Evaluation of detection method to mitigate DoS attacks in MANETs

Albandari Alsumayt
College of Computer and Information Technology
Shaqra University
Albandari.alsumayt@su.edu.sa
Shaqra city, Saudi Arabia

John Haggerty
School of Science and Technology
Nottingham Trent University
john.haggerty@ntu.ac.uk
Nottingham, UK

Ahmad Lotfi
School of Science and Technology
Nottingham Trent University
Ahmad.lotfi@ntu.ac.uk
Nottingham, UK

***Abstract*— A Mobile ad hoc Network (MANET) is a self-configure, dynamic, and non-fixed infrastructure that consists of many nodes. These nodes communicate with each other without an administrative point. However, due to its nature MANET becomes prone to many attacks such as DoS attacks. DoS attack is a severe as it prevents legitimate users from accessing to their authorised services. Monitoring, Detection, and rehabilitation (MrDR) method is proposed to detect DoS attacks. MrDR method is based on calculating different trust values as nodes can be trusted or not. In this paper, we evaluate the MrDR method which detect DoS attacks in MANET and compare it with existing method Trust Enhanced Anonymous on-demand routing Protocol (TEAP) which is also based on trust concept. We consider two factors to compare the performance of the proposed method to TEAP method: packet delivery ratio and network overhead. The results confirm that the MrDR method performs better in network performance compared to TEAP method.**

Keywords- MANETs; DoS; MrDR.

I. INTRODUCTION

Nowadays, there is a high demand of using the technology in different life sectors. A wireless network is a great example of this technology. People can use it in conferences, universities, airports, and even homes. A Mobile ad hoc Networks (MANET) is a group of mobile nodes that communicate freely without any fixed infrastructure. MANET is independent and nodes are considered such as host and router in sending and receiving packets. MANET is used in many sectors such as airports, cafes, conferences, military arena, and disasters relief situations. It is important to distinguish between DoS and Distributed Denial of Service (DDoS) attack. The former the attacker uses single Internet connection and device to launch the attack against the victim device whereas the later uses multiple Internet connections and devices called botnets or zombies to launch this attack against the victim device [1].

MANET has limited energy and even limited bandwidth that can be such limitations of it. Due to all these features of MANET it becomes vulnerable to many attacks such as eavesdropping, fabrication, and Denial of Service (DoS) attacks. DoS attack degrades the network performance as it deprives legitimate users from reaching the network resources for specific time [2]. There are many types of DoS attacks and each one has its own way to launch the attack but they are all agree on the aim which is prevents authorised users from accessing to their authorised services.

The Monitoring, Detection, and Rehabilitation (MrDR) method is proposed in [3]. The aim of this method is to detect DoS attack by using the trust values. In this paper this method will be evaluated by comparing its performance against an existing method in [4]. This paper is organised as follows. Section 2 discusses the previous attempts to detect this attack in MANET. Section 3 explains the proposed method and the existing method which will be compared against the proposed one. Section 4 illustrates the evaluation of the proposed method with the existing method TEAP. Finally, Section 5 shows the conclusion and suggested future work.

II. RELATED WORK

There are many methods in the literature deal with DoS attack in MANET. There are general methods such as firewalls, filtering, using Intrusion Detection System (IDS), traceback, and pushback methods. Moreover, there are specific methods that based on using trust concept and will be illustrated in this section.

978-1-5386-4427-0/18/$31.00 ©2018 IEEE

A. Using general methods

Firewall is a great example to detect misbehaving activities. However, in MANET firewall cannot distinguish between normal and abnormal activities. Thus, distributed firewalls are designed specifically to be used in MANET [5]. Distributed firewalls is reconfigurable and utilise a central policy that defines all inbound and outbound packets, and what is permitted to do and appropriate. Moreover, this policy is applied to all the endpoints and is enforced for all nodes which participate in the distributed firewall.

The Intrusion Detection System or IDS works as an alarm to protect systems from any vulnerability. However, there are some limitations of using IDS in MANET. For instance, many false alarms can be raised by individual nodes and that consumes the network resources. 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. IDS is more complex in MANET due to mobility and dynamic topologies. Fulfilling the requirements of IDS is thus difficult in MANET, such as gather data and apply IDS techniques to detect intrusions [6].

Filtering uses router to detect and stop excessive packets. However, this is not reliable as the packets might overwhelm the router and lead to a DoS attack. [7] proposed the use of statistical filtering to detect DDoS attacks in MANET by using traffic profiling. The main advantage of using this method is that the packet delivery ratio is increased, whereas the average end-to-end delay is decreased. The main disadvantage of filtering is the cluster-based routing protocol filtering mechanism, as it does not guarantee detection of malicious packets and acceptance of the normal ones [8].

Traceback is another method which gained satisfactory results in detecting DoS attacks and determining the source of an attack. There are multiple types of IP traceback techniques available for both wired and MANET networks: such as ICMP traceback schemes (ITrace) [9]. However, in MANET the nodes move arbitrarily so the position between many nodes changes accordingly. There is no fixed gateway for each node, so the address of nodes is flat. The goal of tracing the DoS on MANET is to find out the physical location of the intruder [10].

Pushback is another method which to defend against DoS attacks. It is hard to determine whether a packet belongs to an attacker and drop it, otherwise, the problem is solved. However, routers cannot know if a packet belongs to a good or misbehaving flow. In the pushback method, routers are enabled to determine the high bandwidth aggregates that participate in the congestion rate and limit them. When the congested router fails to control this then it asks the help of its upstream neighbour nodes. If the attackers are collocated on a path separate from the normal traffic, the performance of the pushback mechanism become better. Pushback cannot work in non-contiguous deployment, and unable to compromise attack which does not overcrowd its core routers [11].

B. Methods use trust concept

[12] posited trust levels in the routing process. Source nodes utilise the trust level to determine the security of the destination node. Moreover, trust levels are used such as a guide to the source node and identify the most appropriate and secure route to the destination. Trust management is used to detect misbehaving nodes whether selfish or malicious nodes. Many DoS attacks have been deterred using this method such as wormhole, blackhole and grayhole attacks.

In addition, [13] developed a 'trust manager' element into their scheme. This method is based on identifying the trust level of the node by using draw upon self-monitored information. As a result, reputation is gathered using direct and either indirect observation. No results have been collected from this method, but some important questions are occur. A basic question is the nature of the relationship between the number of tolerated malicious nodes and the total number of nodes within the network.

[14] proposed the usage of the Markov chain trust model to generate Trust Values (TVs) for immediate nodes. TVs are calculated based only on direct observations of node behaviours, not based on the recommendations from immediate nodes. Certificate Authority (CA) server and a backup CA with high levels of TVs are used to delimit a trust-based hierarchical key management method. However, this study is limited because the lacks of consideration of trust decay although trust is based on the recommendations of immediate nodes.

[15] proposed a new method to detect DoS attacks in MANET using a credit-based mechanism. This method encourages nodes to cooperate. The performance of this technique is based on three phases: reputation and score-based cluster creation and cluster head selection, DoS classification of attacks and their detection, and DoS control packet requests. This method is effective, and its only drawback is the mobility aspect. This was not considered when designing the method, as the cluster heads are assumed to be stationary. Scalability is another issue, as to balance the workload on the cluster, the size of the network raises considerably.

III. THE NOVEL METHOD

MrDR method is designed specifically to detect DoS attacks in MANET. This method was tested in [16] to detect four types of DoS attacks : wormhole attack; blackhole attack; grayhole attack; and jellyfish attack. This section will illustrate the MrDR method. In addition, a brief description about the method that compared with our method will be discussed.

A. MrDR method

The MrDR method consists of three main stages, that are aimed to calculate the total trust status value for every node. Its acronym is derived from these three stages: Monitoring; Detection; and Rehabilitation. These stages work together to calculate the Total Trust Status Value (TTSV) for each of the nodes within the network. These trust values whether trusted or not are temporary values and need to be calculated frequently. Figure 1 shows the MrDR components.

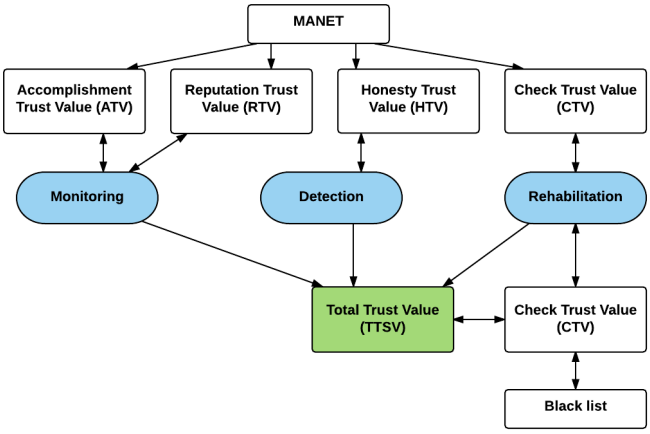

Figure 1. The MrDR components

First stage is monitoring. There are two checks will be done in this stage: Accomplishment Trust Value (ATV) and Reputation Trust Value (RTV). ATV consists of two parts: ATV1 and ATV2. When the node sends the packet to the destination then ATV1=0.5, otherwise it equals zero. In addition, when the node sends confirmation of receiving packet to the node who sends the packet then ATV2=0.5, otherwise it equals zero. Therefore, the ATV is calculated as follows:

$$ATV = ATV1 + ATV2 \qquad (1)$$

Reputation Trust Value (RTV) determines whether the node does not modify or drop packets or even launch DoS attacks. However, regards the MANET feature with its limited energy we cannot consider drop packets is a result of DoS attacks each time as it can be due the power constraints. Thus, in the proposed method if the node drop packets for first time the RTV= 0.5, for second time the RTV=0.25, and if that happens for the third time then the RTV=0. However, if the node does not make the previous misbehaving activities then the RTV=1.

The second stage is detection stage and it calculates the Honesty Trust Value (HTV). If the node gives correct information about its immediate nodes then the HTV=1, otherwise it equals zero.

From stage 1 and stage 2 the Total Trust value is calculated as follows:

$$TTSV = \begin{cases} 0, ATV = 0.5 \text{ or } 0, RTV = 0.5 \text{ or } 0.25 \text{ or } 0, HTV = 0 \\ 1, ATV = 1, RTV = 1, HTV = 1 \end{cases} \qquad (2)$$

Therefore, nodes can be trusted =1 or untrusted =0. These trust values needs to be recalculated frequently depend on the experiment time. In order to save power in MANET, if the node is untrusted three successive times, then the recalculation of TTSV will be longer.

The third stage is rehabilitation or resetting trust values. This stage rehabs misbehaving nodes so they can be used in future transmissions. Equation below shows the duration time that TTSV is calculated.

$$CTV = \frac{\text{ETT}}{3} \qquad (3)$$

The Check Trust Value (CTV) determines the number of times taken to calculate the TTSV for nodes, and ETT means Equation Total Time and that indicates the experiment duration. If the node has TTSV equals zero for three successive times then the CTV is calculated as follows.

$$CTV = \frac{ETT}{2} \qquad (4)$$

B. Trust Enhanced Anonymous on-demand routing Protocol (TEAP)

TEAP is a method based on using trust concept between nodes. TEAP is based on using an anonymity concept for an informant that identify and report abnormalities in the network. In TEAP, if a node does not send any cooperative messages then it is considered as an abnormal node to other nodes. Moreover, if various claims are sent by node, then it is also termed as a misbehaving node. Furthermore, TEAP is based on terms of broadcast with trapdoor information in order to detect misbehaving nodes anonymously in the network. In addition, TEAP is designed in terms of broadcast with trapdoor information in order to detect misbehaving activities anonymously in the network.

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

It is essential to explain the performance of the grayhole attack. In grayhole attack the malicious node 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 can perform numerous attacks by subverting the AODV protocol as it does not have any security methods. For example, routing message integrity and data origin authentication at every receiving node are important. A compromised node impersonates the sender of routing packets or can change the sequence number in RREQ /RREP messages. Moreover, routing information could be modified which leads to inconsistency in the network. Furthermore, routing tables might contain incorrect information regarding the network topology. Thus, changes in sequence number can result in routing loops.

IV. EVALUATION

In order to evaluate the effectiveness of MrDR method we compare it to TEAP method. We use Network Simulator (NS2). There are 72 nodes in this experiment. Two factors are measured the packet delivery ratio and the network overhead. Regards the aspects of packet delivery ratio after detecting malicious activities is shown in Figure 2. The performance of the MrDR in detecting the DoS attacks, here we used grayhole attacks and the performance of MrDR is upper in the aspect of packet delivery ratio than TEAP performance after isolating the malicious nodes from communications.

TEAP assumes that the node is a misbehaving one when it does not send cooperative messages to nodes within the network. Moreover, when multiple claims are received about a specific node being abnormal then it is become a misbehaving node. In MrDR, many trust values need to be calculated to determine the node is normal or not.

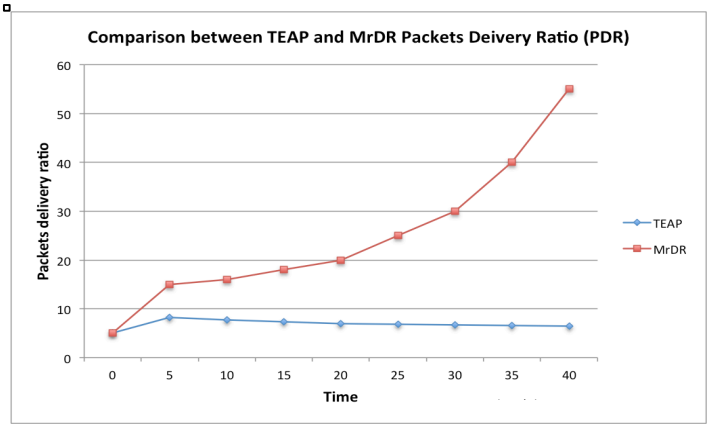

Figure 2. Packet delivery patio in both MrDR and TEAP

In Figure 3, network overhead is measured in both MrDR and TEAP. In this situation TEAP consumes energy and exhausts network resources more than MrDR. From findings MrDR method has a smaller scale of network overhead compared to the TEAP method.

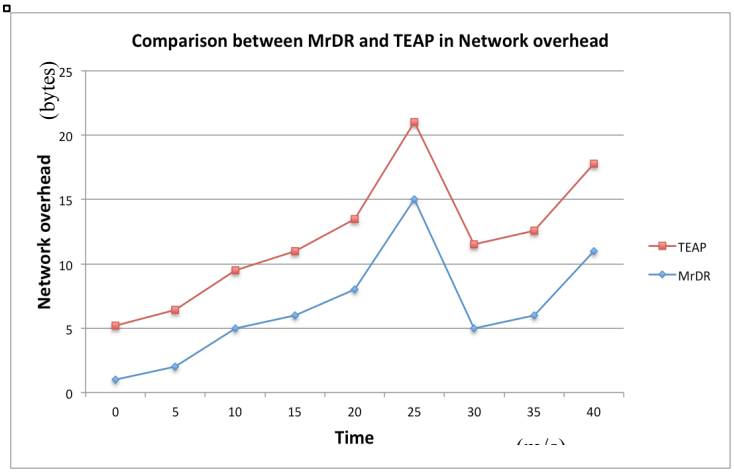

Figure 3. Network overhead in both MrDR and TEAP

I. CONCLUSTION AND FUTURE WORK

MANET with its characteristics such as dynamic topology and the absence of the administrative point becomes vulnerable to many attacks. DoS attack is a severe attack that can affect the network and degrades the network performance drastically. MrDR method is designed to detect DoS attack in MANET environment. The basic idea of this method is to calculate different trust values to determine whether the node is trusted or not. These trust values are considered to be temporal values and need to be calculated each specific time based on the nodes behaviours. MrDR method is based on calculating three trust values: ATV; RTV; and HTV. Each trust value determines specific status of the nodes and the addition of these values will give the current trust value of each node within the network. In this paper we evaluate the performance of MrDR against TEAP method which is also based on trust concept. Two factors are considered in this comparison: the packet delivery ratio and the network overhead. The comparison between these methods proves the effectiveness of the proposed method as it gives better network performance compared with TEAP.

For future work, the proposed method needs to be tested against different methods to detect DoS attacks whether they are based on trust concept or not. In addition, different DoS attacks needs to be tested in methods. In this paper we consider the grayhole attack, so in future we can consider other types of DoS attacks.

REFERENCES

1. Zain, A., et al., *MANETs performance analysis with dos attack at different routing protocols.* International Journal of Engineering & Technology, 2015. **4**(2): p. 390-398.
2. Sorathiya, D. and H. Rathod, *Algorithm to Detect and Recover Wormhole Attack in MANETs.* International Journal of Computer Applications, 2015. **124**(14).
3. Alsumayt, A. and J. Haggerty, *Using Trust Based Method to Detect DoS Attack in MANETs.* 2014.
4. Gunasekaran, M. and K. Premalatha, *TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks.* IET Information Security, 2013. **7**(3): p. 203-211.
5. Filipek, J. and L. Hudec. *Distributed firewall in Mobile Ad Hoc Networks*. in *Applied Machine Intelligence and Informatics (SAMI), 2015 IEEE 13th International Symposium on*. 2015. IEEE.
6. Gowsika, M.Y. and R. Pugazendi, *A Survey on Acknowledgment-Based IDS in Mobile Ad hoc Network (MANET).* 2014.
7. Tan, H.-X. and W.K. Seah. *Framework for statistical filtering against DDoS attacks in MANETs*. in *Embedded Software and Systems, 2005. Second International Conference on*. 2005. IEEE.
8. Tyagi, S., *Analysis Of Techniques For Mitigating Dos Attacks In MANET.* International Journal of Engineering, 2013. **2**(4).
9. Vegda, M.A.K. and M.N. Sahu, *DDoS Attacks Detection and Traceback by Using Relative Entropy.* 2015.
10. Jin, X., et al., *ZSBT: A novel algorithm for tracing DoS attackers in MANETs.* EURASIP Journal on Wireless Communications and Networking, 2006. **2006**(2): p. 82-82.

11. Varadharajan, V. and U. Tupakula, *Securing wireless mobile nodes from distributed denial - of - service attacks.* Concurrency and Computation: Practice and Experience, 2014.
12. Liu, Z., A.W. Joy, and R. Thompson. *A dynamic trust model for mobile ad hoc networks*. in *Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of*. 2004. IEEE.
13. Sun, Y., Z. Han, and K.R. Liu, *Defense of trust management vulnerabilities in distributed networks.* IEEE Communications Magazine, 2008. **46**(2): p. 112-119.
14. Chang, B.-J. and S.-L. Kuo, *Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs.* Vehicular Technology, IEEE Transactions on, 2009. **58**(4): p. 1846-1863.
15. Khan, R. and A. Vatsa, *Detection and control of DDOS attacks over reputation and score based MANET.* J Emerg Trends Comput Inf Sci, 2011. **2**(11): p. 646-655.
16. Alsumayt, A., J. Haggerty, and A. Lotfi. *Comparison of the MrDR method against different DoS attacks in MANETs*. in *Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference on*. 2015. IEEE.