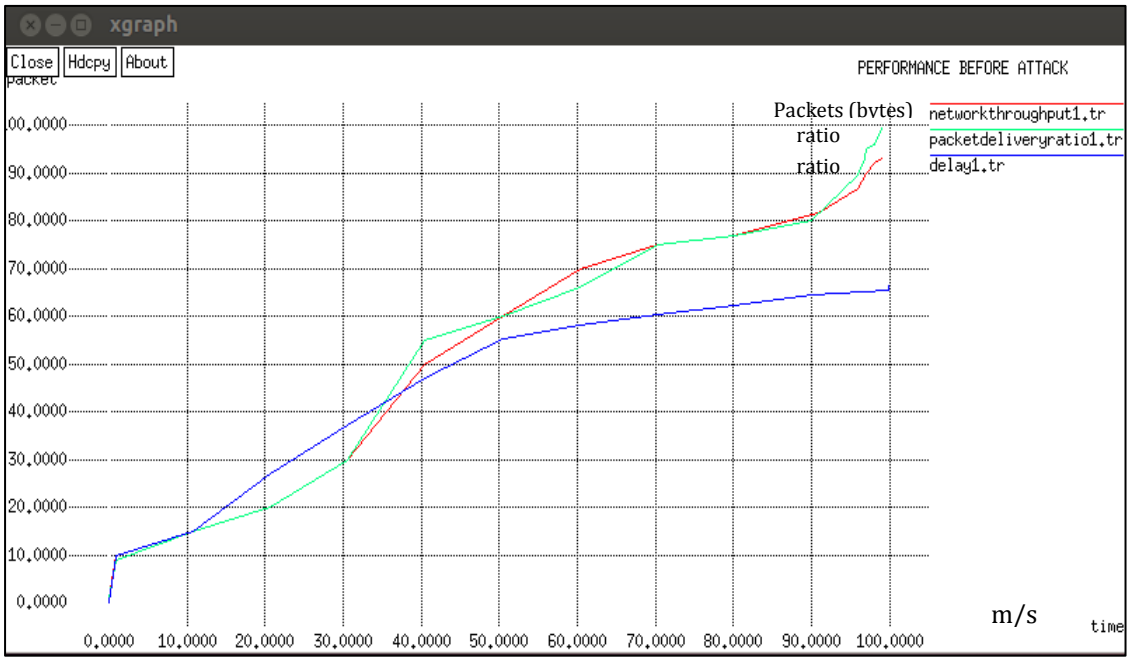

Figure 7.4. Network performance before blackhole attack is launched.

7.2.2.2 *Network performance when blackhole attack occurs*

Figure 7.5 plots the network performance when the blackhole attack is launched during minute four of the experiment or in the attack phase depends on Figure 6.3. The network performance is degraded as the packet delay ratio increases, whereas the network throughput and packet delivery ratio decrease dramatically. In the blackhole attack, the malicious nodes drop packet, so the packet delay ratio increments

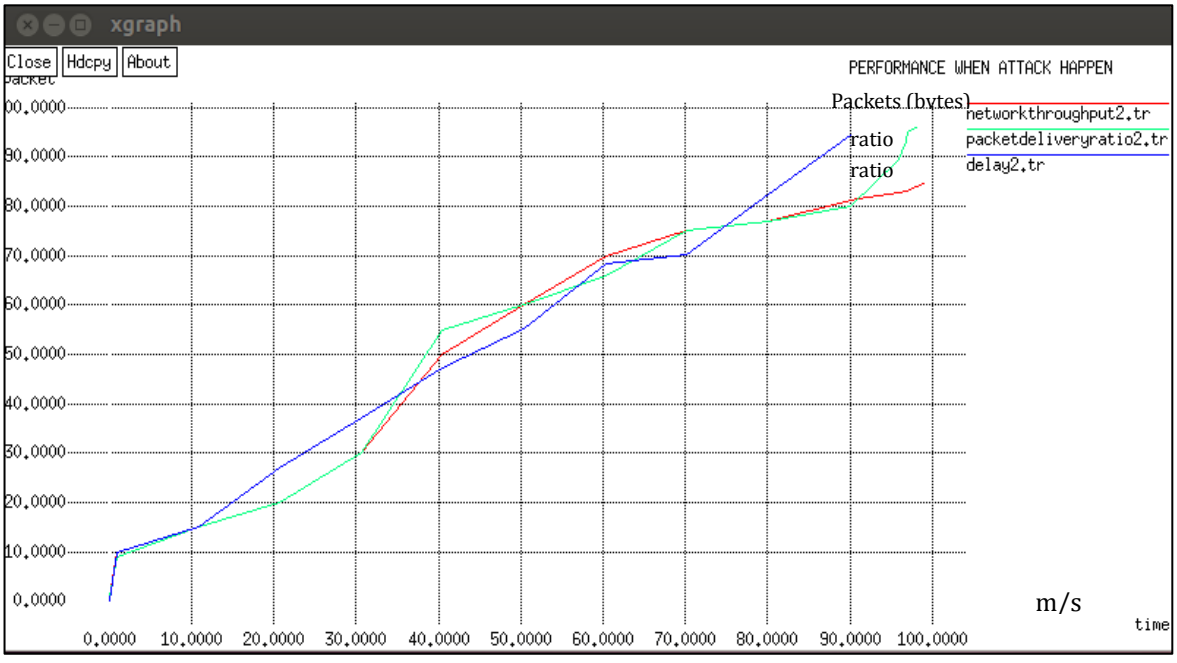

Figure 7.5. Network performance when blackhole attack occurs.

7.2.2.3 Network performance after detecting a blackhole attack using MrDR method

The network performance is positive as shown in Figure 7.6 In other words, the malicious nodes which launch the blackhole attack are detected using the proposed method and isolated from communications until they convert from an untrusted mode to a trusted one. The trust value is checked every two minutes in this experiment. Therefore, the network throughput and packet delivery ratio rise such as before the occurrence of the attack, and packet delay ratio decreases significantly.

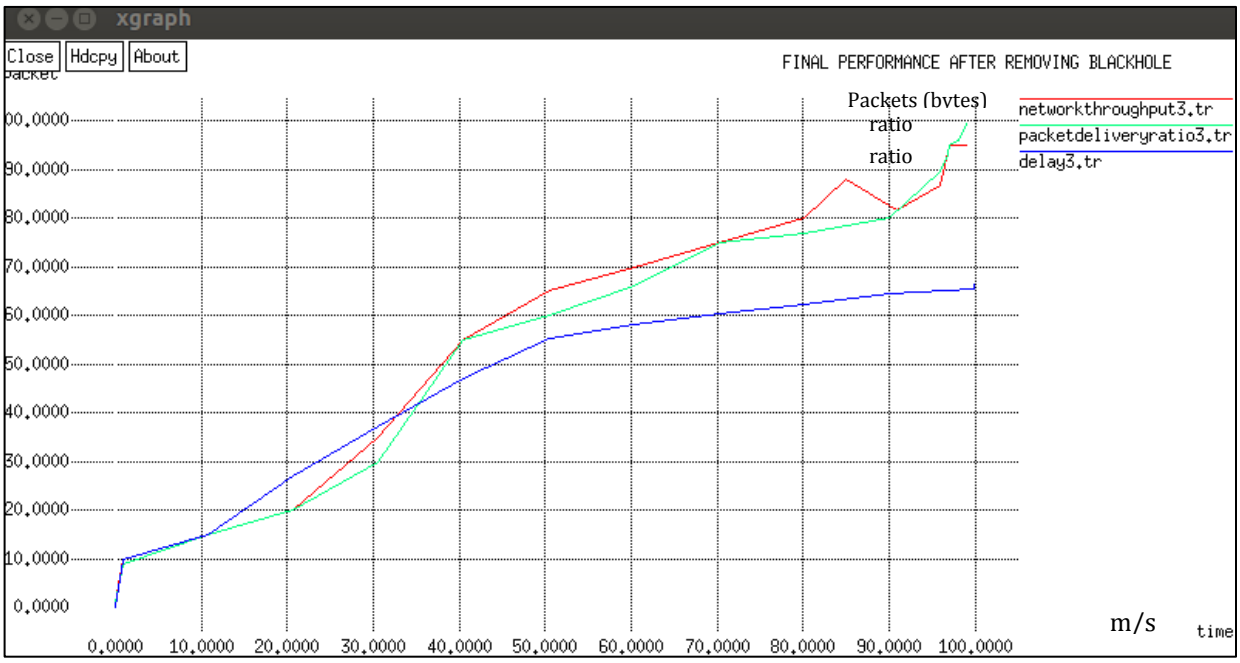

Figure 7.6. Network performance after detecting blackhole attacks.

7.2.3 Testing the MrDR method against grayhole attack

The previous section has shown the results of using the MrDR method to detect blackhole attacks in SM. In this subsection, a grayhole attack is used to test the effectiveness of the proposed method. The whole scenario of the experiment is explained in the previous chapter.

7.2.3.1 Network performance before the occurrence of a grayhole attack

Network activity in the first two minutes of this experiment in the normal network mode as the previous attacks and performs the expected activity because there is no attacks occur which disturb the network performance. Figure 7.7 provides the network performance in that time as network throughput and the packet delivery ratio increase, whereas the packet delay ratio decreases sharply.

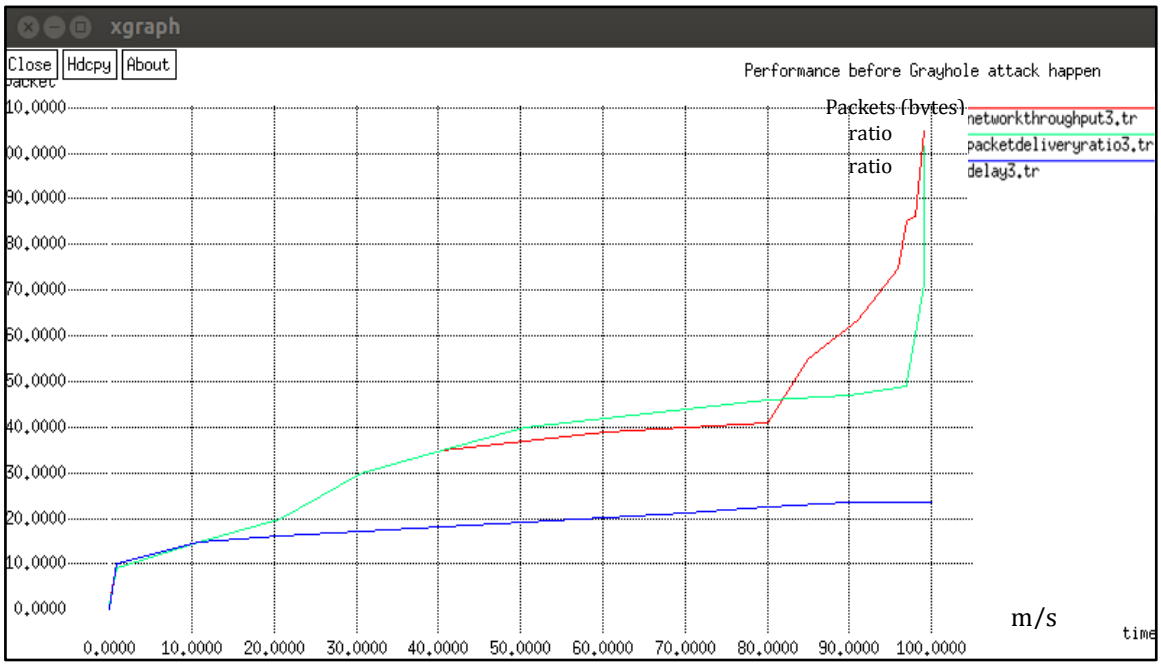

Figure 7.7. Network performance before grayhole attack appears.

7.2.3.2 Network performance when grayhole attack occurs

Furthermore, with the presence of the grayhole attacks, the network performance deteriorates. The network throughput and the packet delivery ratio decrease rapidly, whereas the packet delay ratio increases considerably. Figure 7.8 shows this information clearly. In addition, in this plot the network overhead increases gradually due to the DoS attacks. Grayhole attacks increase the overhead on the network, as explained in the previous chapter about the performance of this attack. The misbehaving nodes can convert from normal mode to malicious mode and drop packets like blackhole attacks. Therefore, the detection of these attacks is considered harder than the blackhole attack (Shanmuganathan and Anand, 2012).

However, in this study, the network overhead is measured on grayhole attack because it is more harmful than the blackhole attack and can be measured in the future for the other DoS attacks. In addition, the measurement of the overhead will give an idea about the effects of using the proposed method on the network overhead.

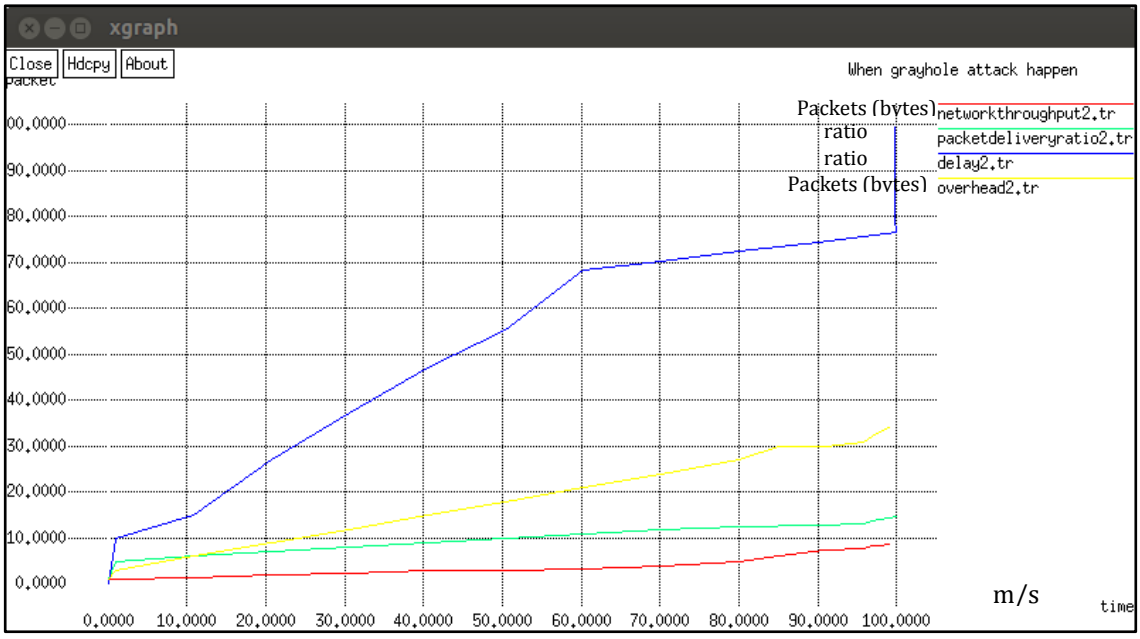

Figure 7.8. Network performance under grayhole attacks.

7.2.3.3 Network performance after detecting grayhole attacks using MrDR method

Figure 7.9 shows the network performance after using the proposed method and the detection of the grayhole attack. From this data, it can be seen that the network throughput and packet delivery ratio improve compared with data in Figure 7.8. The misbehaving nodes that launch this attack are detected using the proposed method and isolated from the communication until they become trusted nodes. Also, packet delay ratio decreases rapidly after detecting the grayhole attack in the network. Furthermore, the network overhead decreases slightly compared to data in Figure 7.8 . Thus, the proposed method does not increase the load on the network, and that is important in an environment such as MANET, with constraints on energy.

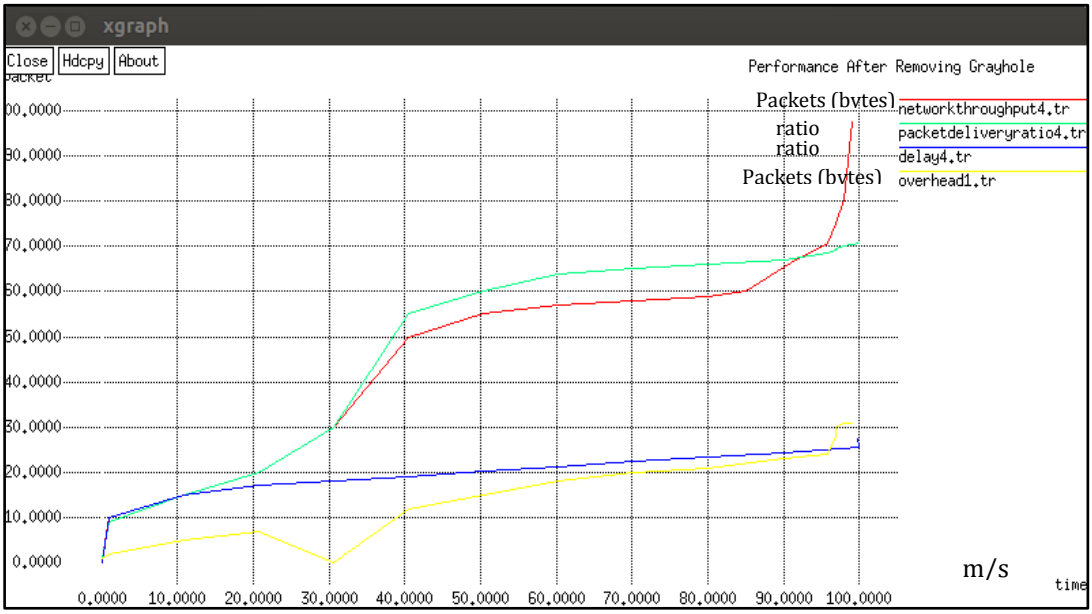

Figure 7.9. Network performance after detecting grayhole attacks.

7.2.4 Testing the MrDR method against jellyfish attack

This subsection presents the results of using the proposed method to detect jellyfish attacks. Again, the completed scenario of this experiment is outlined in the previous chapter.

7.2.4.1 Network performance before the occurrence of jellyfish attack

At the end of minute two or in the normal network mode, since there is no attack, the network performance is the same as is mentioned in the previous experiments. Before the occurrence of any attack, the network performs its tasks normally without any hindrances. Figure 7.10 indicates that both network throughput and packet delivery ratio increment, whereas the packet delay ratio decrements.

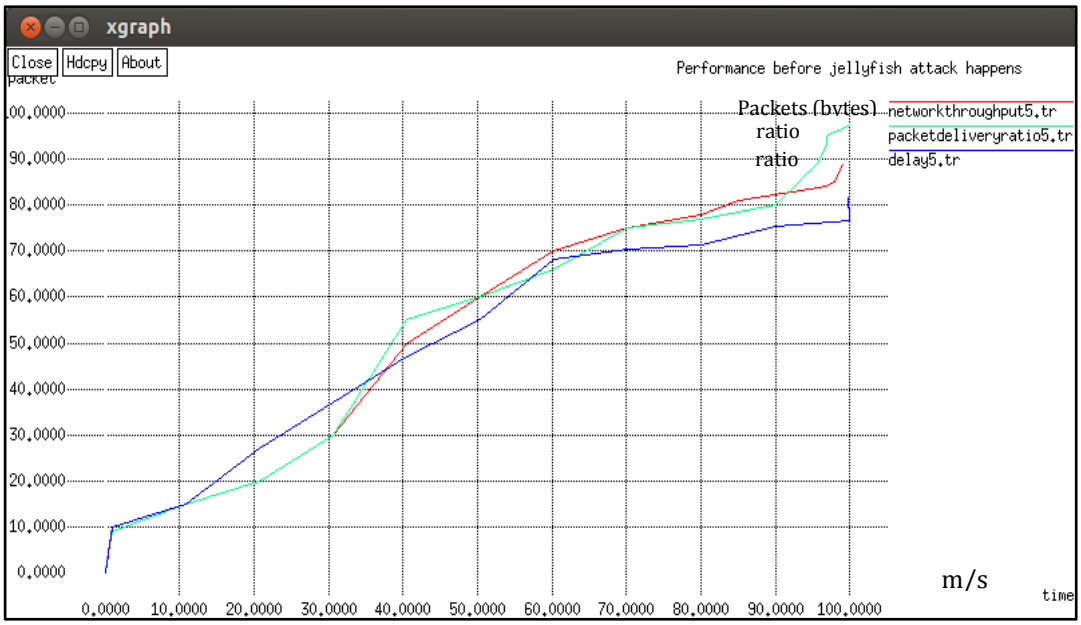

Figure 7.10. Network performance before the occurrence of jellyfish attack.

7.2.4.2 *Network performance when a jellyfish attack occurs*

At the end of minute four, Figure 7.11 plots the network performance after a jellyfish attack at the end of minute four or in the attack phase. A jellyfish attack deteriorates the network and affects the network activities. The packet delivery ratio and the network throughput diminish, with an increase in the packet delay ratio.

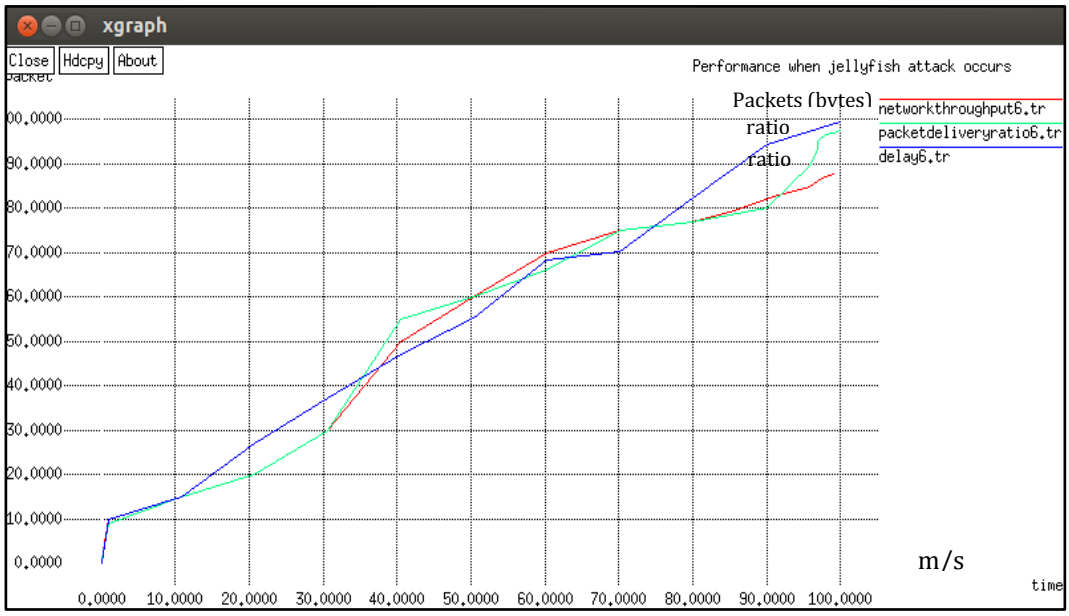

Figure 7.11. Network performance when jellyfish attacks occur.

7.2.4.3 Network performance after detecting a jellyfish attack using MrDR method

Figure 7.12 shows the improvement in network performance after detecting the jellyfish attacks and isolation of the malicious nodes from transmissions using the proposed method, for a certain time until they become trusted nodes. The network throughput and packet delivery ratio increment whereas the packet delay ratio decrements. Thus, the network performance improves as the misbehaving nodes which affect network performance are isolated from communications.

Figure 7.12. Network performance after detecting jellyfish attacks.

7.3 Evaluating the results of detecting different DoS using MrDR between the DoS attacks used

Generally, MrDR method succeeds in detecting different aforementioned DoS attacks, recording results after detecting the attack and isolating the malicious nodes. These attacks affect the performance of the network drastically. However, the performance of the proposed method is measured under different DoS attacks; wormhole attack, grayhole attack, blackhole attack and jellyfish attack. Every DoS attack has its own performance and effects on the network. Despite the fact that the mentioned DoS attacks have the same target which is to degrade the performance of the network, each attack has a different level of effectively and various degrees of difficulty of detection. Based on the experiments to detect the four types of DoS

attacks discussed in the previous section, a comparison of the different DoS attacks is shown in Figure 7.13. This comparison of the network performance after detecting the DoS attacks indicates that the MrDR method works differently, depending on the type of attack.

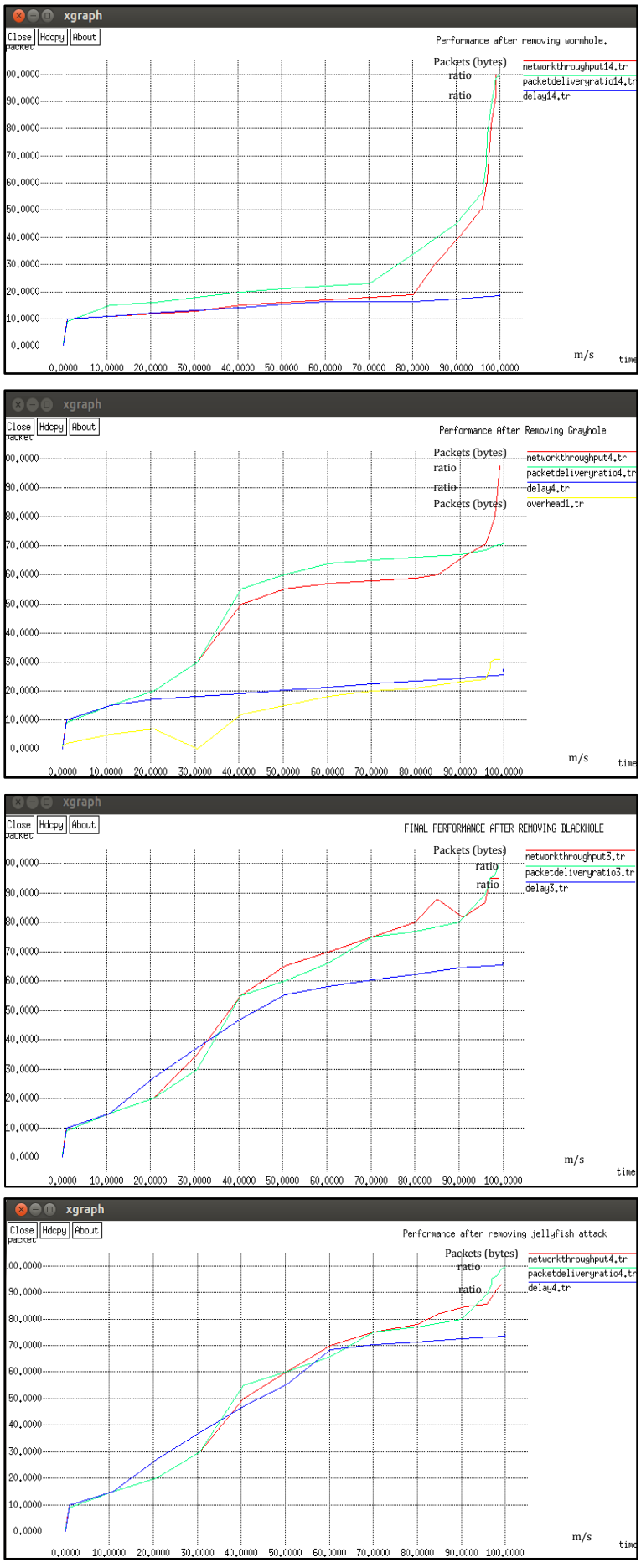

Figure 7.13. Network performance after detecting different DoS using the MrDR.

Now, the three factors measured in previous experiments: network throughput; packet delivery ratio; and packet delay ratio will be compared between all attacks in the situation of detecting the DoS attacks. The reason for this comparison is to evaluate the proposed method effectiveness under different DoS attacks that are plotted in Figure 7.14 , Figure 7.15, and Figure 7.16 respectively. The purpose of this comparison also proves that the effectiveness of the proposed method and its work varies from one attack to another.

Figure 7.14 indicates the packet delivery ratio for each DoS attack used in this experiment, after detecting the attacks using the proposed method. According to Figure 7.14 blackhole attacks have the highest value in packet delivery ratio using the proposed method compared with the other DoS attacks. However, it can be seen from the same figure that wormhole attacks gain the lowest value in the packet delivery ratio between the other DoS attacks. In addition, jellyfish attacks are in second place after blackhole attacks in terms of high level in packet delivery ratio, followed by grayhole attacks.

Further, the present findings from this graph support the hypothesis mentioned in the previous paragraph that each DoS attack responds in different degrees against the proposed method.

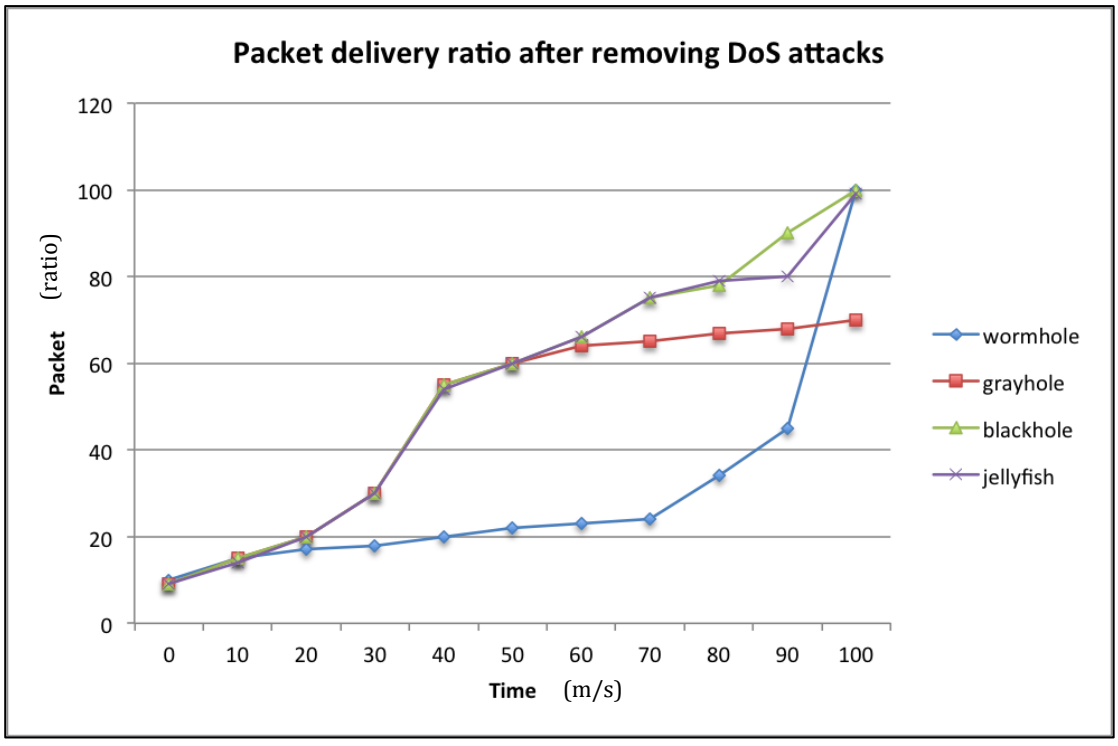

Figure 7.14. Packet delivery ratio after removing DoS attacks.

Moreover, based on Figure 7.15 below, the findings of the present study suggest that in terms of packet delay ratio the jellyfish attack gains the biggest value in packet delay ratio using the proposed method compared with the other attacks. Blackhole attack, grayhole attack, and wormhole attack are respectively followed by the jellyfish attack in this factor.

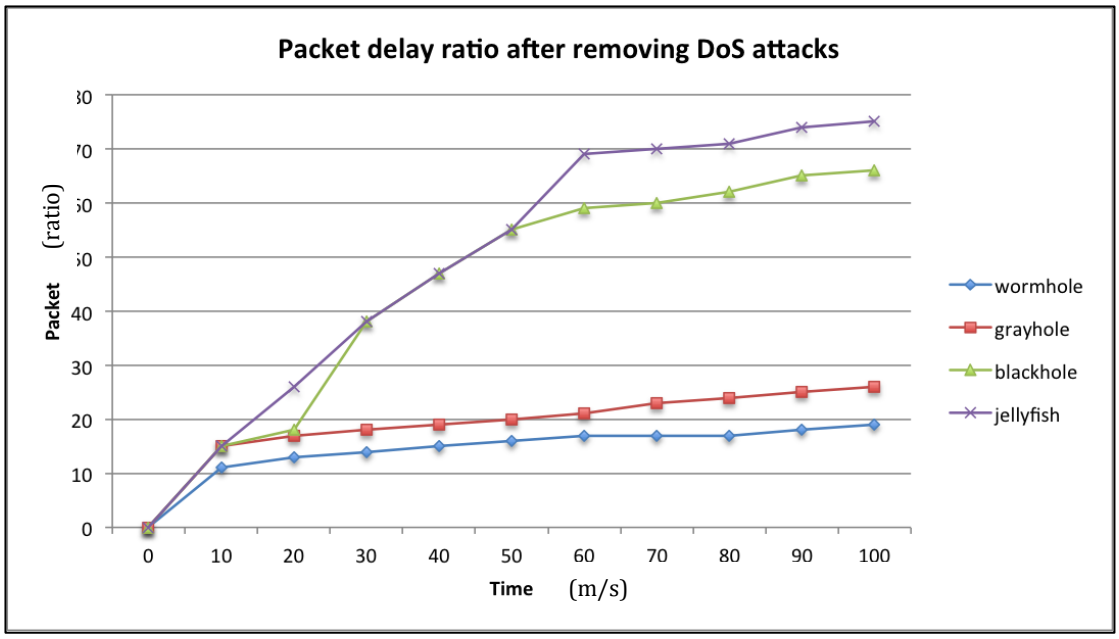

Figure 7.15. Packet delay ratio after removing DoS attacks.

Further, it is observed from Figure 7.16 that jellyfish attacks have the highest value in network throughput followed by blackhole attacks. For grayhole attacks, network throughput decreases significantly compared with jellyfish attacks and blackhole attacks. In addition, wormhole attacks receive the lowest results in this situation, as the network throughput falls considerably. Again, there is no specific reason why any attack succeeds in areas of network performance such as network throughput more than another, so it can be assumed that it is related to the attack's performance, power, and its reaction against the detection method in the network.

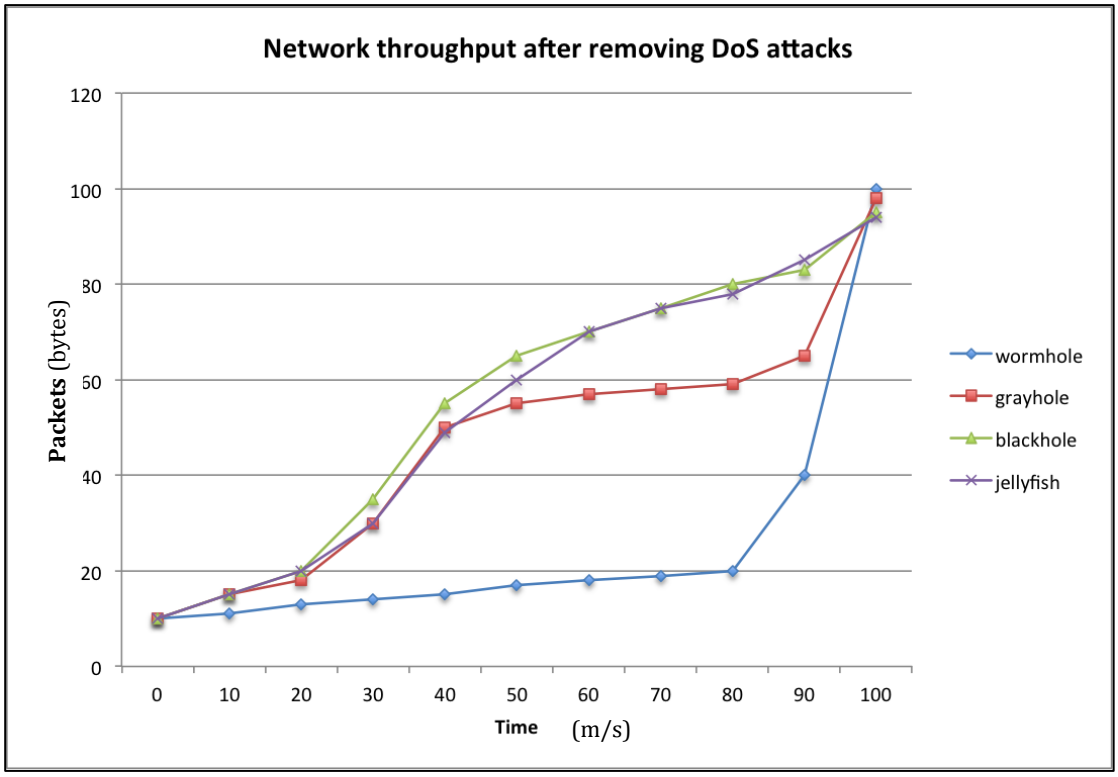

Figure 7.16. Network throughput after removing DoS attacks.

From the perspective of identifying how the best attack reacts to the proposed method and gives the highest value in both packet delivery ratio and network throughput and the lowest value in packet delay ratio can be noted from Figure 7.14 to Figure 7.16, and different DoS attacks react differently. In other words, the meaning here of the best attack, is the attack that is discovered and brought under control using the proposed method before further deterioration of the network.

In terms of packet delivery ratio and network throughput, blackhole attacks give the highest value compared to other attacks. The reason of the latter depends on the attack performance as blackhole attacks can be detected quickly compared to, for example, grayhole attacks. Since the node in grayhole attacks can convert to the normal mode and sometimes returns to the malicious mode which makes the detection process complicated compared to a clear attack such as a blackhole attack. Furthermore, jellyfish attacks rank as the second best attack in terms of both packet delivery ratio and network throughput after blackhole attacks. Jellyfish attacks can also be detected clearly with regards to its performance which delays packets for a specific time before delivering them.

Figure 7.17 shows the ranks for the all DoS attacks that are used in the experiments and their performance in the perspective in both packet delivery ratio and network throughput. Besides, wormhole attacks have the worst values in both

network throughput and packet delivery ratio, as wormhole attacks do not inject unusual volumes of traffic into the network.

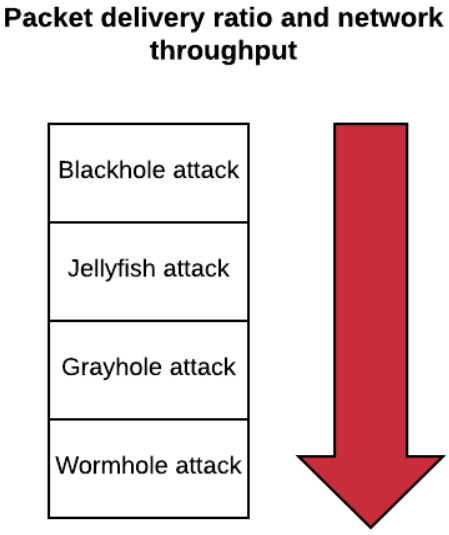

Figure 7.17. Packet delivery ratio and Network throughput in different DoS attacks.

In terms of packet delay ratio, wormhole attacks give the best results as they score the lowest packet delay ratio compared with the other attacks as it is shown in Figure 7.15. Again, Figure 7.18 illustrates the ranks of the DoS attack in terms of packet delay ratio performance ascending. The reason of these results is depends on the experiment specifications and parameters. That is to say it does not mean that attack is lowest in effectively compared with others but as previously explained this regards the parameters used in the experiment. Overall, it is agreed that all the kinds of DoS attack used in these experiments caused packet delay, but that in varying proportions.

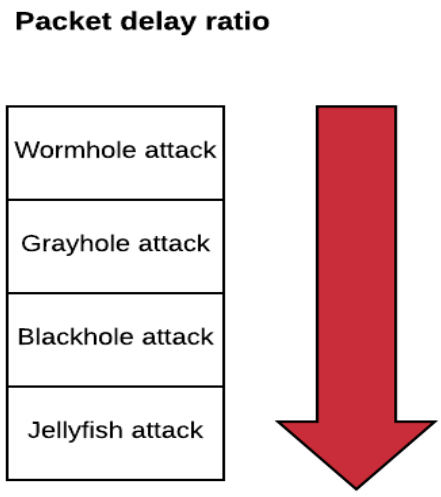

Figure 7.18. Packet delay ratio ranks in different DoS attacks.

7.4 Evaluation of the results from detecting different DoS using MrDR, with existing methods based on trust

It is important to compare the results obtained from the use of the proposed method with the existing method that is based on trust concept to detect malicious behaviours. One of the methods discussed in the literature in Chapter 4 is used for comparison with this proposed method. The trust-enhanced anonymous on-demand routing protocol (TEAP) method is based on using a trust concept (Gunasekaran and Premalatha, 2013). TEAP is based on using an anonymity concept for an informant which can identify and anonymously report abnormalities within the network. In TEAP, when a node does not send any cooperative messages then it is revealed as an abnormal user to other users. Furthermore, when many claims are sent by a user, it is also termed as a misbehaving node. Moreover, TEAP is designed in terms of broadcast with trapdoor information that is used to detect misbehaving activities anonymously within the network.

TEAP is used for comparison with the proposed method in two aspects: packet delivery ratio and network overhead. In this comparison, grayhole attacks are used as an example to compare the results of the performance of the proposed method with TEAP.

In the aspects of packet delivery ratio after detecting malicious activities is shown in Figure 7.19. As can be seen, the performance of the MrDR in detecting the DoS attacks, precisely grayhole attacks in this case, is higher in the aspect of packet

delivery ratio than TEAP performance after removing malicious nodes from communications. Accordingly, the proposed method or MrDR outperforms TEAP in this aspect.

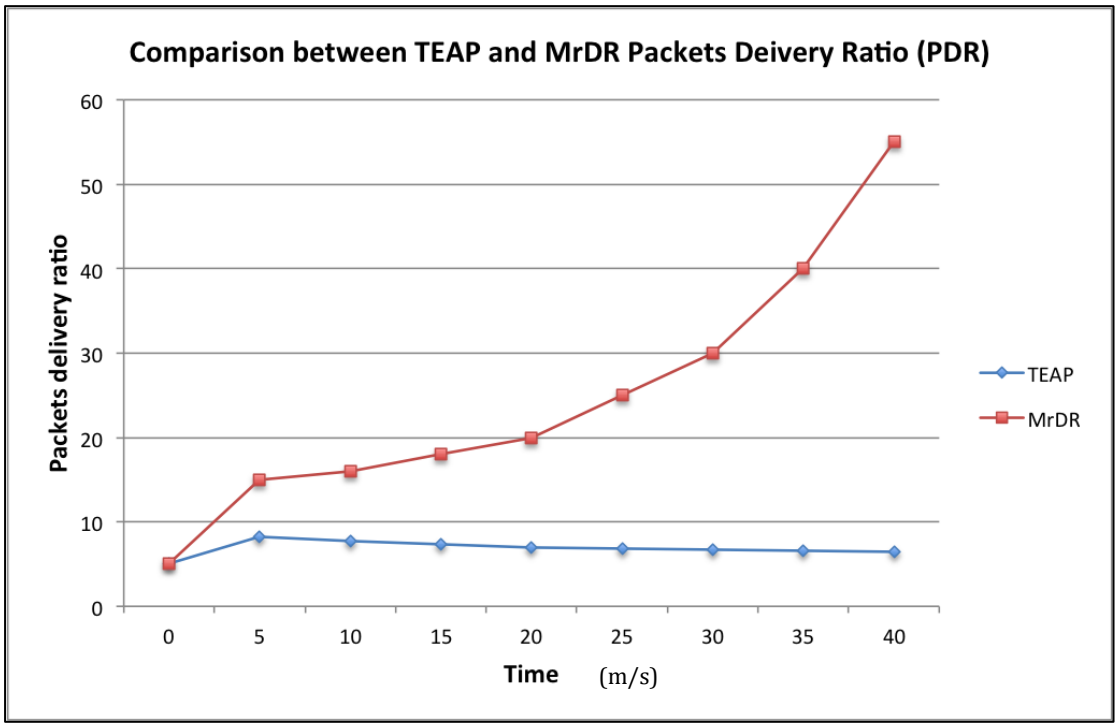

Figure 7.19. Comparison between TEAP and MrDR based on PDR.

In brief, TEAP considers a node as misbehaving when it does not send cooperative messages to other nodes. In addition, in TEAP when many claims are received about a specific node being abnormal then is also considered a malicious node. However, in MrDR different trust values need to be considered to identify the node as normal or misbehaving. Also, in the proposed method, there is rehabilitation to rehab the misbehaving node in order to use it in further communications. Thus, as it is assumed before in MrDR, the trust value is something temporary and short-lived and needs to be calculated every specific time.

Figure 7.20 shows the differences between the two methods when considering network overhead. In this case, TEAP consumes energy and exhausts network resources more than MrDR. Therefore, while both the proposed method and TEAP consume network resources, from findings MrDR does so on a smaller scale which does not affect the network.

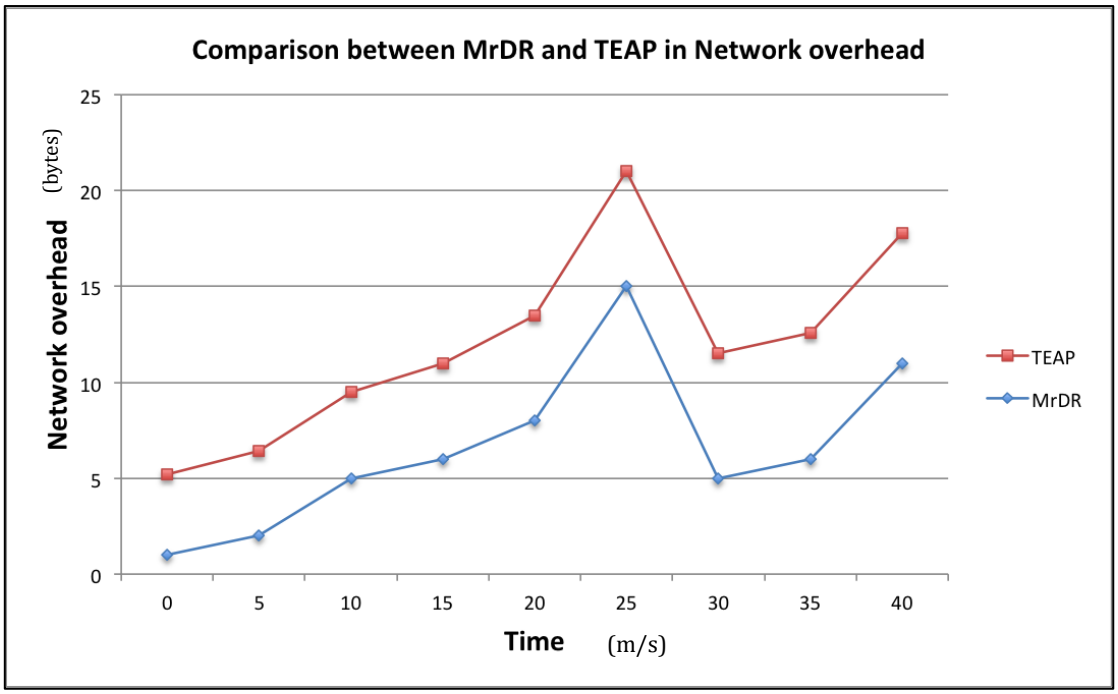

Figure 7.20. Comparison between TEAP and MrDR based on network overhead.

7.5 Results of detecting DoS attack on MM - Two independent configured MANETs

The experiment that addressed the detection of grayhole attacks when two MANETs merged is explained in detail in the previous chapter. Subsequently, in this chapter, the network performance in the three aspects: packet delivery ratio; network throughput; and packet delay ratio will be measured before and after merging. The reason for these measurements is to demonstrate the performance and effectiveness of the proposed method in this specific situation. MANET with its specifications such as dynamic topology and non-fixed infrastructure is prone to merging and even partitioning. These measurements take place three times before merging and three times after merging as it is shown in the timeline of experiment scenario in Figure 6.16 in Chapter 6. This experiment shows how two independent MANETs, which are clustered can merge successfully and detect DoS attacks.

Figure 7.21 measures the network performance in the normal network mode from initiating the simulation when there are no attacks. The findings highlight that, in a normal situation where there is no attack, the network performance is as expected when delivering packets, which enhances the network throughput with no

packet delay. It is apparent from Figure 7.21 that the network throughput and packet delay ratio increase, whereas the packet delay ratio diminishes.

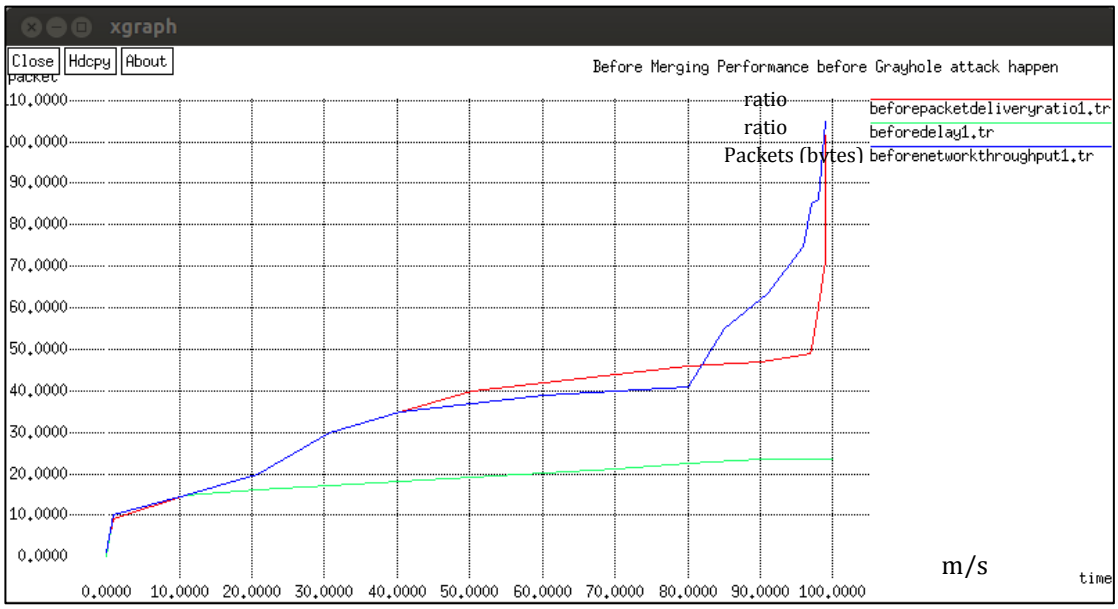

Figure 7.21. Network performance before the occurrence of grayhole attack (Pre-merging).

As explained in the previous chapter in (Figure 6.16), at attack mode from starting the simulation, two grayhole attack nodes occur. Obviously, grayhole attacks harm the network and affect network communications. In Figure 7.22, network performance is measured. In this situation, there is a clear trend of decrease in both network throughput and the packet delivery ratio with regards to the occurrence of grayhole attacks, whereas the packet delay ratio and network overhead increase significantly.

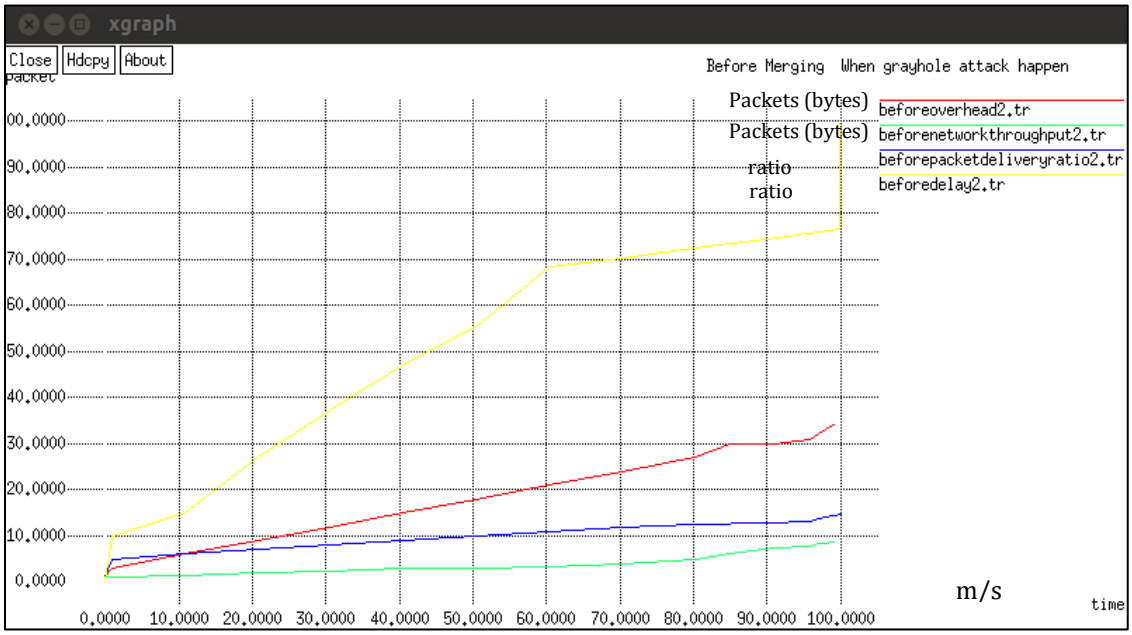

Figure 7.22. Network performance under grayhole attack (Pre- merging).

Moreover, at the detection stage from (Figure 6.16), the proposed method detects the DoS attack and temporally isolates the grayhole nodes from transmission, until their TTSV changes from 0 to 1. To put it another way, nodes become trusted. Figure 7.23 shows the network performance after detecting grayhole attack nodes. The findings suggest that the network throughput and the packet delivery ratio rise sharply, whereas the network overhead and the packet delay ratio drop suddenly. On account of isolating the misbehaving nodes which cause grayhole attacks, the normal nodes will perform the expected missions and deliver packets to the intended nodes. Thus, the network throughput and packet delivery ratio increase whereas the packet delay ratio and network overhead decrease.

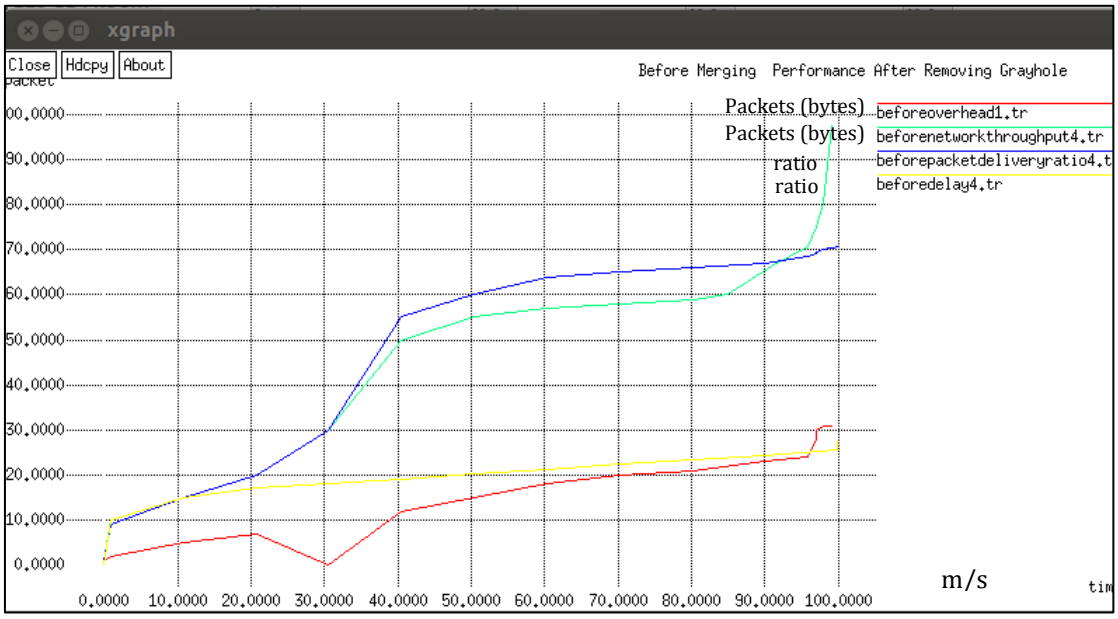

Figure 7.23. Network performance after removing grayhole attacks (Pre-merging).

In addition, as illustrated in the previous chapter, when the grayhole attacks are detected, a new MANET that consists of 30 nodes appears and wants to merge with MANET1 to form a larger, single MANET as it is shown in the experiment timeline in Figure 6.16 in Chapter 6. In order to achieve this, a centralised trust concept is used in this experiment. One trusted node from each network starts negotiations in order to complete the merging process and detect any further DoS attacks.

At the end of minute five, specifically in the detection phase as the two networks merge (See Figure 6.16 in Chapter 6). Figure 7.24 shows the network performance for this larger MANET when there are no DoS attacks. Therefore, both network throughput and packet delivery ratio are high, whereas the network overhead and packet delay ratio are low. These results stem from the absence of grayhole attacks which considerably diminish the performance of the network.

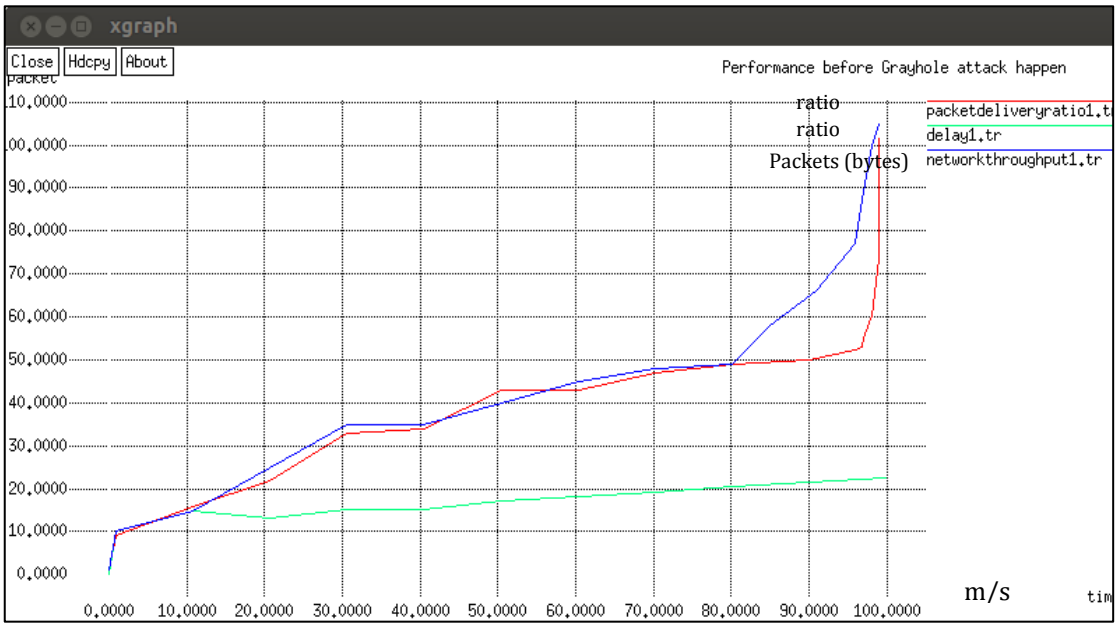

Figure 7.24. Network performance before DoS attack (Post-merging).

After merging is complete as it shown in the timeline in Figure 6.16 in Chapter 6, grayhole attacks occur in two nodes as explained in the previous chapter. Figure 7.25 shows the network performance in this situation, where the network throughput and packet delivery ratio decrease dramatically due to the occurrence of grayhole attacks which drop packets. Thence, the packet delay ratio which increases network overhead also rises considerably.

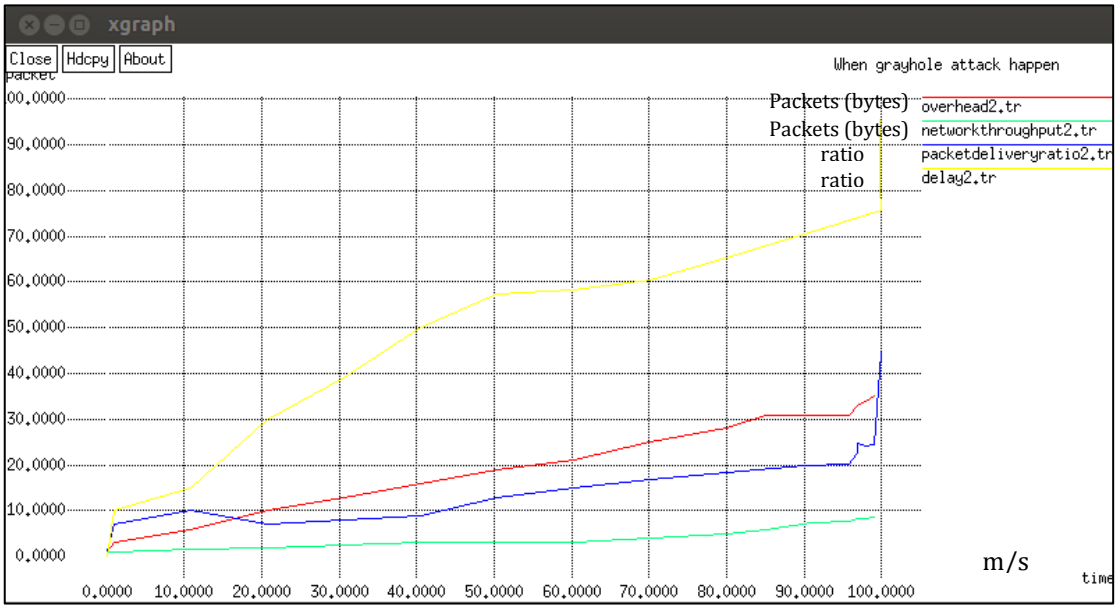

Figure 7.25. Network performance under grayhole attacks (Post-merging).

At the next detection phase (See Figure 6.16 In Chapter 6), grayhole nodes are detected using the proposed MUMrDR method. Figure 7.26 demonstrates the network performance after handling grayhole attacks. The packet delivery ratio and network throughput increment considerably and the packet delay ratio and network overhead decrement drastically. To put it another way, after detecting the misbehaving nodes, the other normal nodes perform the normal activities such as delivering packet to the intended destination. Thus, network performance is again enhanced.

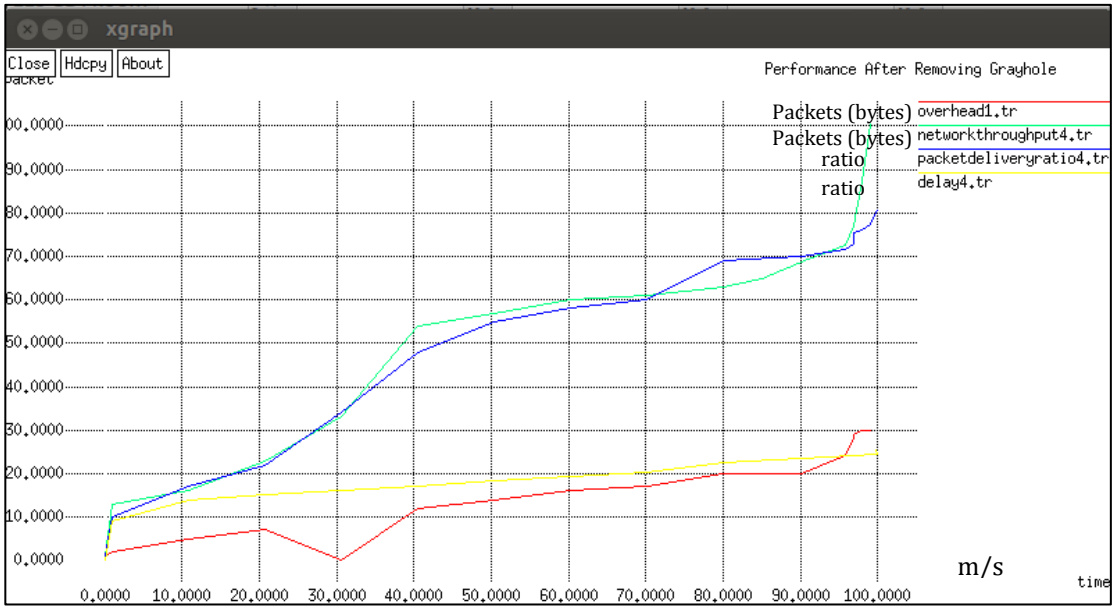

Figure 7.26. Network performance after removing grayhole attacks (Post- merging).

7.6 Results of the detection of DoS attacks on MM - Four independently configured MANETs

In the previous chapter, the experiment of merging four MANETs is explained in detail. Moreover, different types of DoS attacks occur in each MANET pre- and post-merging when it becomes one larger MANET with 50 nodes.

At the beginning the experiment, precisely in the normal network mode according to the experiment timeline illustrated in the previous chapter (See Figure 6.23 in Chapter 6), as no attacks existed in any MANET, the network performance is normal. Normality means that the nodes perform their tasks as they are expected to in terms of sending and receiving packets. As explained in Chapter 3, nodes in MANET act as a router and a host when sending and receiving packets. Figure 7.27 shows that network throughput and packet delivery ratio are at their highest points

because nodes send and receive packets without hindrance as there is no attack occurring, so the packet delay ratio is at its lowest.

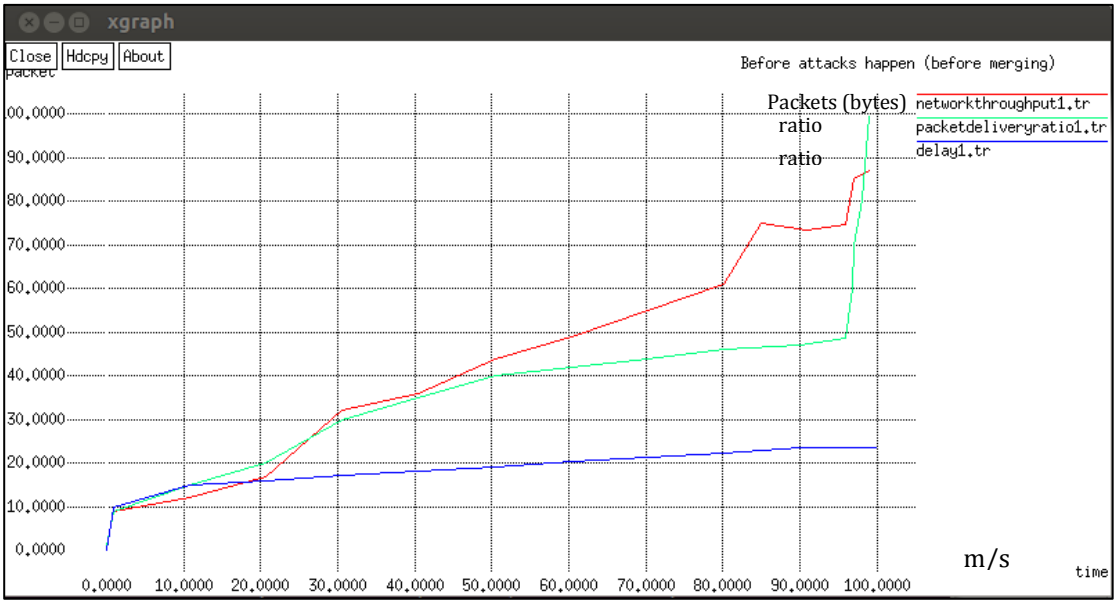

Figure 7.27. Network performance before the occurrence of DoS attacks (Pre- merging).

Following this, based on the timeline shown in Figure 6.23 in Chapter 6, different types of DoS attacks occur in each MANET prior to merging. Figure 7.28 illustrates the degradation in network performance due to these DoS attacks: grayhole attack; jellyfish attack; and wormhole attack. A clear decline occurs in both network throughput and packet delivery ratio, as well as an increasing trend in packet delay ratio.

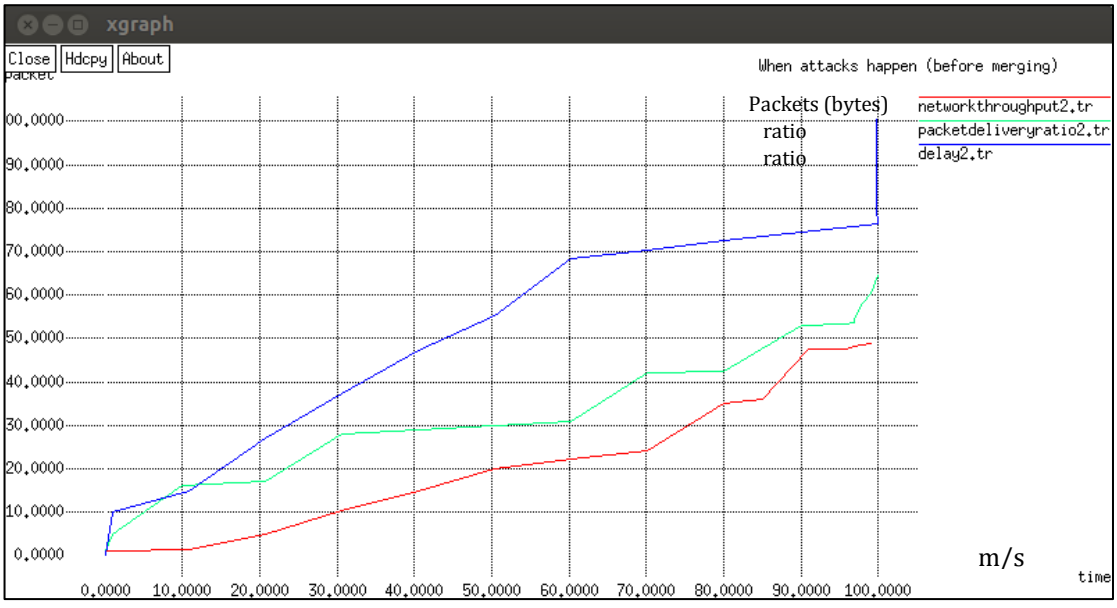

Figure 7.28. Network performance when DoS attacks occur (Pre-merging).

At the minute three mark which is the detection phase according to Figure 6.23 in Chapter 6, the complete detection of all DoS attack nodes is performed to isolate all malicious or selfish nodes until their trust values change from 0 (untrusted) to 1 (trusted) under the proposed method. Figure 7.29 shows the improvements in the network performance after detecting DoS attacks in the networks.

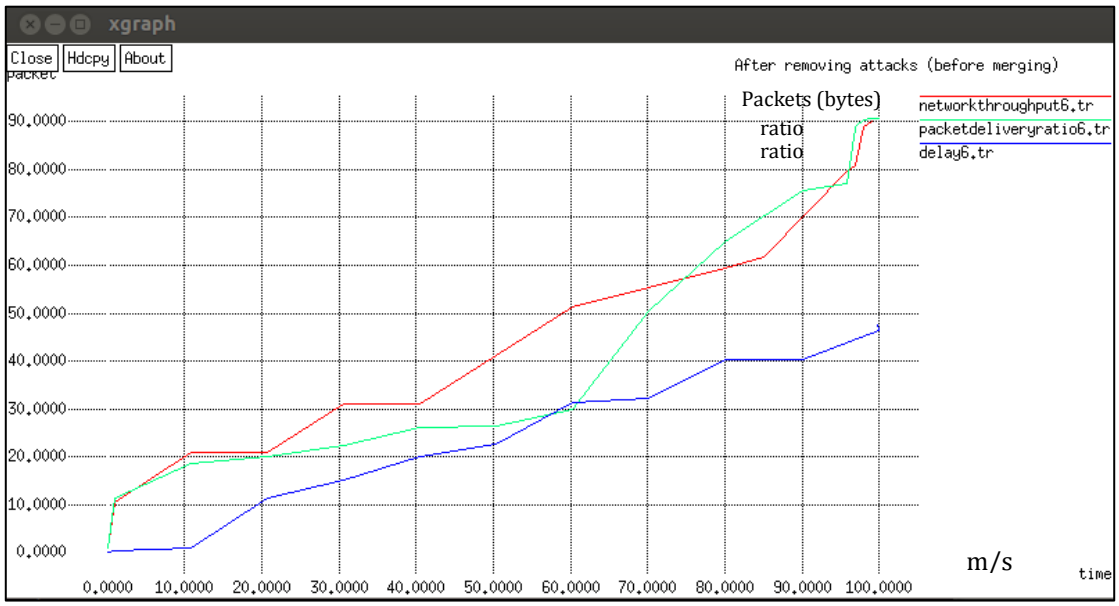

Figure 7.29. Network performance after detecting DoS attacks (Pre-merging).

At the middle of minute three (See Figure 6.23 in Chapter 6), the four MANETs start negotiations in order to merge and to become a single, larger MANET, based on using decentralised trust concept which is explained early in Chapter 6. At the middle of minute four, (See Figure 6.23 in Chapter 6) MANET 2 starts merging with MANET 1 and MANET 3. Figure 7.30 shows the network performance of the MANETs when there are no DoS attacks. The findings show how the network performance is positive. As explained before, due to the absence of DoS attacks the nodes perform their tasks as usual in sending and receiving packets.

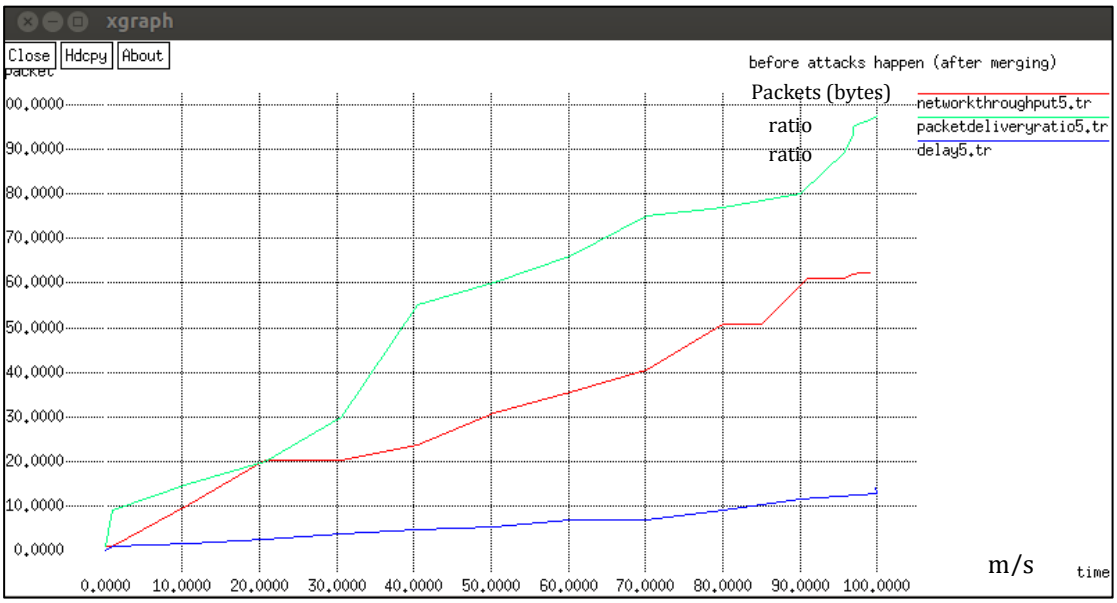

Figure 7.30. Network performance before DoS attacks occur (after start merging process).

At the beginning of minute five, MANET 1, MANET 2 and MANET 3 merge. Many DoS attacks occur: jellyfish attacks; blackhole attacks; grayhole attacks; and wormhole attacks in this new MANET, as well as in MANET 4, which nearly merges with the larger MANET. Figure 7.31 demonstrates the network performance with the occurrence of the DoS attacks. Data in Figure 7.31 shows the decrease in the network throughput and packet delivery ratio, with an increase in packet delay ratio. In fact these results are expected in the presence of the different DoS attacks, which cause packet delays and also reduce the network throughput and packet delivery level.

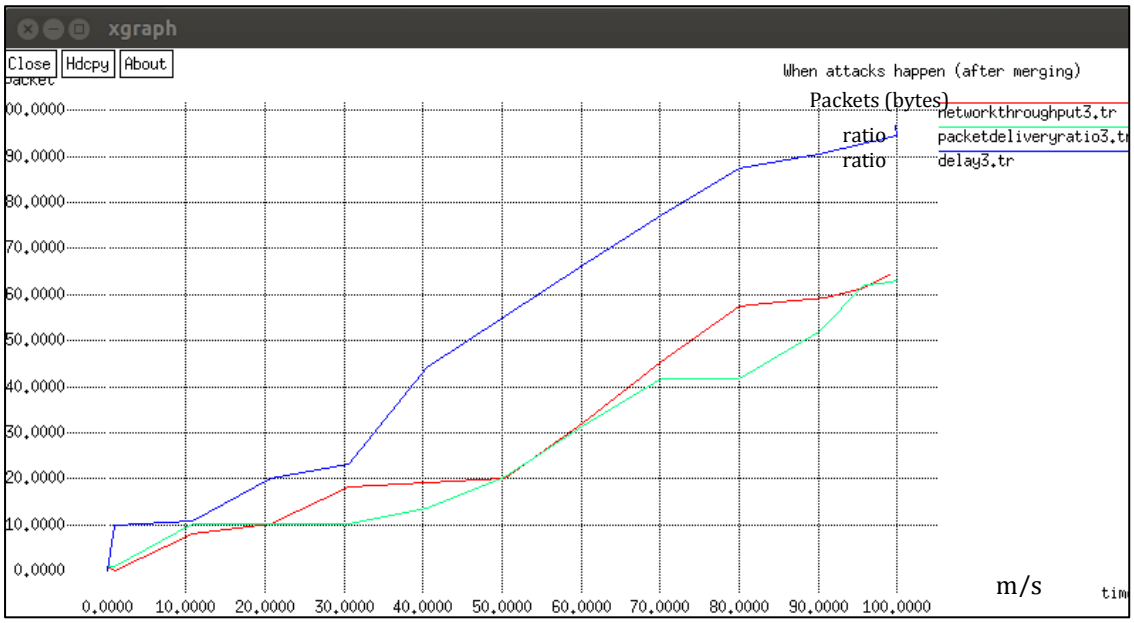

Figure 7.31. Network performance after DoS attacks exist (Post-merging).

In minute five (See timeline Figure 6.23 in Chapter 6), MANET 4 starts negotiations to merge with the big MANET based on the decentralised trust concept. Furthermore, DoS attacks: blackhole attacks; grayhole attacks; and wormhole attacks occur again whilst the merging is in process, and all DoS are detected in the middle of minute five, as discussed in Chapter 6. At the beginning of minute six, the merging process is completed and the four MANETs form a single larger MANET. Figure 7.32 shows that the network performance is normal after merging as no attack occurs and the network in the normal mode. Thence, the nodes perform their tasks without any problems. The packet delay ratio decreases rapidly, whereas network throughput and the packet delivery ratio increase considerably.

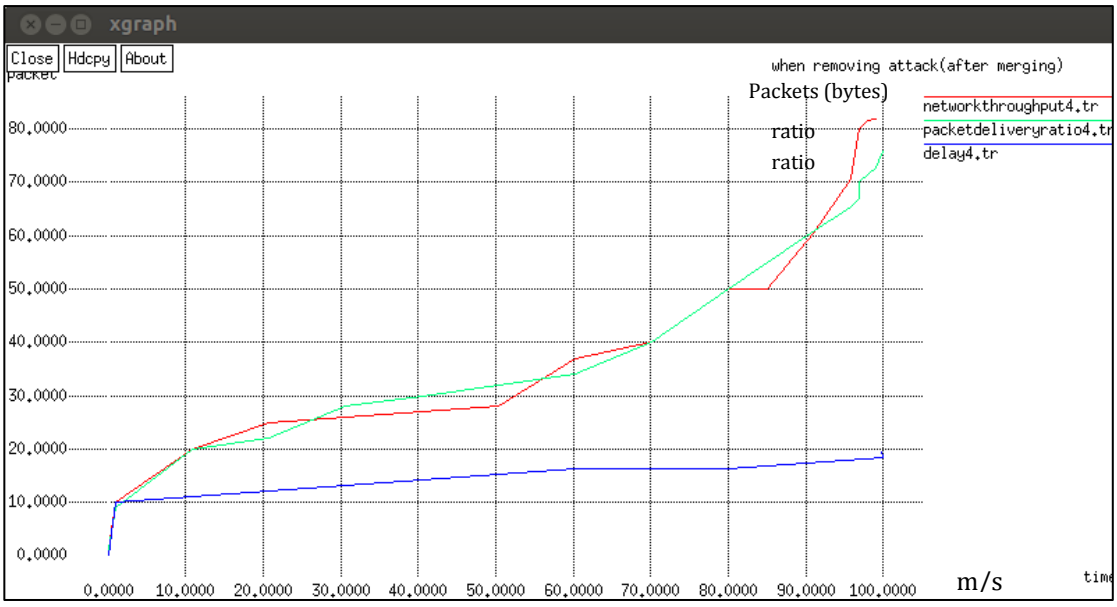

Figure 7.32. Network performance after detecting DoS attacks (Post-merging).

7.7 Discussion

The proposed method aims to detect DoS attacks in both SM and MM. due to the nature of MANET's non-fixed infrastructure, dynamic topology, and lack of central administration, many aspects need to be considered. The MrDR method is built on calculating various trust values in order to calculate the total trust value or TTSV for each node.

The first experiments are applied to detect four types of DoS attacks: blackhole attacks; wormhole attacks; grayhole attacks; and jellyfish attacks in SM. In order to evaluate the performance of the proposed method and its power to combat these attacks, three aspects are measured: packet delivery ratio; network throughput;

and packet delay ratio. These three aspects are calculated in three scenarios: in the normal network mode; attack phase; and detection phase. Thus, the performance of the proposed method to detect the DoS attack would emphasise the importance and efficiency of it. The MrDR helps to establish trust between nodes and apply central administration in decentralised networks such as MANET. The findings from the simulation indicate the success of the proposed method in detecting different DoS attacks in SM, as explained in previous sections.

However, as has been explained, in MANET the nodes move frequently into and out of the network. Thus, the chance of networks either merging or partitioning exists. For this purpose, the MUMrDR is used to help merging multiple MANET using the MrDR method which can also guarantee that in this certain scenario, no DoS attacks will affect the network. Two experiments are conducted to investigate the effectiveness of this proposed method in MM. the first experiment uses the centralised trust concept with MUMrDR to complete the merging process. This means one trusted node from each network will help to apply the proposed method and complete the merging operation smoothly. Furthermore, the centralised trust concept will ensure that many issues are handled in this situation such as no IP address conflict, MANET IDs; and assigning IP addresses if required. Grayhole attacks are used as an example in this experiment and detected using the proposed method. The results of this simulation prove the importance of this method in this critical situation. Thus, this study contributes to the MANET field of knowledge by addressing this critical situation and showing that it is possible to protect the network in the merging process.

Also, the last experiment is also applied to the MUMrDR to detect different types of DoS attacks when four MANETs merge using the decentralised trust concept. The decentralised trust concept will enable all nodes to cooperate when merging. However, if the node is untrusted and gives incorrect information then it will be isolated from communication until the merging process is complete or it becomes a trusted node. The findings from this simulation again confirm the importance of this method to help merging in MM.

The detection of DoS attacks when the MANETs are merging increases the level of security between nodes, as they can exchange correct information about their immediate nodes in each MANET. In addition, IP address conflict is also an

important issue which is considered, as using the level of security between nodes, they can exchange correct information about their immediate nodes in each MANET. These findings provide evidence that the proposed method succeeds in an increase in the network performance and a decrease in packets delay ratio, which is absolutely appropriate in an environment such as MANET with limited resources and energy.

To knowledge, this is the first study to deal with and examine this critical situation of detecting DoS attacks in MM. In addition, when using the proposed method on SM it is also a unique method which utilises different aspects to calculate the trust value which is temporal and in binary mode trusted and untrusted. Thus, in SM the proposed method is compared with a method which uses the trust concept to identify misbehaving activities, but in MM the originality of this solution lies in the fact that no study to date has examined this situation.

7.8 Chapter summary

This chapter presents the results of the three experiments, which are explained in the previous chapter. The first experiment is on SM and four DoS attacks are tested to evaluate the performance of the proposed method. The second experiment tests the proposed method in a situation where two MANETs merge using the centralised trust concept, to determine how the detection of DoS attack will be effective in this situation. Finally, the third experiment tests the performance of the proposed method when four independently configured MANETs merge and how to control DoS attacks in this complicated scenario using the decentralised trust concept. The findings of this study emphsise the importance and effectivness of this study, which give positive results. Positive means that the network performance increases while packet delay ratio and network overhead decrease drastically. Further, it is notable that the current findings add a novel view to the literature on detecting DoS attacks in situations of both SM and MM. The next chapter concludes the thesis, outlines strengths and limitations of the proposed method, and suggests further developments.

Chapter 8: Conclusions and Future Work

This chapter draws on work explained in the previous chapters. Here, the proposed MrDR method is used to detect DoS attacks in many scenarios and using many types of DoS attacks. The main aim of the proposed method is to detect DoS attacks in MANET. Trust value is the main concept of the proposed method. Three main experiments are carried out to evaluate the effectiveness of this method in both SM and MM. This chapter highlights the overall scope of the research, revisits the objectives, presents the significance of the findings and limitations of the study, and finally presents ideas for future work.

8.1 Review the research objectives

There is undoubtedly a pressing need to use devices to communicate and exchange data to perform duties and tasks. IoT with MANET can be used in many sectors, such as healthcare, where devices are joined wirelessly in mobile environments. For example, mobile nurse technology within the hospital using smartphones and tablets enables hospitals to deliver bedside care. Rather than relying on computers and landline phones to access the health information of patients and communicate with doctors and nurses, access to these MANET solutions helps the hospital to deliver immediate care.

When reviewing the research objectives presented in Chapter 1, the focus of this research is the detection of DoS attacks in both SM and MM. Thus, the entire development is to achieve this aim. Each objective will be reviewed and connected to the research in order to understand how this specific objective has been achieved successfully.

1. *To study and understand the nature of MANET and its security challenges and vulnerabilities. The research will focus on DoS attacks in particular in order to*

determine how they occur, the various types, and the threat they pose to MANET architecture, resources, and users.

MANET is an autonomous group, or collection, of mobile nodes. Each node in this network is considered to be both a host and a router in sending and receiving packets. Nodes can be any kind of device which has an available wireless connection, including mobile smartphones and mobile tablets. Further, MANET is a self-configured, multi-hop network, with a non-fixed infrastructure, spontaneous network, dynamic topology, and self-maintenance capabilities; it does not require central administration to control other nodes within the network. In the MANET network, nodes communicate with others in radio range via wireless links; thus, due to the easy setup of this kind of network, the MANET system has proved useful, and is used across a variety of sectors including cafes, airports, conferences, emergency relief situations, and the military arena.

However, despite the fact that all networks, whether wired or wireless, are vulnerable to attacks, the inherent nature of wireless networks (like MANET) makes them more vulnerable than their wired counterparts. Because of their characteristics, MANET nodes are freely able to frequently join, and leave a network. Further, because the topology changes dynamically in MANET, this increases the range of challenges and risks, including the unpredictable availability of resources, and the occurrence of multiple kinds of attack, as there are no administrator points which can monitor the whole network. In addition, power limitations also constrain MANET as energy is expended in both packet transmission and reception. Moreover, due to the dynamic topology of nodes, they have a high probability of being compromised by intruders. Many attacks can be launched, and exist in MANET including eavesdropping and DoS attacks.

A DoS attack is an attack which aims to deprive, or prevent, legitimate users from accessing services, or resources, such as a computer system, web service, or website. The attack continues over a specific time, determined by the intruder, even if detected. A DDoS attack is a distributed DoS attack in which the attacker floods the victim's network with a huge number of packets. Subsequently, DoS attacks affect the efficacy of security services as a network, and its defences, become unavailable to authenticated users as a result. Overall, many kinds of DoS attack can occur in MANET and their behaviour can be malicious or selfish.

A DoS attack is defined as a complicated attack on the basis of three main factors. First, there is no detection benchmark, or even baseline rule, which can be used to identify this attack in its different forms. As each type of DoS attack has various criteria and performance, each requires the use of several methods to be revealed. Second, there is a great deal of software available online to launch this kind of attack and thus, predominantly, these can be initiated easily by inexpert users. Third, there is a limited amount of attack incident details available that can be used to help conquer attacks in the future. Thus, although MANET networks are vulnerable to DoS attacks, there is no software yet available in the industry, or on the market, which can be used to completely solve this problem.

2. *To critically evaluate existing countermeasures used to identify DoS attacks on MANET and identify their advantages and disadvantages. This will highlight any flaws in the existing detection methods.*

In Chapter 4, a comprehensive study illustrates the existing methods of detecting DoS attacks in MANET. Traditional methods such as firewalls and methods which use the trust concept are also discussed. In addition, advantages and disadvantages are also defined for each method in order to design a new method which avoids such limitations. Moreover, some methods which show the assigning of the IP address in MANET are explained.

3. *To design and implement a novel method for the early identification of DoS attacks in both SM and MM, acknowledging the disadvantages of existing methods.*

In this thesis, the MrDR method is proposed for use to detect DoS attacks in the MANET environment. This method is based on the use of trust values, which are based on the calculation of multiple trust values, and can help to enforce cooperation between nodes in multi-hops networks such as MANET. The trust concept is used to calculate the Total Trust Value (TTSV) for each node in the network, based on a binary system with two values of trust; 1= trusted, or 0= untrustworthy. Because of the dynamic topology of MANET, each trust value is temporary, and the TTSV of each node will be calculated again every time as outlined in Chapter 5. Moreover,

this proposed method is based on three stages, each one is responsible for calculating one of the factors in order to calculate the TTSV.

The first stage of this process is the monitoring phase where the entire network is monitored and any misbehaviour is detected. In addition, two types of trust are calculated at this stage; the Accomplishment Trust Value (ATV), and the Reputation Trust Value (RTV). Of these, the ATV determines whether, or not, a node sends required packets to intended nodes, or destinations, and whether, or not, it received confirmation from the destination that these are received. If this task is confirmed then ATV=1, otherwise ATV= 0.

The RTV is used to determine whether, or not, a node has been responsible for any misbehaviour, including dropping packets or launching a DoS attack. Of these outcomes, the punishment attached to packet dropping is smaller than either packet fabrication or DoS attack because it might not always happen because of misbehaviour. Packet dropping can also occur because of power failure, network congestion, or the nature of the MANET network having limited energy. Thus, RTV is set to 0 automatically and the node becomes malicious if it fabricates packets, misroutes them, or launches DoS attacks. If the node drops packets for the first time, then RTV=0.5, but if this happens for a second time, then RTV= 0.25. Finally, if a node drops packets for a third successive time, then RTV=0, and it is defined as malicious. However, if a node behaves normally and does not misbehave, then RTV remains 1.

The second stage of this process is the detection phase, which aims to detect misbehaving nodes. To achieve this, an Honesty Trust Value (HTV) is calculated to assess the relative trustworthiness of nodes. In a given situation, nodes exchange their trust values and if this information matches with that from the majority of nodes, then the HTV equals 1. If not, HTV equals 0. In addition, the TTSV is calculated at this stage can have just two values; 0, untrustworthy, and 1, trusted. Note that trust values in this method are short-lived and non-transitive.

Rehabilitation is considered in this approach when a node has misbehaved three successive times, and thus calculation of the TTSV takes a longer time to conserve energy in the network.

4. *To evaluate the proposed novel method in an effort to establish its strengths and weaknesses, particularly with respect to SM, under various types of DoS attack.*

This proposed method is applied on SM in order to detect four kinds of DoS attacks; wormhole, blackhole, grayhole, and jellyfish attacks. Results support the effectiveness of this proposed method as network performance improves considerably. Three factors are measured to detect each kind of DoS attack; network throughput, packet delivery ratio, and packet delay ratio. These factors are measured three times in the experiment; before the attack occurs, when the attack occurs, and after the attack has been detected or the misbehaving node is isolated. Note that isolation of the DoS attacked node will be temporary until the TTSV changes from 0 to 1 and a node returns to trusted status.

5. *To compare the performance of the proposed method with existing methods using the trust concept to detect DoS attacks on SM.*

In fact, there is no existing method based on using the trust value as a binary. Indeed, comparisons between the detection of DoS using MrDR on SM are evaluated in light of different attacks, and against the types of detection explained in detail in Chapter 4 (TEAP). The MrDR method manages to outperform TEAP, as shown in Chapter 7. This comparison confirms the success of the proposed method in detecting examples of misbehaviour when compared to TEAP.

6. *To use the trust concept to assign IP addresses on MM.*

The dynamic topology of MANET means it likely can be merged with other networks, and MUMrDR is used to detect DoS attacks in MM. In this situation, two main experiments are done to test the performance of the proposed method; merging two MANETs, and merging four MANETs. In this situation, a number of aspects need to be considered including IP configuration, and the lack of IP address conflict. A proposed protocol to assign IP address to the new node is explained in detail in Chapter 5. This protocol guarantees that unused IP addresses will be reassigned in future to a new node or any other node needing one. IP address conflicts need to be managed during MANET merging. Two methods are used for merging: the centralised trust concept and decentralised trust concept. In the centralised trust concept, which is used when two MANETs merge, a trusted node from each MANET would be used as a manager which is responsible for completing the merging process. In addition, the node's responsibilities include checking any IP

address conflicts and assigning IP addresses when a node needs one. However, in the decentralised trust concept which is used in the last experiment when four MANETs merge, all nodes participate in completing the merging process whether they are trusted or not. The reason for this is that misbehaving nodes in some DoS attacks do not behave maliciously all the time and can sometimes be converted into a normal mode. Thus, even if the node is untrusted it will participate in the merging process unless it gives incorrect information then it will be isolated until the merging process is complete or it becomes a trusted node.

7. *To test the proposed method in MM where two MANETs merge, and in MM where more than two MANETs merge. This is the first attempt to use the trust concept to detect DoS attacks during the merger of MM.*

Thus, the first experiment on MM is done in the scenario where two MANETs merge to look at how the detection of a DoS attack, such as a grayhole attack, can be undertaken. In this experiment, a centralised trust concept is used as one trusted node from each MANET helped to check IP addresses, detect any IP address conflicts, assign IP addresses, and complete the merging process. Results of this investigation show that this proposed method is successful in detecting DoS attacks in this critical situation, and how the trust nodes from each network complete the merging process. Network performance is high in terms of both throughput and packet delivery ratio, while the packet delay ratio and network overhead are low, as appropriate in MANET.

Further, MUMrDR is also tested when four MANETs merge with the occurrence of different DoS attacks. In this experiment, a decentralised trust concept is used as all nodes participate to complete the process. It is notable that even malicious nodes can participate in this merging process if they give correct information. This is because some DoS attacks such as grayhole attacks do not behave maliciously all the time as they can convert to a normal mode and behave ordinarily. However, if these grayhole nodes give incorrect information such as false vacant IP addresses, these untrustworthy nodes will not be able to assign IP addresses to others until the merging process is complete, or until their TTSV becomes equal to 1. The results of this experiment corroborate the effectiveness of

the proposed method in detecting the four types of DoS attack and network performance is positive.

In sum, this study gives positive results for defence against DoS attacks despite all the challenges of the MANET environment. The findings of this study make several contributions to the current literature, as described in Chapter 1. However, it is also important to mention that MUMrDR on MM does not compared to existing work as there is no work that presently discusses this point. This study provides evidence of the contribution to the detection of DoS attacks on MM in merging situations.

8.2 Strengths and limitations of the study

The proposed method helps to detect DoS attacks in both SM and MM. Due to the nature of MANET such as dynamic topology and nodes being able to join or leave the network frequently, the proposed method is appropriate in many aspects.

First, the trust value is in binary mode so it can be identified whether the node can be trusted or not, which saves the energy power of nodes. Thus, trusted nodes can perform tasks such as sending packets and temporarily isolating the untrusted nodes.

Second, the rehabilitation of nodes helps to encourage nodes to cooperate in the communications. As explained before, the MANET is a temporal network so the node condition can change from trusted to untrusted and vice versa.

Third, again the nodes in MANET have limited energy. Thence, any node which is identified as untrusted three successive times will be isolated longer from communications and sent to the blacklist until it becomes a trusted node.

Fourth, the simulation results from testing the proposed method in both SM and MM give positive results in network performance which prove the efficacy of these methods. Furthermore, Our system is tested in (Chalamasetty et al., 2016). They present the Supervisory Control And Data Acquisition (SCADA) system, which monitors and controls power system operations. It is intended for utilities' ad-hoc networks in residential power distribution networks to enable the collection of data from smart meters. Our method (MrDR) is used to protect the network from cyber-attacks and they confirm regards the experiments results that the proposed method is efficient and effective in detecting DoS attacks.

Although the proposed method succeeds in detecting DoS attacks in both SM and MM, there are some limitations in certain scenarios. When the novel method is designed and implemented it takes into account the avoidance of any obstacles or limitations in existing methods. The proposed method is based on using trust, and exchanges trust values between nodes. In the rare but possible scenario that all nodes in the network are malicious, the proposed method would not work effectively as the majority of nodes in this situation will give incorrect information about trust values and adversely affect the method. However, some nodes can behave normally but convert to a malicious mode occasionally such as in grayhole attacks. Thus, it is dependent on the DoS attack type whether the method can succeed and give correct information even when the majority of nodes are untrusted.

8.3 Future work

This thesis attempts to overcome some of the limitations of previous work, and build a new method to detect DoS attacks in the MANET environment. As a result, this research has thrown up many questions that are in need of further investigation; both further investigation, and experimentation, can now be done on both SM and MM. In the case of SM, the number of nodes can be increased to test the performance of the method proposed here in this situation, while other kinds of DoS attacks can also be used to compare the results of the proposed method in each case. Additionally, in the MM situation, there is a need to explore the performance of the proposed method in cases where many MANETs merge (i.e., ten, 20, or even more).

Moreover, in the case of MM, the partition scenario needs further consideration. Given high mobility, there is a high probability that a network will split into many smaller ones, and partition occurs when some nodes move out of network range. An additional study could assess the performance of the method proposed here in this critical situation. In addition, in further research it might be beneficial to use the proposed method for the detection of other kinds of attacks, including fabrication, and then to compare the results with a DoS attack. Such a comparison will enable performance evaluation of the proposed method when faced with different attacks, including Sybil attacks and session hijacking.

8.4 Chapter summary

This chapter concludes the thesis and summarises the scope of research based on the research objectives. The strengths and limitations of the study are also presented. Findings presented suggest a number of research directions for the future and demonstrate that the security aspects of each network are important for preserving their resources and services. The nature of the MANET network creates many challenges and means that it is vulnerable to many attacks. However, the method proposed here mitigates DoS attacks in both SM and MM. This method uses a combination of trust values to calculate a TTSV for each node which then helps to detect DoS attacks. Establishing trust between nodes helps to improve network security levels as each node can easily explore the behaviours of its immediate neighbours.

References

ABBAS, S., MERABTI, M. & LLEWELLYN-JONES, D. A Survey of Reputation Based Schemes for MANET. The 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK, 2010. 21-22.

ABBAS, S., MERABTI, M. & LLEWELLYN-JONES, D. Identity-based Attacks Against Reputation-based Systems in MANETs. 12th Annual Postgraduate Symposium on Convergence of Telecommunications, Networking and Broadcasting (PGNet 2011), Liverpool, UK, 2011. 27-28.

ABBAS, S., MERABTI, M., LLEWELLYN-JONES, D. & KIFAYAT, K. 2013. Lightweight Sybil attack detection in MANETs. *Systems Journal, IEEE,* 7**,** 236-248.

ABBAS, S., MERABTI, M. & LLEWELLYN-JONES, D. 2015. On the evaluation of reputation and trust-based schemes in mobile ad hoc networks. *Security and Communication Networks,* 8**,** 4041-4052.

ABDELAZIZ, A. K., NAFAA, M. & SALIM, G. Survey of routing attacks and countermeasures in mobile ad hoc networks. Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on, 2013. IEEE, 693-698.

ABDELMALEK, A., FEHAM, M. & TALEB-AHMED, A. 2009. On Recent Security Enhancements to Autoconfiguration Protocols for MANETs: Real Threats and Requirements. *IJCSNS,* 9**,** 401-407.

ABRAHAM, J. 2013. A survey of intrusion detection for ad-hoc network. *Journal of global research in computer science,* 4**,** 182-185.

AGGARWAL, N. & DHANKHAR, K. 2014. Attacks on Mobile Adhoc Networks: A Survey. *International Journal of Research in Advent Technology,* 2**,** 307-316.

AGRAWAL, V. M. & CHAUHAN, H. 2015. An Overview of security issues in Mobile Ad hoc Networks. *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND SCIENCES,* 1**,** 9-17.

AHMAD, M., TAJ, S., MUSTAFA, T. & ASRI, M. Performance analysis of wireless network with the impact of security mechanisms. Emerging Technologies (ICET), 2012 International Conference on, 2012. IEEE, 1-6.

AL-MISTARIHI, M. F., AL-SHURMAN, M. & QUDAIMAT, A. 2011. Tree based dynamic address autoconfiguration in mobile ad hoc networks. *Computer Networks,* 55**,** 1894-1908.

AL-ROUBAIEY, A., SHELTAMI, T., MAHMOUD, A., SHAKSHUKI, E. & MOUFTAH, H. AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement. Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, 2010. IEEE, 634-640.

ALANI, M. M. 2014. TCP/IP Model. *Guide to OSI and TCP/IP models.* Springer.

ALDOSARI, H. M., SNASEL, V. & ABRAHAM, A. 2016. A New Security Layer for Improving the security of internet of things (IoT).

ALICHERRY, M., KEROMYTIS, A. D. & STAVROU, A. 2008. Distributed firewall for MANETs. *Computer Science Technical Report Series*.

ALNAGHES, M. S. & GEBALI, F. A Survey on Some Currently Existing Intrusion Detection Systems for Mobile Ad Hoc Networks. The Second International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing (EEECEGC2015), 2015. 12.

ALPCAN, T. & BAŞAR, T. 2010. *Network security: A decision and game-theoretic approach*, Cambridge University Press.

AMBHORE, P., WANKHADE, K. A., CHATUR, P. & DEORANKAR, A. 2013. A MANET.

AMGAHD, Y. A. & YADAV, R. 2016. Survey of Mobile IP Protocols.

ANANTVALEE, T. & WU, J. 2007. A survey on intrusion detection in mobile ad hoc networks. *Wireless Network Security.* Springer.

ANCONA, M., DODERO, G., MINUTO, F., GUIDA, M. & GIANUZZI, V. Mobile computing in a hospital: the WARD-IN-HAND project. Proceedings of the 2000 ACM symposium on Applied computing-Volume 2, 2000. ACM, 554-556.

ANTONY, J. 2014. *Design of experiments for engineers and scientists*, Elsevier.

ARAVINDH, S., VINOTH, R. & VIJAYAN, R. 2013. A Trust Based Approach for Detection and Isolation of Malicious Nodes in Manet.

ARUNKUMAR, R. & ANNALAKSHMI, A. 2014. A Recent Analysis of Intrusion Detection and Prevention System for Protecting Range of Attack using Data Gathering Technique in MANET. *International Journal of Computer Applications,* 85.

AUJLA, G. S. & KANG, S. S. 2013. Comprehensive evaluation of AODV, DSR, GRP, OLSR and TORA routing protocols with varying number of nodes and traffic applications over MANETs. *IOSR Journal of Computer Engineering,* 9**,** 54-61.

BAGWARI, A., JEE, R., JOSHI, P. & BISHT, S. Performance of AODV Routing Protocol with increasing the MANET Nodes and its effects on QoS of Mobile Ad hoc Networks. Communication Systems and Network Technologies (CSNT), 2012 International Conference on, 2012. IEEE, 320-324.

BAHGA, A. & MADISETTI, V. 2014. *Internet of Things: A Hands-on Approach,* VPT.

BAI, F., SADAGOPAN, N. & HELMY, A. IMPORTANT: A framework to systematically analyze the Impact of Mobility on Performance of RouTing protocols for Adhoc NeTworks. INFOCOM 2003. Twenty-second annual joint conference of the IEEE computer and communications. IEEE societies, 2003. IEEE, 825-835.

BALAKRISHNAN, V., VARADHARAJAN, V., TUPAKULA, U. K. & LUES, P. Trust and recommendations in mobile ad hoc networks. Networking and Services, 2007. ICNS. Third International Conference on, 2007. IEEE, 64-64.

BALANDIN, S. 2010. *Smart Spaces and Next Generation Wired/Wireless Networking: Third Conference on Smart Spaces, RuSMART 2010, and 10th International Conference, NEW2AN 2010, St. Petersburg, Russia, August 23-25, 2010, Proceedings*, Springer Science & Business Media.

BANG, A. O. & RAMTEKE, P. L. 2013. MANET: History, Challenges And Applications. *International Journal of Application or Innovation in Engineering & Management (IJAIEM),* 2**,** 249-251.

BANSAL, B., TRIPATHY, M. R., GOYAL, D. & GOYAL, M. Improved Routing Protocol for MANET. Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on, 2015. IEEE, 340-346.

BEGAM, U. S. & MURUGABOOPATHI, D. G. 2013. A Recent secure intrusion detection system for MANETs. *International Journal of Emerging Technology and Advanced Engineering,* 3.

BELLAVISTA, P., CARDONE, G., CORRADI, A. & FOSCHINI, L. 2013. Convergence of MANET and WSN in IoT urban scenarios. *Sensors Journal, IEEE,* 13**,** 3558-3567.

BELLO GARBA, A., ARMAREGO, J. & MURRAY, D. 2015. Bring your own device organizational information security and privacy. *ARPN Journal of Engineering and Applied Sciences,* 10**,** 1279-1287.

BERMAN, V. & MUKHERJEE, B. Data security in manets using multipath routing and directional transmission. Communications, 2006. ICC'06. IEEE International Conference on, 2006. IEEE, 2322-2328.

BISHOP, M. 2003. What is computer security? *Security & Privacy, IEEE,* 1**,** 67-69.

BISHOP, M. 2005. *Introduction to computer security,* Addison-Wesley Boston, MA.

BLAZE, M., FEIGENBAUM, J. & LACY, J. Decentralized trust management. Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on, 1996. IEEE, 164-173.

BOSWORTH, S., KABAY, M. E. & WHYNE, E. 2009. *Computer Security Handbook,* USA, John Wily & Sons.

BOTKAR, S. P. & CHAUDHARY, S. R. An enhanced Intrusion Detection System using Adaptive Acknowledgment based algorithm. Information and Communication Technologies (WICT), 2011 World Congress on, 2011. IEEE, 606-611.

BUCHEGGER, S. & LE BOUDEC, J.-Y. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, 2002. ACM, 226-236.

BUDDHA, G. 2013. An Improved Watchdog Intrusion Detection Systems In Manet. *International Journal of Engineering,* 2.

BURBANK, J. L., CHIMENTO, P. F., HABERMAN, B. K. & KASCH, W. T. 2006. Key challenges of military tactical networking and the elusive promise of MANET technology. *Communications Magazine, IEEE,* 44**,** 39-45.

BUTTYÁN, L. & HUBAUX, J.-P. 2003. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications,* 8**,** 579-592.

CANO, J.-C. & MANZONI, P. A performance comparison of energy consumption for mobile ad hoc network routing protocols. Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 2000. Proceedings. 8th International Symposium on, 2000. IEEE, 57-64.

CARMINATI, B., FERRARI, E. & VIVIANI, M. 2013. Security and trust in online social networks. *Synthesis Lectures on Information Security, Privacy, & Trust,* 4**,** 1-120.

CARRELL, J., CHAPPELL, L., TITTEL, E. & PYLES, J. 2012. *Guide to TCP/IP*, Cengage Learning.

CASAD, J. 2011. *Sams teach yourself TCP/IP in 24 hours*, Sams Publishing.

CHALAMASETTY, G. K., MANDAL, P. & TSENG, T.-L. Secure SCADA communication network for detecting and preventing cyber-attacks on power systems. Power Systems Conference (PSC), 2016 Clemson University, 2016. IEEE, 1-7.

CHANG, B.-J. & KUO, S.-L. 2009. Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs. *Vehicular Technology, IEEE Transactions on,* 58**,** 1846-1863.

CHATTERJEE, M., DAS, S. K. & TURGUT, D. An on-demand weighted clustering algorithm (WCA) for ad hoc networks. Global Telecommunications Conference, 2000. GLOBECOM'00. IEEE, 2000. IEEE, 1697-1701.

CHATTERJEE, M., DAS, S. K. & TURGUT, D. 2002. WCA: A weighted clustering algorithm for mobile ad hoc networks. *Cluster Computing,* 5**,** 193-204.

CHATURVEDI, A. & SHARMA, S. 2013. Exploring Intrusion Detection Schemes and their Comparison in MANETs. *International Journal of Computer Applications,* 71**,** 55-59.

CHAUDHARI, M. B. S. & PRASAD, D. R. S. 2015. Particle Swarm Optimization Based Intrusion Detection for Mobile Ad-hoc Networks.

CHEN, R., GUO, J., BAO, F. & CHO, J.-H. 2014. Trust management in mobile ad hoc networks for bias minimization and application performance maximization. *Ad Hoc Networks,* 19**,** 59-74.

CHHABRA, M., GUPTA, B. & ALMOMANI, A. 2013. A Novel Solution to Handle DDOS Attack in MANET.

CHITKARA, M. & AHMAD, M. W. 2014. Review on MANET: Characteristics, Challenges, Imperatives and Routing Protocols. *International Journal of Computer Science and Mobile Computing, 3 (2)***,** 432-437.

CHO, J.-H., SWAMI, A. & CHEN, I.-R. 2011. A survey on trust management for mobile ad hoc networks. *Communications Surveys & Tutorials, IEEE,* 13**,** 562-583.

CHO, J.-H., SWAMI, A. & CHEN, R. 2012. Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks. *Journal of Network and Computer Applications,* 35**,** 1001-1012.

CHOUDHURY, P., MAJUMDER, K. & DE, D. 2015. Secure and Dynamic IP Address Configuration Scheme in MANET. *Intelligent Computing, Communication and Devices.* Springer.

CIAMPA, M. 2014. *Comptia Security+ SY0-401 in Depth*, Cengage Learning Trade.

CONTI, M. & GIORDANO, S. 2014. Mobile ad hoc networking: milestones, challenges, and new research directions. *Communications Magazine, IEEE,* 52**,** 85-96.

CROWCROFT, J., GIBBENS, R., KELLY, F. & ÖSTRING, S. 2004. Modelling incentives for collaboration in mobile ad hoc networks. *Performance Evaluation,* 57**,** 427-439.

DALAL, R., KHARI, M. & SINGH, Y. 2012. Different ways to achieve Trust in MANET. *International Journal on AdHoc Networking Systems (IJANS) Vol*, 2.

DAVE, D. & DAVE, P. An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET. Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on, 2014. IEEE, 1690-1696.

DEAN, T. 2012. *Network+ guide to networks*, Cengage Learning.

DENKO, M. K. 2005. Detection and prevention of denial of service (DoS) attacks in mobile ad hoc networks using reputation-based incentive scheme. *Journal Systemics, Cybernetics and Informatics*, 3**,** 1-9.

DEV, P. M. & AUGUSTIN, A. 2015. Malicious Packet Dropping Detection in Wireless Ad Hoc Networks based on Public Auditing Architecture. *Wireless Communication*, 7**,** 94-100.

DHANALAKSHMI, S. 2013. A reliable and secure framework for detection and isolation of malicious nodes in MANET.

DHENAKARAN, D. S. & PARVATHAVARTHINI, A. 2013. An Overview of Routing Protocols in Mobile Ad-Hoc Network. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3.

DROMS, R. 1997. Dynamic host configuration protocol.

EL EMARY, I. M. & RAMAKRISHNAN, S. 2013. *Wireless Sensor Networks: From Theory to Applications*, CRC Press.

ELIZABETH, L. A., PRASANTH, S. H., GOPESH, S. & SANKAR, B. K. 2014. Enhanced Adaptive Acknowledgment in MANET'S with Clustering.

ENGLAND, P., SHI, Q., ASKWITH, B. & BOUHAFS, F. A Survey of Trust Management in Mobile Ad-Hoc Networks. Proceedings of the 13th annual post graduate symposium on the convergence of telecommunications, networking, and broadcasting, PGNET, 2012.

FAISAL, M., KUMAR, M. & AHMED, A. 2013. ATTACKS IN MANET.

FAZIO, M., VILLARI, M. & PULIAFITO, A. 2006. IP address autoconfiguration in ad hoc networks: Design, implementation and measurements. *Computer Networks*, 50**,** 898-920.

FELICI, M. 2013. *Cyber Security and Privacy: Trust in the Digital World and Cyber Security and Privacy EU Forum 2013, Brussels, Belgium, April 2013, Revised Selected Papers*, Springer.

FILIPEK, J. & HUDEC, L. Distributed firewall in Mobile Ad Hoc Networks. Applied Machine Intelligence and Informatics (SAMI), 2015 IEEE 13th International Symposium on, 2015. IEEE, 233-238.

FIREWALL, B. 2003. *Barracuda Firewall* [Online]. Available: https://www.barracuda.com/products/ngfirewall 2016].

FOROUSHANI, V. A. Deterministic and authenticated flow marking for IP traceback. Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on, 2013. IEEE, 397-404.

GAMMAR, S. M., AMINE, E. & KAMOUN, F. 2010. Distributed address auto configuration protocol for Manet networks. *Telecommunication Systems,* 44**,** 39-48.

GANDHI, J. R. & JHAVERI, R. H. Addressing packet forwarding misbehaviour using trust-based approach in Ad-hoc networks: A survey. Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on, 2015. IEEE, 391-396.

GARCÍA VILLALBA, L. J., GARCÍA MATESANZ, J., SANDOVAL OROZCO, A. L. & MÁRQUEZ DÍAZ, J. D. 2011. Auto-configuration protocols in mobile ad hoc networks. *Sensors,* 11**,** 3652-3666.

GASTI, P., TSUDIK, G., UZUN, E. & ZHANG, L. Dos and ddos in named data networking. Computer Communications and Networks (ICCCN), 2013 22nd International Conference on, 2013. IEEE, 1-7.

GEETHA, K. & SREENATH, N. 2015. Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol. *Arabian Journal for Science and Engineering***,** 1-12.

GHODAKE, M. K. S., BADE, M. M. J., PANGE, M. P. A. & BANSODE, M. A. D. 2015. EAACK—A Secure Intrusion-Detection System for MANETs.

GHOSH, U. & DATTA, R. 2011. A secure dynamic IP configuration scheme for mobile ad hoc networks. *Ad Hoc Networks,* 9**,** 1327-1342.

GOVINDAN, K. & MOHAPATRA, P. 2012. Trust computations and trust dynamics in mobile adhoc networks: a survey. *Communications Surveys & Tutorials, IEEE,* 14**,** 279-298.

GOYAL, A. 2014. Selective Packet Drop Attack in MANET-A Review.

GUIZANI, M., RAYES, A., KHAN, B. & AL-FUQAHA, A. 2010. *Network modeling and simulation: a practical perspective,* John Wiley & Sons.

GULIA, P. & SIHAG, S. 2013. Review and analysis of the security issues in MANET. *International Journal of Computer Applications,* 75**,** 23-26.

GUNASEKARAN, M. & PREMALATHA, K. 2013. TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks. *IET Information Security,* 7**,** 203-211.

GUPTA, B., JOSHI, R. C. & MISRA, M. 2012. Distributed Denial of Service Prevention Techniques. *arXiv preprint arXiv:1208.3557*.

HAGGERTY, S. 2012. *'Merely for Money'?: Business Culture in the British Atlantic, 1750-1815*, Liverpool University Press.

HALL, K. 2015a. *Eclipse staggers to feet, gets smacked by second DDoS* [Online]. The register Available: http://www.theregister.co.uk/2015/11/25/eclipse_isp_ddos/.

HALL, K. 2015b. *Freeparking hit by DDoS, vexed customers scream into abyss* [Online]. the register website. Available: http://www.theregister.co.uk/2015/06/09/freeparking_hit_by_ddos_attack/ 2015].

HAN, S. Y. & LEE, D. 2013. An adaptive hello messaging scheme for neighbor discovery in on-demand MANET routing protocols. *Communications Letters, IEEE,* 17**,** 1040-1043.

HAN, Z. 2012. *Game theory in wireless and communication networks: theory, models, and applications*, Cambridge University Press.

HARPER, R. 2014. Reflections on Trust, Computing, and Society. *Trust, Computing, and Society***,** 299.

HASHMI, M. J., SAXENA, M. & SAINI, R. 2012. Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System. *International Journal of Computer Science & Communication Networks,* 2.

HE, Q., WU, D. & KHOSLA, P. SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks. Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE, 2004. IEEE, 825-830.

HORVÁTH, R. 2013. Does trust promote growth? *Journal of Comparative Economics,* 41**,** 777-788.

HRABIK, M., GUILFOYLE, J. & MAC BEAVER, E. 2006. Method and apparatus for verifying the integrity and security of computer networks and implementing counter measures. Google Patents.

HSU, Y.-Y. & TSENG, C.-C. 2005. Prime DHCP: a prime numbering address allocation mechanism for MANETs. *IEEE communications letters,* 9**,** 712-714.

HU, J. & BURMESTER, M. LARS: a locally aware reputation system for mobile ad hoc networks. Proceedings of the 44th annual Southeast regional conference, 2006. ACM, 119-123.

HU, S. & MITCHELL, C. J. 2005. Improving IP address autoconfiguration security in MANETs using trust modelling. *Mobile Ad-hoc and Sensor Networks.* Springer.

HU, Y.-C., PERRIG, A. & JOHNSON, D. B. Packet leashes: a defense against wormhole attacks in wireless networks. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, 2003. IEEE, 1976-1986.

HUCABY, D. 2014. *CCNA Wireless 640-722 Official Cert Guide*, Pearson Education.

HUNT, C. 2002. *TCP/IP network administration*, " O'Reilly Media, Inc.".

INDRASINGHE, S., PEREIRA, R. & HAGGERTY, J. Conflict free address allocation mechanism for mobile ad hoc networks. Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, 2007. IEEE, 852-857.

INDRASINGHE, S., PEREIRA, R. & HAGGERTY, J. Protocol Specification for Conflict Free MANET Address Allocation Mechanisms. Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on, 2008. IEEE, 1434-1439.

INDRASINGHE, S., PEREIRA, R. & HAGGERTY, J. Disjointed Conflict Free Address Auto-Configuration for Mobile Ad Hoc Networks. Network-Based Information Systems, 2009. NBIS'09. International Conference on, 2009. IEEE, 343-349.

INDRASINGHE, S., PEREIRA, R. & MOKHTAR, H. Hosts Address Auto Configuration for Mobile Ad Hoc Networks. 4th International Conference on Performance Modeling and Evaluation of Heterogeneous Networks, 2006.

ISSARIYAKUL, T. & HOSSAIN, E. 2011. *Introduction to network simulator NS2*, Springer Science & Business Media.

JAIN, A. & BUKSH, B. 2016. Solutions for Secure Routing in Mobile Ad Hoc Network (MANET): A Survey. *Imperial Journal of Interdisciplinary Research,* 2.

JAIN, A. K. & TOKEKAR, V. Classification of denial of service attacks in mobile ad hoc networks. Computational Intelligence and Communication Networks (CICN), 2011 International Conference on, 2011. IEEE, 256-261.

JAIN, R. & GARG, S. 2013. SECURITY GOALS OF MANETs ALONG WITH RESEARCH CHALLENGES & ISSUES.

JAIN, S. 2014. Security Threats in MANETS: A Review. *arXiv preprint arXiv:1405.5320*.

JATHE, S. R. & DAKHANE, D. M. 2012. Indicators for detecting Sinkhole Attack in MANET. *International Journal of Emerging Technology and Advanced Engineering Website: www. ijetae. com (ISSN 2250-2459, Volume 2, Issue 1*.

JHAVERI, R. H., PATEL, S. J. & JINWALA, D. C. Dos attacks in mobile ad hoc networks: A survey. Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, 2012a. IEEE, 535-541.

JHAVERI, R. H., PATEL, S. J. & JINWALA, D. C. A novel approach for grayhole and blackhole attacks in mobile ad hoc networks. Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, 2012b. IEEE, 556-560.

JHUMKA, A., GRIFFITHS, N., DAWSON, A. & MYERS, R. 2008. An outlook on the impact of trust models on routing in mobile ad hoc networks (MANETs).

JIA, Q., SUN, K. & STAVROU, A. 2013. Capability-Based Defenses Against DoS Attacks in Multi-path MANET Communications. *Wireless personal communications,* 73**,** 127-148.

JIANG, S. 2012. *Future wireless and optical networks: networking modes and cross-layer design,* Springer Science & Business Media.

JIN, X., ZHANG, Y., PAN, Y. & ZHOU, Y. 2006. ZSBT: A novel algorithm for tracing DoS attackers in MANETs. *EURASIP Journal on Wireless Communications and Networking,* 2006**,** 82-82.

KAHATE, A. 2013. *Cryptography and network security*, Tata McGraw-Hill Education.

KARTHA, G. K. & NEEBA, E. Trust Establishment in Mobile Ad Hoc Networks. Eco-friendly Computing and Communication Systems (ICECCS), 2014 3rd International Conference on, 2014. IEEE, 133-137.

KAUR, A. & SIDHU, M. 2014. Mitigation of Black Hole and Grey Hole Attack In Mobile Ad hoc Networks.".

KAUR, N. & MONGA, S. M. 2014. COMPARISONS OF WIRED AND WIRELESS NETWORKS:A REVIEW. *International Journal of Advanced Engineering Technology,* V.

KAUR, S., KAUR, R. & VERMA, A. Jellyfish attack in MANETs: A review. Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on, 2015. IEEE, 1-5.

KAUSHIK, S. & SHARMA, S. 2015. Securing Ad hoc Networks for Intrusion Detection, A study.

KHAN, R. & VATSA, A. 2011. Detection and control of DDOS attacks over reputation and score based MANET. *J Emerg Trends Comput Inf Sci,* 2**,** 646-655.

KHATRI, A., KOLHE, S. & GIRI, N. 2016. Dynamic Address Allocation Algorithm for Mobile Ad hoc Networks. *arXiv preprint arXiv:1605.00398*.

KIM, I. Y. & KIM, I. Y. A resource-efficient ip traceback technique for mobile ad-hoc networks based on time-tagged bloom filter. Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on, 2008. IEEE, 549-554.

KIM, S.-C. & CHUNG, J.-M. Scalability analysis of stateful and stateless MANET address auto-configuration protocols. ICT Convergence (ICTC), 2013 International Conference on, 2013. IEEE, 408-409.

KIZZA, J. M. 2009. *Guide to computer network security*, Springer.

KOCH, R., STELTE, B. & GOLLING, M. Attack trends in present computer networks. Cyber Conflict (CYCON), 2012 4th International Conference on, 2012. IEEE, 1-12.

KRISHNAN, M. M., BALACHANDER, T. & RAJASEKAR, P. 2015. Agent Based Trust Estimation for Mobile Ad Hoc Network. *Indian Journal of Science and Technology,* 8**,** 223-227.

KUMAR, A. & SINGH, J. 2015. Security Attacks in Mobile Adhoc Networks (MANET): A Literature Survey. *International Journal of Computer Applications*, 122.

KUMAR, B. P., SEKHAR, P. C., PAPANNA, N. & BHUSHAN, B. B. 2013. A SURVEY ON MANET SECURITY CHALLENGES AND ROUTING PROTOCOLS. *P Chandra Sekhar et al, Int. J. Computer Technology & Applications,* 4**,** 248-256.

KUMAR, M. & RISHI, R. 2010. Security aspects in mobile ad hoc network (MANETs): Technical review. *International Journal of Computer Applications IJCA,* 12**,** 24-28.

LAXMI, V., LAL, C., GAUR, M. & MEHTA, D. 2014. JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. *Journal of Information Security and Applications*.

LAXMI, V., LAL, C., GAUR, M. & MEHTA, D. 2015. JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. *Journal of Information Security and Applications,* 22**,** 99-112.

LI, R., LI, J., LIU, P. & CHEN, H.-H. An objective trust management framework for mobile ad hoc networks. Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th, 2007. IEEE, 56-60.

LI, W., PARKER, J. & JOSHI, A. 2009. Security through collaboration in manets. *Collaborative Computing: Networking, Applications and Worksharing.* Springer.

LI, W., PARKER, J. & JOSHI, A. 2012. Security through collaboration and trust in manets. *Mobile Networks and Applications*, 17**,** 342-352.

LIANG, C. & YU, F. R. 2015. Wireless network virtualization: A survey, some research issues and challenges. *Communications Surveys & Tutorials, IEEE,* 17**,** 358-380.

LIU, B., BESTAVROS, A., DU, D.-Z. & WANG, J. 2009. Wireless Algorithms, Systems, and Applications. *Lecture Notes in Computer Science,* 5682.

LIU, G., WANG, Y. & ORGUN, M. A. Social Context-Aware Trust Network Discovery in Complex Contextual Social Networks. AAAI, 2012. 101-107.

LIU, Z., JOY, A. W. & THOMPSON, R. A dynamic trust model for mobile ad hoc networks. Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of, 2004. IEEE, 80-85.

LOO, J., MAURI, J. L. & ORTIZ, J. H. 2011. *Mobile Ad hoc networks: current status and future trends*, CRC Press.

LOTFY, P. A. & AZER, M. A. Performance evaluation of AODV under dos attacks. Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP, 2013. IEEE, 1-4.

MAHAJAN, R. K. & PATIL, S. M. Protection against data drop, an enhanced security model of authentication protocol for Ad-hoc N/w. Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on, 2015. IEEE, 1-4.

MALHOTRA, N., GARG, R. & MAHAJAN, R. 2013. Quantitative Detection of AODV against Black Hole and Worm Hole Attacks in MANET. *International Journal of Computer Applications,* 68**,** 42-48.

MANI, P. & KAMALAKKANNAN, P. 2013. Mitigating selfish behavior in mobile ad hoc networks: a survey. *International Journal of Computer Applications,* 73**,** 1-7.

MANSI, R. & RAVI, P. 2006. A distributed protocol for dynamic address assignment inmobile ad hoc networks. *IEEE Transactions on Mobile Computing,* 5**,** 4-19.

MARAS, E. 2015. *HACKER PARALYZES RUTGERS UNIVERSITY WITH DDOS ATTACKS; MOCKS ITS CYBERSECURITY EFFORTS* [Online]. Hacked website. Available: https://hacked.com/hacker-paralyzes-rutgers-university-ddos-attacks-mocks-cybersecurity-efforts/.

MARSHALL, A. & ELGHOSSAIN, N. 2014. Trust Within Government. *Public Manager,* 43**,** 58.

MARTI, S., GIULI, T. J., LAI, K. & BAKER, M. Mitigating routing misbehavior in mobile ad hoc networks. International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking, 2000. 255-265.

MARTIN, A. J. 2015. *TalkTalk offers customer £30.20 'final settlement' after crims nick £3,500* [Online]. theregister.com. 2015].

MCA, K. M. Routing Protocols in MANET. Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications, 2015.

MENAKA, R. & RANGANATHAN, D. V. 2013. A Survey of Trust related Routing Protocols for Mobile Ad Hoc Networks. *International Journal of Emerging Technology and Advanced Engineering", ISSN***,** 2250-2459.

MERKOW, M. S. & BREITHAUPT, J. 2004. *Computer security assurance using the common criteria*, Cengage Learning.

MICHEAL, G. & ARUNACHALAM, A. 2014. EAACK: Enhanced Adaptive Acknowledgment for MANET. *Middle-East Journal of Scientific Research,* 19**,** 1205-1208.

MICHIARDI, P. & MOLVA, R. 2002. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. *Advanced Communications and Multimedia Security*. Springer.

MILLER, K. W., VOAS, J. & HURLBURT, G. F. 2012. BYOD: Security and privacy considerations. *It Professional***,** 53-55.

MISHRA, A., JAISWAL, R. & SHARMA, S. A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network. Advance Computing Conference (IACC), 2013 IEEE 3rd International, 2013. IEEE, 499-504.

MISRA, S., MISRA, S. C. & WOUNGANG, I. 2009a. *Guide to wireless mesh networks*, Springer.

MISRA, S., WOUNGANG, I. & MISRA, S. C. 2009b. *Guide to wireless ad hoc networks*, Springer Science & Business Media.

MISZTAL, B. 2013. *Trust in modern societies: The search for the bases of social order*, John Wiley & Sons.

MITROKOTSA, A. & DIMITRAKAKIS, C. 2013. Intrusion detection in MANET using classification algorithms: The effects of cost and model selection. *Ad Hoc Networks,* 11**,** 226-237.

MITTAL, S. 2015. Identification Technique for All Passive Selfish Node Attacks In a Mobile Network. *International Journal,* 3.

MOE, M. E., HELVIK, B. E. & KNAPSKOG, S. J. TSR: Trust-based secure MANET routing using HMMs. Proceedings of the 4th ACM symposium on QoS and security for wireless and mobile networks, 2008. ACM, 83-90.

MOHSENI, S., HASSAN, R., PATEL, A. & RAZALI, R. Comparative review study of reactive and proactive routing protocols in MANETs. Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on, 2010. IEEE, 304-309.

MORI, M. V. & JETHAVA, G. 2013. Node registration in MANET. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume,* 2.

MUNJAL, A., SINGH, Y. N., PHANEENDRA, A. & ROY, A. Scalable Hierarchical Distributive Auto-configuration Protocol for MANETs. Signal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on, 2013. IEEE, 699-705.

MURALISHANKAR, V. & RAJ, D. E. G. D. P. 2014. Routing Protocols for MANET: A Literature Survey. *International Journal of Computer Science and Mobile Applications,* 2**,** 18-24.

MUTLU, S. & YILMAZ, G. 2011. A distributed cooperative trust based intrusion detection framework for MANETs. *ICNS,* 11**,** 292-298.

NADEEM, A. & HOWARTH, M. P. 2013. A survey of MANET intrusion detection & prevention approaches for network layer attacks. *Communications Surveys & Tutorials, IEEE,* 15**,** 2027-2045.

NAGRATH, P. & GUPTA, B. Wormhole attacks in wireless adhoc networks and their counter measurements: A survey. Electronics Computer Technology (ICECT), 2011 3rd International Conference on, 2011. IEEE, 245-250.

NANDINI, N. & AGGARWAL, R. 2015. Prevention of black hole attack by different methods in MANET. *network,* 4.

NASSER, N. & CHEN, Y. Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks. Communications, 2007. ICC'07. IEEE International Conference on, 2007. IEEE, 1154-1159.

NESARGI, S. & PRAKASH, R. MANETconf: Configuration of hosts in a mobile ad hoc network. INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 2002. IEEE, 1059-1068.

NIKOLIKJ, V. & JANEVSKI, T. 2014. Applicable cost modeling of LTE-Advanced and IEEE 802.11 ac based heterogeneous wireless access networks. *Proceedings of AICT***,** 20-24.

NODA, C., PÉREZ-PENICHET, C. M., SEEBER, B., ZENNARO, M., ALVES, M. & MOREIRA, A. 2015. On the Scalability of Constructive Interference in Low-Power Wireless Networks. *Wireless Sensor Networks.* Springer.

OTROK, H., MOHAMMED, N., WANG, L., DEBBABI, M. & BHATTACHARYA, P. 2008. A game-theoretic intrusion detection model for mobile ad hoc networks. *Computer communications,* 31**,** 708-721.

PADIYA, S., PANDIT, R. & PATEL, S. 2013. Survey of innovated techniques to detect selfish nodes in MANET. *International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), ISSN***,** 2250-1568.

PARK, S. & YOO, S.-M. 2013. An efficient reliable one-hop broadcast in mobile ad hoc networks. *Ad Hoc Networks,* 11**,** 19-28.

PARKER, S. K., BINDL, U. K. & STRAUSS, K. 2010. Making things happen: A model of proactive motivation. *Journal of management*.

PATCHIPULUSU, P. 2001. *Dynamic address allocation protocols for mobile ad hoc networks.* Texas A&M University.

PATEL, A., PATEL, N. & PATEL, R. Defending against Wormhole Attack in MANET. Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on, 2015a. IEEE, 674-678.

PATEL, D. 2015. Survey of flooding attack mobile Adhoc network. *International Journal of Management, IT and Engineering,* 5**,** 119-132.

PATEL, M. & SHARMA, S. Detection of malicious attack in manet a behavioral approach. Advance Computing Conference (IACC), 2013 IEEE 3rd International, 2013. IEEE, 388-393.

PATEL, N., PAWAR, A. & SHEKOKAR, N. 2015b. A Survey on Routing Protocols for MANET. *International Journal of Computer Applications,* 110.

PATIL, J. A. & SIDNAL, N. 2013. Survey-secure routing protocols of MANET. *International Journal of Applied Information Systems (IJAIS),* 5.

PERKINS, C. E. 2008. *Ad hoc networking,* Addison-Wesley Professional.

PERRY, B., HUSS, C. & FIELDS, J. 2010. *VCP VMware Certified Professional on vSphere 4 Study Guide: Exam VCP-410,* John Wiley & Sons.

PFLEEGER, C. P., PFLEEGER, S. L. & MARGULIES, J. 2015. *Security in Computing,* United states of America, Library of Congress Cataloging-in-Publication Data.

PINYOL, I. & SABATER-MIR, J. 2013. Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review,* 40**,** 1-25.

POKHARIYAL, S. & KUMAR, P. 2014. A Novel Scheme for Detection and Elimination of Blackhole/Grayhole Attack in Manets. *International Journal of Computer Science and Mobile Computing,* 3**,** 217-223.

PONSAM, J. G. & SRINIVASAN, R. 2014. A Survey on MANET Security Challenges, Attacks and its Countermeasures. *International Journal of Emerging Trends & Technology in Computer Science (IJETICS) Volume,* 3.

PRESS, C. U. 2016a. *Detection* [Online]. Cambridge Dictionaries online. Available: http://dictionary.cambridge.org/dictionary/english/detection.

PRESS, C. U. 2016b. *evaluation* [Online]. Cambridge Dictionaries online. Available: http://dictionary.cambridge.org/dictionary/english/evaluation.

PRESS, C. U. 2016c. *monitor* [Online]. Cambridge Dictionaries online. Available: http://dictionary.cambridge.org/dictionary/english/monitor 2016].

PRESS, C. U. 2016d. *rehabilitation* [Online]. Cambridge Dictionaries online. Available: http://dictionary.cambridge.org/dictionary/english/rehabilitation 2016].

PRESS, C. U. 2016e. *reputation* [Online]. Cambridge Dictionaries online. Available: http://dictionary.cambridge.org/dictionary/english/reputation.

QUINTERO, R. M. H., GARCIA, J. A. G., TORCATT, C. M. & HERNANDEZ, F. 2013. Network Simulator-NS2. *Revista de Tecnologia e Informacion,* 1.

RACHEDI, A., BENSLIMANE, A., OTROK, H., MOHAMMED, N. & DEBBABI, M. 2010. A secure mechanism design-based and game theoretical model for manets. *Mobile Networks and Applications,* 15**,** 191-204.

RAGHAVENDRAN, C., SATISH, G. N. & VARMA, P. S. 2013. Security challenges and attacks in mobile ad hoc networks. *International Journal of Information Engineering Electronic Business,* 5**,** 49-58.

RAI, A. K., TEWARI, R. R. & UPADHYAY, S. K. 2010. Different types of attacks on integrated MANET-Internet communication. *International Journal of Computer Science and Security,* 4**,** 265-274.

RAJ, N., BHARTI, P. & THAKUR, S. Vulnerabilities, Challenges and Threats in Securing Mobile Ad-Hoc Network. Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on, 2015. IEEE, 771-775.

RAJAKUMAR, P., PRASANNA, V. T. & PITCHAIKKANNU, A. Security attacks and detection schemes in MANET. Electronics and Communication Systems (ICECS), 2014 International Conference on, 2014. IEEE, 1-6.

RANDHAWA, T. S. & HARDY, S. 2013. *Network management in wired and wireless networks*, Springer Science & Business Media.

REARDON, B. A. 2015. *Feminist concepts of peace and security*, Springer.

REINA, D. G., TORAL, S. L., BARRERO, F., BESSIS, N. & ASIMAKOPOULOU, E. 2013. The Role of Ad Hoc Networks in the Internet of Things: A Case Scenario for Smart Environments. *Internet of Things and Inter-Cooperative Computational Technologies for Collective Intelligence.* Springer.

ROONEY, T. 2011. *Introduction to IP address management*, John Wiley & Sons.

ROTH, D. 2013. Building Cultures of Trust (Book Review). *Pro Rege,* 41**,** 34-36.

SADOK, D., ASCHOFF, R. R., KELNER, J. & SOUTO, E. 2014. Network address allocation method. Google Patents.

SAHU, L. & SINHA, C. 2013. A Cooperative Approach for Understanding Behavior of Intrusion Detection System in Mobile Ad Hoc Networks. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE,* 1.

SARKAR, S. K., BASAVARAJU, T. & PUTTAMADAPPA, C. 2007. *Ad hoc mobile wireless networks: principles, protocols and applications*, CRC Press.

SASTRY, A. S., SULTHANA, S. & VAGDEVI, S. 2013. Security Threats in Wireless Sensor Networks in Each Layer. *Int. J. Advanced Networking and Applications,* 4**,** 1657-1661.

SECUREWORKS, D. 2015. *Incident Response:Plan for the Inevitable Cyber Attack* [Online]. Available: http://go.secureworks.co.uk 2016].

SEDGHI, H., PAKRAVAN, M. R. & AREF, M. R. 2013. A misbehavior-tolerant multipath routing protocol for wireless ad hoc networks. *Int J Res Wireless Syst,* 2**,** 6-15.

SEET, B.-C. 2009. *Mobile Peer-to-Peer Computing for Next Generation Distributed Environments: Advancing Conceptual and Algorithmic Applications: Advancing Conceptual and Algorithmic Applications*, IGI Global.

SEIDL, D., DOHERTY, J. & ORIYANO, S.-P. 2015. *Wireless and Mobile Device Security*, Jones & Bartlett Publishers.

SEIGNEUR, J.-M., KÖLNDORFER, P., BUSCH, M. & HOCHLEITNER, C. A survey of trust and risk metrics for a byod mobile working world. Third International Conference on Social Eco-Informatics (SOTICS 2013), 2013.

SHAH, R., SUBRAMANIAM, S. & DASARATHAN, D. B. L. 2016. Mitigating Malicious Attacks Using Trust Based Secure-BEFORE Routing Strategy in Mobile Ad Hoc Networks. *CIT. Journal of Computing and Information Technology*, 24**,** 237-252.

SHAKSHUKI, E. M., KANG, N. & SHELTAMI, T. R. 2013. EAACK—a secure intrusion-detection system for MANETs. *Industrial Electronics, IEEE Transactions on*, 60**,** 1089-1098.

SHANMUGANATHAN, V. & ANAND, T. 2012. A Survey on Gray Hole Attack in MANET. *IJCNWC*, 2**,** 647-650.

SHARMA, G. & FATIMA, M. 2013. Security & Power Consumption Challenges in MANET: A Review. *International Journal of Advances in Engineering & Technology*, 6**,** 1199-1204.

SHARMA, N., RAINA, B., RANI, P., CHABA, Y. & SINGH, Y. 2013a. Attack prevention methods for DDOS attacks in MANETs. *ASIAN JOURNAL OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY*, 1.

SHARMA, T., TIWARI, M., KUMAR SHARMA, P., SWAROOP, M. & SHARMA, P. An Improved Watchdog Intrusion Detection Systems In Manet. International Journal of Engineering Research and Technology, 2013b. ESRSA Publications.

SHEN, X. S., YU, H., BUFORD, J. & AKON, M. 2010. *Handbook of peer-to-peer networking*, Springer Science & Business Media.

SHI, S., GU, X.-M., ZHANG, W.-B. & SHA, X.-J. 2008. Working mechanism and code analysis of NS2 simulation for mobile Ad hoc networks [J]. *Computer Engineering and Design*, 18**,** 002.

SHINDE, M. S. & BAKAL, J. 2015. Traceback Mechanism for DDoS Attacks Using Local Flow Monitoring in MANET. *nature*, 2**,** 6.

SHINDE SANDEEP, A. & BAKAL, J. 2014. Review on DDoS Attack Traceback Mechanism in MANET.

SHOREY, R., ANANDA, A., CHAN, M. C. & OOI, W. T. 2006. *Mobile, wireless, and sensor networks: technology, applications, and future directions*, John Wiley & Sons.

SINGH, A. & DUA, T. S. 2014. Mobile Ad-Hoc Networks Routing Protocol and its Challenges: A Survey. *International Journal of Computer Applications*, 108.

SINGH, H., KAUR, H., SHARMA, A. & MALHOTRA, R. Performance Investigation of Reactive AODV and Hybrid GRP Routing Protocols under Influence of IEEE 802.11 n MANET. Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on, 2015. IEEE, 325-328.

SINGH, J. P. & GUPTA, A. K. 2013. Protocol Stack based Security Vulnerabilities in MANETs. *International Journal of Computer Applications*, 69.

SINGH, M., SARANGAL, M. & SINGH, G. 2014a. Review of MANET: Applications & Challenges. *Networking and Communication Engineering,* 6**,** 193-197.

SINGH, S., RAJPAL, N. & SHARMA, A. 2014b. Address allocation for MANET merge and partition using cluster based routing. *SpringerPlus,* 3**,** 1-13.

SINGH, U., SAMVATSAR, M., SHARMA, A. & JAIN, A. K. Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol. Colossal Data Analysis and Networking (CDAN), Symposium on, 2016. IEEE, 1-6.

SINHA, S. K., SINGH, R., KUMAR PANDEY, K. & SAHU, M. K. 2013. Distributed Denial of Service Attack Prevention Using Critical Link Method in Manet. *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE),* 2**,** pp: 325-328.

SIVAKUMAR, K. & SELVARAJ, D. G. 2013. Overview of Various Attacks in MANET and Countermeasures for attacks. *International Journal of Computer Science and Management Research,* 2.

SOLTANALI, S., PIRAHESH, S., NIKSEFAT, S. & SABAEI, M. An efficient scheme to motivate cooperation in mobile ad hoc networks. Networking and Services, 2007. ICNS. Third International Conference on, 2007. IEEE, 98-98.

SORATHIYA, D. & RATHOD, H. 2015. Algorithm to Detect and Recover Wormhole Attack in MANETs. *International Journal of Computer Applications,* 124.

STALLINGS, W. 2014. *Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice*, Pearson Higher Ed.

STAPLETON, J. J. 2014. *Security Without Obscurity: A Guide to Confidentiality, Authentication, and Integrity*, CRC Press.

STEWART, J. M. 2013. *Network Security, Firewalls and VPNs*, Jones & Bartlett Publishers.

SU, W., GERLA, M. & DE VERDIERE, A. C. 2014. Mobile Ad hoc Networking (MANET) Y. Yi Internet-Draft S. Lee Intended status: Experimental University of California, Los Expires: September 6, 2014 Angeles.

SUN, Y. & BELDING-ROYER, E. M. 2004. A study of dynamic addressing techniques in mobile ad hoc networks. *Wireless Communications and Mobile Computing,* 4**,** 315-329.

SUN, Y., HAN, Z. & LIU, K. R. 2008. Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine,* 46**,** 112-119.

SURI, P. & SINGH, P. 2014. Wireless Communication-Overview of MANET.

TAN, H.-X. & SEAH, W. K. Framework for statistical filtering against DDoS attacks in MANETs. Embedded Software and Systems, 2005. Second International Conference on, 2005. IEEE, 8 pp.

TAYAL, S. & GUPTA, V. 2013. A Survey of Attacks on Manet Routing Protocols. *International Journal of Innovative Research in Science, Engineering and Technology,* 2**,** 2280-2285.

THORAT, S. & KULKARNI, P. Design issues in trust based routing for MANET. Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on, 2014. IEEE, 1-7.

TYAGI, S. 2013. Analysis Of Techniques For Mitigating Dos Attacks In MANET. *International Journal of Engineering*, 2.

TYLER, T. R., KRAMER, R. M. & JOHN, O. P. 2014. *The psychology of the social self*, Psychology Press.

UDHAYAMOORTHI, M., SENTHILKUMAR, C., KARTHIK, S. & KALAIKUMARAN, T. 2014. An Analysis of Various Attacks in MANET.

VACCA, J. R. 2012. *Computer and information security handbook*, Newnes.

VAIDYA, N. H. Weak duplicate address detection in mobile ad hoc networks. Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, 2002. ACM, 206-216.

VARADHARAJAN, V. & TUPAKULA, U. 2014. Securing wireless mobile nodes from distributed denial-of-service attacks. *Concurrency and Computation: Practice and Experience*.

VARSHNEY, P., BIBHU, V., SAHOO, B. M. & GUPTA, A. 2014. Quantitative Review of Malicious Node Detection of Mobile Ad-Hoc Network.

VASANTH, A. V., SREENIVASAN, M., BABU, S. & SATHISH, B. 2014. A Trust Relation Protocol in Peer-to-Peer Network. *International Journal of Advanced Research in Computer and Communication Engineering,* 3**,** 4928-4932.

VEGDA, M. A. K. & SAHU, M. N. 2015. DDoS Attacks Detection and Traceback by Using Relative Entropy.

VIJAYAN, R. & JEYANTHI, N. 2016. A Survey of Trust Management in Mobile Ad hoc Networks. *International Journal of Applied Engineering Research,* 11**,** 2833-2838.

VIR, D., AGARWAL, S. & IMAM, S. 2013. Investigation on Performance of Trust Based Model and Trust Evaluation of Reactive Routing Protocols in MANET. *wireless networks,* 2.

VISHWAKARMA, D. & RAO, D. 2014. Detection Mechanism for Distributed Denial of Service (DDoS) Attack in Mobile Ad-hoc Networks. *International Journal of Computer Applications,* 102**,** 23-26.

WALLACE, K. 2003. Common Criteria and Protection Profiles: How to Evaluate Information Technology Security. *SANS Institute GIAC practical repository-version,* 1.

WANG, X. & QIAN, H. 2014. A Distributed Address Configuration Scheme for a MANET. *Journal of Network and Systems Management,* 22**,** 559-582.

WANGI, N., PRASAD, R. V., JACOBSSON, M. & NIEMEGEERS, I. 2008. Address autoconfiguration in wireless ad hoc networks: Protocols and techniques. *Wireless Communications, IEEE,* 15**,** 70-80.

WEIMERSKIRCH, A. & THONET, G. 2002. A distributed light-weight authentication model for ad-hoc networks. *Information Security and Cryptology—ICISC 2001*. Springer.

WENIGER, K. Passive duplicate address detection in mobile ad hoc networks. Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE, 2003. IEEE, 1504-1509.

WENIGER, K. 2005. PACMAN: Passive autoconfiguration for mobile ad hoc networks. *Selected Areas in Communications, IEEE Journal on,* 23**,** 507-519.

WU, X. & YAU, D. K. Mitigating denial-of-service attacks in MANET by distributed packet filtering: A game-theoretic approach. Proceedings of the 2nd ACM symposium on Information, computer and communications security, 2007. ACM, 365-367.

XIA, H., JIA, Z., LI, X., JU, L. & SHA, E. H.-M. 2013. Trust prediction and trust-based source routing in mobile ad hoc networks. *Ad Hoc Networks,* 11**,** 2096-2114.

XIAO, Y., SHEN, X. S. & DU, D.-Z. 2007. *Wireless network security,* Springer Science & Business Media.

XIAONAN, W. & HUANYAN, Q. 2013. Cluster-based and distributed IPv6 address configuration scheme for a MANET. *Wireless personal communications,* 71**,** 3131-3156.

YADAV, N. & SHARMA, D. 2015. MANET: Mobile Ad-hoc Network its Characteristics, Challenges, Application and Security Attacks.

ZARGAR, S. T., JOSHI, J. & TIPPER, D. 2013. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *Communications Surveys & Tutorials, IEEE,* 15**,** 2046-2069.

ZHANG, Y. & LEE, W. Intrusion detection in wireless ad-hoc networks. Proceedings of the 6th annual international conference on Mobile computing and networking, 2000. ACM, 275-283.

ZHONG, S., CHEN, J. & YANG, Y. R. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, 2003. IEEE, 1987-1997.

ZHOU, H. & MUTKA, M. W. 2012. *Review of Autoconfiguration for MANETs*, INTECH Open Access Publisher.

ZHOU, H., MUTKA, M. W. & NI, L. M. 2010. Secure prophet address allocation for MANETs. *Security and communication networks*, 3**,** 31-43.

ZHOU, P. & LI, W. A bidirectional backup routing protocol for mobile ad hoc networks. 2012 Second International Conference on Business Computing and Global Informatization, 2012. IEEE, 603-606.

ZOURIDAKI, C., MARK, B. L., HEJMO, M. & THOMAS, R. K. Robust cooperative trust establishment for MANETs. Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, 2006. ACM, 23-34.

Appendix A

Calculations of trust values of nodes

```
procedure trustvalue()
{
networkscan()
{
nodes = for loop 1:71;
}
# checking for the trust values
 set ATV=0, ATV1=0, ATV2=0
 set RTV=0, RTV1=0, RTV2=0, RTV3=0;
 set HTV=0, HTV1=0, HTV2=0, HTV3=0
 set TTSV=0, TTSV1=0, TTSV2=0
now_recordfunctionns2()
{
scan_manet(nodes)
return node_address
}
Rehabilitationstage(node_address)
{
Network node_address= scan_manet(nodes);
return node_address;
}
scan_manet(nodes)
{
Network network= new network(nodes);
network.when(geResponse(every360)) thenReturn(nodeAddres);
network.when(geResponse (every360)) thenReturn(trustStatus);
network.when(geResponse(every360)) thenReturn(nonTrustStatus);
return network;
}
```

```
Detectionstage()
{
CALL now_recordfunctionns2()
CALL Rehabilitationstage(node_address)
CALL stage1repeat1()
}
stage1repeat1(360seconds)
{
calculate ATV()
calculate RTV()
calculate HTV()
calculate TTSV()
}
stage1repeat2(360seconds)
{
calculate ATV()
calculate RTV()
calculate HTV()
calculate TTSV()
}
interface check_for_manet()
{
stage1repeat1(360seconds)
stage1repeat2(360seconds)
}
interface threshold()
{
beingtrustedmethod()
testedtrustedinthework()
}
Rehabilitation()
{
threshold(n)
networkscan()
```

```
if(message==null & notequal(message)) then
{
print "node is trusted”
}
if (Recursion call Rehabilitation()) then
{
repeated= for(1:threshold(n)); //n number of times take every
specific minutes
print “misbehaviour  rate  of  the  node"
}
else if(CTV) then
{
Print "until the  value  of  RTS  has changed"
}
else
{
networkscan(every500seco)
}
}
calculate ATV(ATV1 , ATV2)
{
if(ATV1>0) then
{
Print  " Node transmits the required packet to the intended
destination"
print  "ATV1 =0.5"
}
else if(ATV1<0)) then
{
threshold(n)
networkscan()
Print "ATV1=0 and the node is a malicious"
Print "ATV1 =0"
}
```

```
if (ATV2 =0.5) then
{
print "Then  Node sends the confirmation message to the sender"
}
else if(ATV2=0) then
{
 print  "Node is a selfish"
}
Recursion Call ATV(ATV1+ATV2)
trustvalueATV = Trust_scale()
trustvalueATV = Trust_facet()
}
Calculate RTV(RTV1, RTV2,RTV3)
{
node_drop=packet
if (node_drop>=0) then
{
print " node drops the first time"
print " RTV=0.5"
}
else if (node_drop=1) then
{
Print "Node drops the packet for the second time"
Print "RTV=0.25"
}
else
{
Print  "node is a malicious"
Print  "RTV=0"
}
Recursion  Call RTV(RTV1, RTV2, RTV3)
}
calculate HTV(HTV1, HTV2,HTV3)
{
```

```
Initialize Boolean HTV=0
Network information_between_nodes = now_recordfunctionns2()
if(information_between_nodes) then
{
print  "no conflict in the information between nodes"
print  "HTV=1";
}
else
{
print  "HTV=0"
print  "information between nodes are conflict"
}
recursion Call HTV(HTV1, HTV2, HTV3)
}
// [TTSV calculation starts]
calculate TTSV(TTSV1,TTSV2,TTSV3)
 {
calculate ATV(ATV1 , ATV2)
calculate RTV(RTV1, RTV2,RTV3)
calculate HTV(HTV1, HTV2,HTV3)
threshold(n)
networkscan()
if(ATV==1 && RTV==1 && HTV==1) then
{
print  " TTSV=1"

print  " The node is trusted"
}
else
{
print  "TTSV=0"
print  "The node is untrusted"
}
recursion Call TTSV(TTSV1, TTSV2, TTSV3)
```

```
}
}
End procedure
```