symmetry

IMPACT FACTOR 2.940

CITESCORE 4.3

Article

Man-in-the-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation

Mahmood A. Al-Shareeda and Selvakumar Manickam

Special Issue

Optical and Wireless Communications towards 6G Networks

Edited by

Dr. Rogério Dionísio, Prof. Dr. Ali Jamoos and Dr. Hai Dao Thanh

MDPI

https://doi.org/10.3390/sym14081543

symmetry

MDPI

Article

Man-in-the-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation

Mahmood A. Al-Shareeda and Selvakumar Manickam *

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang 11800, Malaysia; m.alshareeda@nav6.usm.my
* Correspondence: selva@usm.my; Tel.: +604-653-3004

Abstract: Mobile ad hoc networks (MANETs) are being used more and more in a variety of fields, including the environment, energy efficiency, smart transportation, intelligent agriculture, and in Internet of Things (IoT) ecosystems. They are also anticipated to play an increasingly significant role in the future of the Internet due to the strong evolution of wireless technology in recent years. Nevertheless, this inter-node communication is vulnerable to various security attacks such as Man–In-The-Middle (MITM) attacks, which are considered to be the main challenge in MANETs. This happens when a harmful node intercepts data shared by legal nodes. Therefore, the main goal of this work is to investigate the impact of attackers' strategies to execute MITM assaults in MANETs, such as message-delayed and message-dropped assaults. The output of this work shows that these assaults have a severe impact on legal entities in MANETs as the network experiences a high number of compromised messages as well as high E2ED and PLD. Finally, by using symmetry or asymmetry cryptographies, our proposal will avoid MITM attacks that intercept the communication between legal nodes.

Keywords: mobile ad hoc network (MANET); Man-In-The-Middle (MITM) attack; security issue; message delayed; message dropped

Citation: Al-Shareeda, M.A.; Manickam, S. Man-in-the-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation. *Symmetry* **2022**, *14*, 1543. https://doi.org/10.3390/sym14081543

Academic Editors: Rogério Dionísio, Ali Jamoos and Hai Dao Thanh

Received: 29 June 2022
Accepted: 26 July 2022
Published: 27 July 2022

1. Introduction

Wireless technology may be managed by a core infrastructure that regulates the connections between network nodes, or it may operate as an infrastructure-free system known as an ad hoc network [1,2]. The mobile ad hoc network (MANET) is a class of wireless ad hoc network (WANET) that provides a large number of applications in various fields [3,4].

The main characteristics of MANET include its fast deployable wireless network, and the fact that it is self-organizing as well as infrastructure-less. As a result, they are incredibly suitable for use in unique outdoor events, communication in areas without a crises, radio infrastructure, natural catastrophes, and military operations, among others [5,6]. Figure 1 explains the structure of MANET in various fields, where message sharing is achieved by connecting nodes to each other via wireless communication [7].

According to [8], there are several types of security attacks in MANET, including the black hole attack, worm hole attack, snooping attack, routing attack, session hijacking, man-in-the-middle attack, and traffic analysis attack. The main aim of these attacks is to inject fault packets into the network. Therefore, security should be considered carefully.

Typically, the MANET operates under the supposition that every node is a trustworthy node. However, in reality, there are some harmful nodes that misbehave and launch assaults in networks; an example is the "man-in-the-middle (MITM)" assault, where the harmful nodes interpret the communication line between the source and the destination in order to disturb the MANET [9,10].

MITM assaults are regarded as significant threats in MANET because they give harmful nodes the ability to delay or drop important network information. Attackers can

perform MITM assaults in two ways, i.e., actively or passively. As a result, we propose a study that addresses this research gap by taking into account two types of MITM attackers and by examining the effects of these attackers on the MANET. The major contributions of our work are as follows.

- We discovered two types of MITM attackers in the MANET, each of which had unique skills such as message dropping and message delaying;
- We determined various strategies of the MITM attacker according to the stationary mobility of legal nodes and the distribution of the harmful nodes in the MANET;
- We implemented a model based on simulation in order to estimate the influence of the attackers' patterns.

Figure 1. Illustration of the mobile ad hoc network (MANET) structure.

The remainder of this paper is organized as follows. Section 2 reviews some studies on MITM assaults. Section 3 identifies the MITM assaults in MANET. Section 4 describes the simulation environment of this paper. Section 5 provides the results and a discussion. Finally, we conclude our work in Section 6.

2. Related Work

In this section, we review some studies on MITM assaults. Chen et al. [11] investigated a mathematical model for MITM assaults on SSL protocols in wired technology. Stricot et al. [12] proposed the classification of HTTPs by categorizing the assailants into four layers, i.e., vulnerability, behavior, target, and state. Conti et al. [13] provided a review about MITM assaults on OSI layers based on two mobile communication technologies, i.e., UMTS and GSM. Glass et al. [14] investigated the influence of MITM assaults on the MAC layer for wireless communications. Kaplanis et al. [15] investigated MITM assaults through WiFi technology.

A large amount of research [16–24] has been performed to address MITM assaults in a vehicular ad hoc network (VANET). Alazzawi et al. [16] proposed a security protocol based on elliptic curve cryptography for signing messages and verifying signatures in order to avoid the occurrence of MITM assaults. Ali et al. [24] proposed a hybrid approach that secures communication between nodes in order to avoid MITM assaults.

Recently, Abass et al. [25] proposed a key exchange-based Diffie–Hellman protocol to secure MITM attacks in MANET. Sowah et al. [26] used artificial neural network (ANN)-based predictive techniques for detecting and preventing MITM assaults in MANET.

Evidently, MITM assaults are severe in MANET, and there is no research that directly analyzes and evaluates a comparison of the two modes of MITM assaults. To close this gap, we have constructed and assessed two kinds of MITM assaults in the MANET as part of our simulation-based research.

3. Man-in-the-Middle Attacks

The phrase "Man-in-the-Middle" was coined in a basketball game, where a player in the middle attempts to intercept the ball as the two other players attempt to pass it [27,28]. A similar idea is used in MANET, where MITM attackers put legal nodes' communications at risk by altering their messages. Such assaults have serious effects on the communication, particularly if the message's content includes information about safety. In MANET, the attacker should meet the following two requirements in order to execute an MITM assault: (1) The attacker node must receive a message containing significant information; (2) The assailant should be capable of interpreting the message's content. Figure 2 shows two ways in which MITM assaults can be initiated in the MANET.

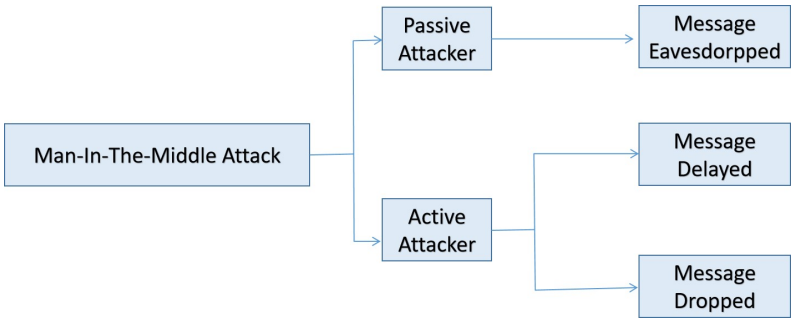

Figure 2. MITM attacks in MANET.

- Passive Mode: The communication line between legal nodes can be passively eavesdropped on by an attacker.
- Active Mode: Attackers have the active capability to delay or drop the content of data that is received in a communication.

Figure 3 illustrates the explanation for both the active and passive modes of MITM assaults in MANET. We can observe that passively, the MITM assailant can eavesdrop on the channel involving valid nodes, and actively, the MITM assailant can drop or delay the legal data that are broadcast over the system.

Figure 3. Illustration of both the active and passive modes of MITM assaults in MANET.

- MITM as Message Delayed: The successful delivery of messages to each valid node is essential to the operation of MANET. In this assault architecture, the harmful nodes purposefully pass the messages on to the neighboring nodes with a "delay" factor. Since MANET communications are extremely sensitive, delaying such signals might have disastrous effects on the network.
- MITM as Message Dropped: This kind of assault also indicates a "black hole" assault in MANET, which is when the attacker willfully drops the valid message they have

just received, hence preventing further valid message propagation. As a result, the assailant prevents the valid node from receiving any communication, which then prevents the messages from reaching their intended recipients. Dropping the messages can have a big effect on the network because they carry delicate data, such as in collision avoidance. Imagine an instance where valid nodes are supposed to announce the presence of black ice on the path.

4. Environment of Simulation

4.1. Setup of Simulation

The main goal of our experiment was to investigate the performance of the MANET in the presence of harmful nodes launching MITM assaults. To simplify our simulation, this paper made use of the INET framework [29] and NETwork Attacks (NETA) [30], as depicted in Figure 4.

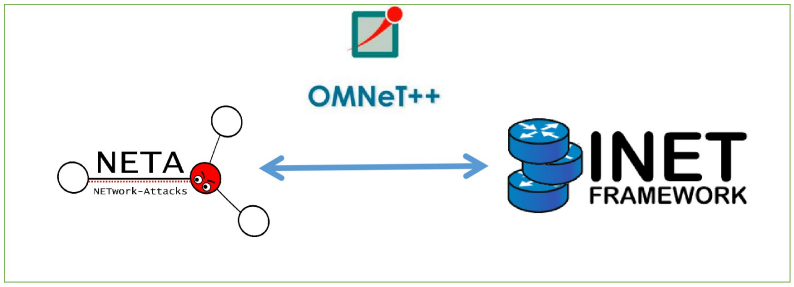

Figure 4. Workflow of frameworks in OMNeT++.

The INET framework is an OMNeT++ model [31]-based open-source suite for MANET. NETA is a framework devised to imitate assaults in MANET by utilizing OMNeT++ and the INET framework. OMNET++ describes several modules (PHY layer and MAC layer, application layer) to satisfy the actual system manner.

- Scenario one: Assailants are dispersed randomly throughout the system;
- Scenario two: Assailants are gathered in a fleet configuration.

4.2. Simulation Scenario Setup

To estimate the performance of MITM assaults in MANET, this paper made use of the default simulation in OMNeT++, as depicted in Figure 5. We introduced 100 nodes into the system; the message was shared by nodes. We then injected 1, 3, 5, and 7 harmful nodes into the system to investigate the influence of attackers' strategies, where the assailant either dropped or delayed the exchanged data. Subsequently, we selected a single-source node (e.g., Node[0]) to broadcast the UDP packets and a single-destination node (e.g., Node[20]) to receive them. Note that the source node broadcast the packets to all nodes within its coverage area, while the destination address was unicast. Table 1 describes many of the simulation-related parameters.

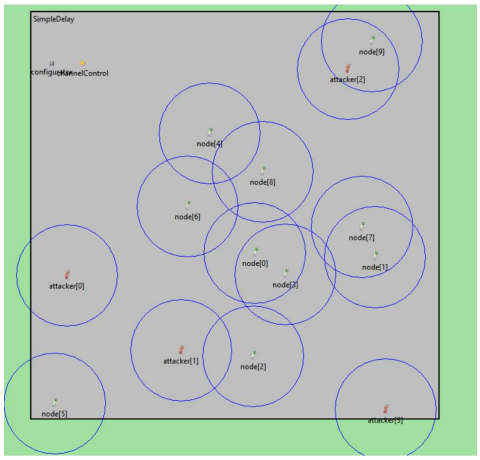

Figure 5. Snapshot of OMNeT++.

Table 1. Simulation Details.

Parameters	Values
Network Simulator	OMNeT++ 4.3
MANET Simulator	INET Framework 2.1.0
NETwork Attacks	NETA v1-1.0
No. of Nodes	100
No. of Harmful Node	1, 3, 5, 7
Simulation Area	3.0 km · 3.0 km
Simulation Time	1000 s
Node Mobility	Stationary
Source Application	UDPBasicApp
Destination Application	UDPSink
Packet Size	512 B
Send Interval	0.5 s + uniform (−0.001 s, 0.001 s)
MAC Standard	802.11 g
Number of Repetitions	4
Bit Rate	54 Mbps
Routing Protocol	AODVUU
AODVUU Type	Link Layer Feedback
Transmitter Power	2.0 mW
Sensitivity	−85 dBm
Thermal Noise	−110 dBm
Carrier Frequency	2.4 GHz
Path Loss Alpha	2

4.3. Performance Evaluation Metrics

This section explains the evaluation criteria used to estimate the performance of MANET in the presence of assailants.

- End-to-End Delay (E2ED): The E2ED refers to the delay experienced by a packet that has been issued by the legal node and which is to be shared with neighboring nodes. The E2ED is a metric related to the quality of service (QoS) of the network, as shown in the following equation:

$$\text{E2ED} = T_R - T_G \tag{1}$$

  where T_R is the packet reception time, and T_G is the packet generation time. Hence, E2ED is the difference of T_G and T_R.
- Packet Loss Ratio (PLR): The PLR indicates the amount of data that is lost due to MITM nodes, as expressed by the following equation:

$$\text{PLR} = \frac{M_L}{M_T} \tag{2}$$

where M_T is the overall number of messages received, and M_L is the total number of messages lost. Therefore, PLR is the difference of M_T and M_L. More specifically, the total number of messages M_T includes messages received at both the legal node M_R and the harmful node M_L, as shown in the following equation:

$$M_L + M_R = M_T \tag{3}$$

- Amount of delayed messages: This indicator displays the number of data that the rogue node has delayed.
- Amount of dropped messages: The dropping of messages from legal nodes is the statistic that is defined for MITM. The number of messages discarded by network attackers is indicated by this measure.

5. Results and Discussion

Here, we firstly show the output of our work for message-delayed and message-dropped MITM assaults in MANET. Then, we concentrate on the discussion of a few potential solutions to help in resisting MITM assaults.

5.1. Simulation Results

In this section, we present the results of MITM assaults in MANET by simulating MITM assailants and evaluating the system performance according to the metric of evaluation explained above. Moreover, each experiment was carried out ten times with a random seed amount and in four repetitions to satisfy an individual initial node assignment within the system.

5.1.1. Message-Delayed Assaults

Figure 6 depicts E2ED in the presence of MITM, which caused message delays of 2 ms. It is clear that adding harmful nodes that delay valid communications within the network causes the E2ED to rise. Nevertheless, an MITM assailant with message-delaying capabilities prevent the legal nodes from receiving the messages on time. Ideally, the legal nodes should receive such legal communications with the least amount of delay. Additionally, Figure 6 shows that E2ED grows as assailants are dispersed around the network.

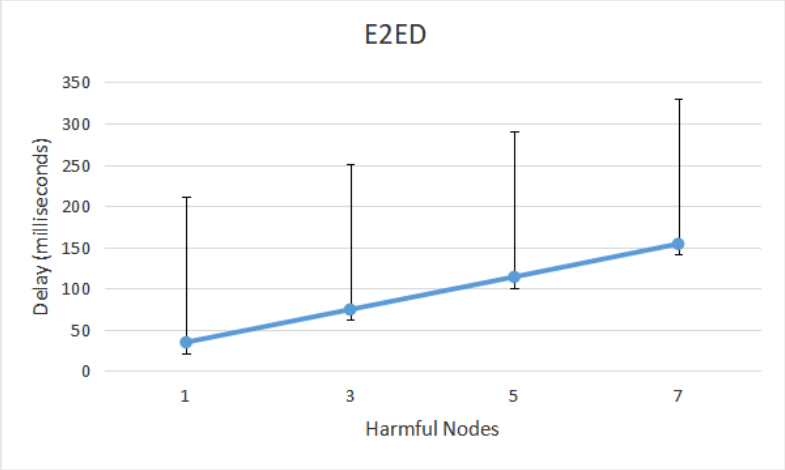

Figure 6. End-to-End delay caused by message-delayed assaults.

Next, Figure 7 shows the number of delayed messages produced by the harmful nodes. It is evident that when harmful nodes proliferate in the network, the number of delayed messages rises. The delayed messages increase to 55.02% when seven assailants are introduced into the network.

Figure 8 shows the Packet Loss Ratio (PLR) in the presence of harmful nodes. It demonstrates that PLR rises as the number of harmful nodes in the network rises. For example, when the network was flooded with seven harmful nodes, about 55.11% more packets were lost in the presence of attackers. Based on our experiment, this is because the destination that discarded the packets due to the excessive delay was in the presence of harmful nodes.

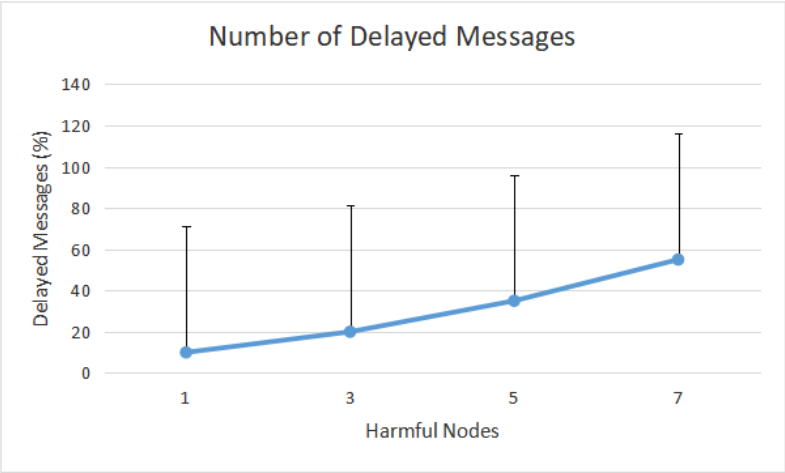

Figure 7. Delayed messages caused by message-delayed assaults.

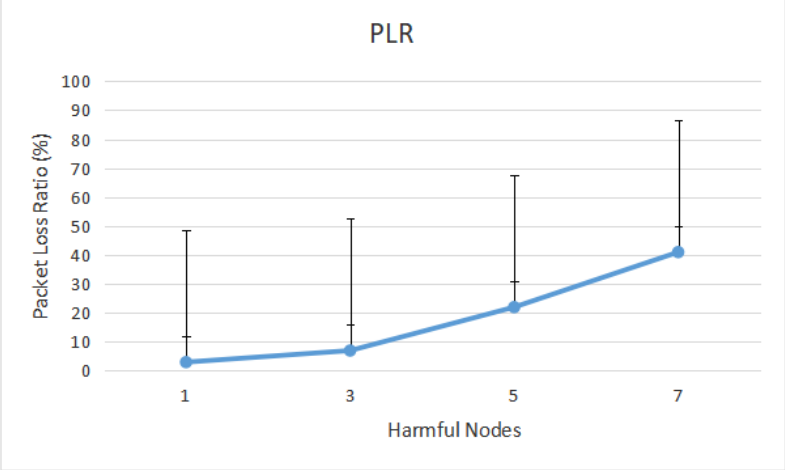

Figure 8. Packet Loss Ratio from message-delayed assaults.

5.1.2. Message-Dropped Assaults

Figure 9 depicts E2ED in the presence of MITM, which caused a message drop of 2 s. It is clear that adding harmful nodes that drop valid communications within the network causes the E2ED to rise. However, MITM attackers with message-dropping capabilities prevent the legal nodes from receiving all messages. Ideally, the legal nodes should receive all messages without dropping them. Additionally, Figure 9 shows that E2ED grows as attackers are dispersed around the network.

Next, Figure 10 illustrates the number of messages dropped by harmful nodes and suggests that a high number of messages are discarded when the proportion of harmful nodes in the network increases. For instance, with five attackers in the network, the simulation dropped 1721 messages.

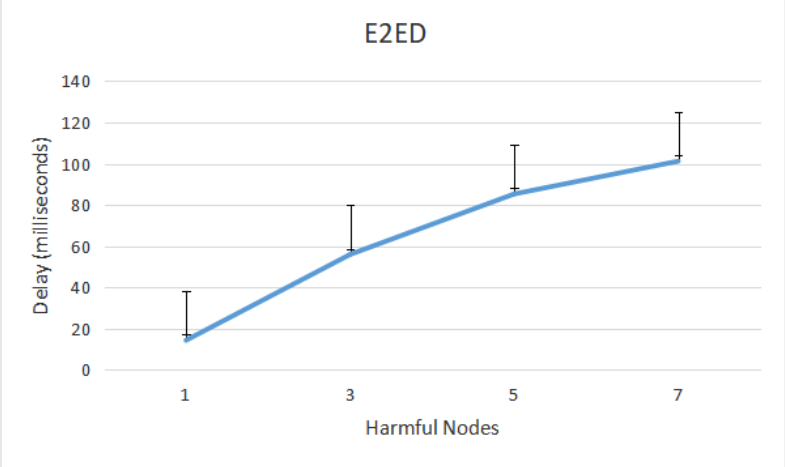

Figure 9. End-to-End Delay caused by message-dropped assaults.

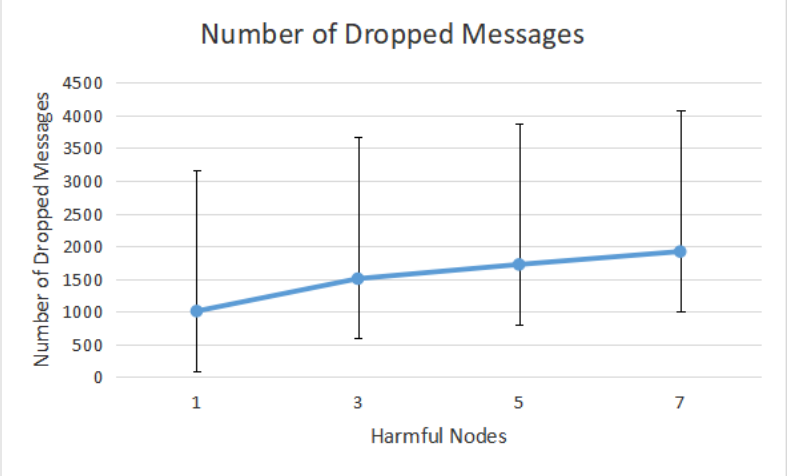

Figure 10. Dropped messages caused by message-dropped assaults.

Figure 11 shows PLR in the presence of harmful nodes. It demonstrates that PLR rises as the number of harmful nodes in the network rises. For example, when the network is flooded with five harmful nodes, only about three packets are received by the destination in the presence of attackers, as shown in Figure 12.

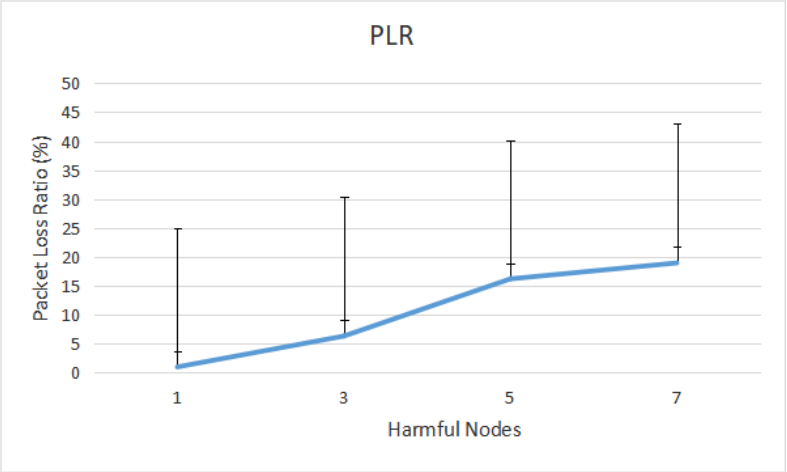

Figure 11. Packet Loss Ratio from message-dropped assaults.

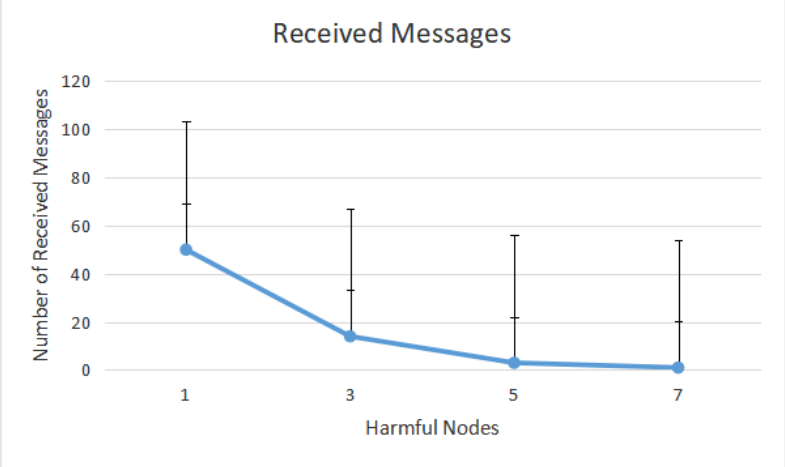

Figure 12. Number of received messages after message-dropped assaults.

5.2. Discussion

It is evident from the subsections above that the messages delayed and messages dropped due to MITM assaults have a high influence on the MANET. In this paper, the network in this scenario presented high E2ED, the propagation of a high number of delayed messages and dropped messages, and higher PLR. Thus, in order to achieve a secure approach in MANET, these MITM metrics must be considered prior to deployment in a real scenario. For example, singing and verifying messages can decrease the probability of broadcasting forage data among nodes in the MANET. Moreover, approaches based on trust can also be applied within the system to resist MITM assaults with delaying and dropping abilities. An environment based on trust can enable the legal nodes to determine and estimate the validity and authenticity of the received messages, therefore decreasing the probability of assailants executing MITM assaults. Similar to this, another plausibility verification inside the network may also prove to be useful in limiting the spread of harmful messages. These verification steps may be established according to the message threshold and detection ranges, the data approval area, and different mobility-controlled factors such as the direction and speed of the nodes. Therefore, symmetry or asymmetry cryptographies should be executed in order to encrypt the messages exchanged among the nodes. As a result, our proposal will prevent MITM attacks from intercepting communications between legal nodes.

6. Conclusions

MANET is a fast and deployable wireless network, and it is self-organizing as well as infrastructure-less. Nevertheless, since MANET has the most open channels, it is vulnerable to several assaults, such as MITM assaults. We performed a detailed evaluation of the influence of MITM attackers in MANET. We simulated two types of MITM assaults (delayed messages and dropped messages) in MANET to investigate the impact that these caused. The simulation of MITM assaults was carried out in OMNeT++ with the use of NETA and the INET frameworks. Our results show that these two types of assaults have a huge influence on the network in terms of high E2ED, delayed messages, dropped messages, and PLR.

We will expand on this paper's findings in future work by assessing the impact of the MITM assault models in accordance with the nodes' mobility and routing protocols for diverse MANET situations. Additionally, based on the literature analysis, we will expand this research by choosing appropriate landscape areas as well as landscape areas within MANET. Moving forward, our focus will also be on developing a trust-based strategy aimed at defending against MITM attacks in MANET.

Author Contributions: Conceptualization, writing—review and editing, M.A.A.-S.; writing—original draft preparation, investigation, supervision, S.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Vice Chancellor Initiative Allocation, Universiti Sains Malaysia grant number 311/PNAV/4119101.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that they have no conflict of interest to report regarding the present study.

References

1. Hamdi, M.M.; Mustafa, A.S.; Mahd, H.F.; Abood, M.S.; Kumar, C.; Al-shareeda, M.A. Performance Analysis of QoS in MANET based on IEEE 802.11 b. In Proceedings of the 2020 IEEE International Conference for Innovation in Technology (INOCON), Bangalore, India, 6–8 November 2020; pp. 1–5.
2. Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks. *Int. J. Eng. Manag. Res.* **2020**, *10*, 153–158. [CrossRef]
3. Yasin, A.; Abu Zant, M. Detecting and isolating black-hole attacks in MANET using timer based baited technique. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 9812135. [CrossRef]
4. Al-shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network. *Symmetry* **2020**, *12*, 1687. [CrossRef]
5. Veeraiah, N.; Khalaf, O.I.; Prasad, C.; Alotaibi, Y.; Alsufyani, A.; Alghamdi, S.A.; Alsufyani, N. Trust aware secure energy efficient hybrid protocol for manet. *IEEE Access* **2021**, *9*, 120996–121005. [CrossRef]
6. Kausar Fatima, S.; Gauhar Fatima, S.; Abdul Sattar, S.; Mohd Ali, S. Mobile Adhoc Networks Security Challenges: A Survey. *Int. J. Adv. Res. Eng. Technol.* **2019**, *10*, 224–237.
7. Saed, M.; Aljuhani, A. Detection of Man in The Middle Attack using Machine learning. In Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 25–27 January 2022; pp. 388–393.
8. Dorri, A.; Kamel, S.R.; Kheirkhah, E. Security challenges in mobile ad hoc networks: A survey. *arXiv* **2015**, arXiv:1503.03233.
9. Javeed, D.; MohammedBadamasi, U.; Ndubuisi, C.O.; Soomro, F.; Asif, M. Man in the middle attacks: Analysis motivation and prevention. *Int. J. Comput. Netw. Commun. Secur.* **2020**, *8*, 52–58. [CrossRef]
10. Shekhar, S.; Mahajan, M.; Kaur, S. A Comprehensive Review of Various Attacks in Mobile Ad Hoc Networks. In Proceedings of the 2022 IEEE 6th International Conference on Trends in Electronics and Informatics (ICOEI), Cheranmahadevi, Tirunelveli, India, 28–30 April 2022; pp. 638–643.
11. Chen, Z.; Guo, S.; Duan, R.; Wang, S. Security analysis on mutual authentication against man-in-the-middle attack. In Proceedings of the 2009 IEEE First International Conference on Information Science and Engineering, Nanjing, China, 26–28 December 2009; pp. 1855–1858.
12. Stricot-Tarboton, S.; Chaisiri, S.; Ko, R.K. Taxonomy of Man-in-the-Middle Attacks on HTTPS. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 527–534.
13. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. [CrossRef]
14. Glass, S.M.; Muthukkumarasamy, V.; Portmann, M. Detecting man-in-the-middle and wormhole attacks in wireless mesh networks. In Proceedings of the 2009 IEEE International Conference on Advanced Information Networking and Applications, Bradford, UK, 26–29 May 2009; pp. 530–538.
15. Kaplanis, C. Detection and Prevention of Man in the Middle Attacks in Wi-Fi Technology. Ph.D. Thesis, Aalborg University, Aalborg, Denmark, 2015.
16. Alazzawi, M.A.; Al-behadili, H.A.; Srayyih Almalki, M.N.; Challoob, A.L.; Al-shareeda, M.A. ID-PPA: Robust identity-based privacy-preserving authentication scheme for a vehicular ad-hoc network. In Proceedings of the International Conference on Advances in Cyber Security, Penang, Malaysia, 8–9 December 2020; Springer: Singapore, 2020; pp. 80–94.
17. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. A Secure Pseudonym-Based Conditional Privacy-Preservation Authentication Scheme in Vehicular Ad Hoc Networks. *Sensors* **2022**, *22*, 1696. [CrossRef] [PubMed]
18. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Password-Guessing Attack-Aware Authentication Scheme Based on Chinese Remainder Theorem for 5G-Enabled Vehicular Networks. *Appl. Sci.* **2022**, *12*, 1383. [CrossRef]
19. Al-Shareeda, M.A.; Manickam, S.; Mohammed, B.A.; Al-Mekhlafi, Z.G.; Qtaish, A.; Alzahrani, A.J.; Alshammari, G.; Sallam, A.A.; Almekhlafi, K. CM-CPPA: Chaotic Map-Based Conditional Privacy-Preserving Authentication Scheme in 5G-Enabled Vehicular Networks. *Sensors* **2022**, *22*, 5026. [CrossRef] [PubMed]

20. Al-Shareeda, M.A.; Manickam, S.; Mohammed, B.A.; Al-Mekhlafi, Z.G.; Qtaish, A.; Alzahrani, A.J.; Alshammari, G.; Sallam, A.A.; Almekhlafi, K. Chebyshev Polynomial-Based Scheme for Resisting Side-Channel Attacks in 5G-Enabled Vehicular Networks. *Appl. Sci.* **2022**, *12*, 5939. [CrossRef]
21. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. SE-CPPA: A Secure and Efficient Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks. *Sensors* **2021**, *21*, 8206. [CrossRef] [PubMed]
22. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Access* **2021**, 9, 113226–113238. [CrossRef]
23. Al-Shareeda, M.A.; Anbar, M.; Alazzawi, M.A.; Manickam, S.; Al-Hiti, A.S. LSWBVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network. *IEEE Access* **2020**, *8*, 170507–170518. [CrossRef]
24. Ali, I.; Lawrence, T.; Omala, A.A.; Li, F. An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 11266–11280. [CrossRef]
25. Abass, R.; Habyarimana, A.; Tamine, K. Securing a mobile ad hoc NETwork against the man in the middle attack. *Int. J. Artif. Intell. Inform.* **2022**, *3*, 53–62. [CrossRef]
26. Sowah, R.A.; Ofori-Amanfo, K.B.; Mills, G.A.; Koumadi, K.M. Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN). *J. Comput. Netw. Commun.* **2019**, *2019*, 4683982. [CrossRef]
27. Nayak, G.N.; Samaddar, S.G. Different flavours of man-in-the-middle attack, consequences and feasible solutions. In Proceedings of the 2010 3rd IEEE International Conference on Computer Science and Information Technology, Chengdu, China, 9–11 July 2010; Volume 5, pp. 491–495.
28. Ahmad, F.; Adnane, A.; Franqueira, V.N.; Kurugollu, F.; Liu, L. Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies. *Sensors* **2018**, *18*, 4040. [CrossRef] [PubMed]
29. Mészáros, L.; Varga, A.; Kirsche, M. Inet framework. In *Recent Advances in Network Simulation*; Springer: Berlin, Germany, 2019; pp. 55–106.
30. Sánchez-Casado, L.; Rodríguez-Gómez, R.A.; Magán-Carrión, R.; Maciá-Fernández, G. NETA: Evaluating the effects of NETwork attacks. MANETs as a case study. In Proceedings of the International Conference on Security of Information and Communication Networks, Cairo, Egypt, 3–5 September 2013; Springer: Berlin, Germany, 2013; pp. 1–10.
31. Varga, A. OMNeT++. In *Modeling and Tools for Network Simulation*; Springer: Berlin, Germany, 2010; pp. 35–59.