EFFECT MAN-IN THE MIDDLE ON THE NETWORK PERFORMANCE IN VARIOUS ATTACK STRATEGIES

Iyas Alodat

Department of Computer and Information System,
Jerash University, Jerash, Jordan

ABSTRACT

In this paper, we examined the effect on network performance of the various strategies an attacker could adopt to launch Man-In The Middle (MITM) attacks on the wireless network, such as fleet or random strategies. In particular, we're focusing on some of those goals for MITM attackers - message delay, message dropping. According to simulation data, these attacks have a significant effect on legitimate nodes in the network, causing vast amounts of infected packets, end-to-end delays, and significant packet loss.

KEYWORDS

Wireless Network, Mobile Network, security; Man-In-The-Middle Attack; smart cities; simulation; Intelligent Transportation System; Internet-of-Things.

1. INTRODUCTION

A wireless ad hoc network is a set of nodes that communicate wirelessly. These networks are decentralized, meaning they don't rely on a pre-existing infrastructure to set up their network topology [1][2][3]. It also refers to the communication between wireless network points (access points) without the use of a router or a central intermediary. To put it another way, each network point has a professional task for doing, i.e. (Ad hoc).

With the widespread use of smartphones, the first thing we look for when entering a cafe or restaurant is to turn on the Wi-Fi. If the Wi-Fi network has a password, it must be entered so that everyone can use the Internet to access social networking sites and other applications. The speed of connection to free Wi-Fi networks is also something we see in any other public place! Unfortunately, we are unaware of the dangers of using free public Wi-Fi networks and the consequences that can result...!? It appears that free public Wi-Fi networks pose a serious threat to the user's personal information. Thousands of people have been harmed as a result of them, and large-scale violations are common in public places. It appears that free public Wi-Fi networks present a danger to the user's personal information. Thousands of people have been harmed as a result of them, and large-scale violations are common in public places with shared free hotspots. All open Wi-Fi networks that are distributed to the Internet, whether in cafes or public places, are vulnerable to total penetration, and even your penetration.

When you connect to the Internet through a password-protected network, an encrypted tunnel is created between your computer and the router that distributes the Internet [5]. Your information passes through it, ensuring that your data is secure if a hacker attempts to obtain it. The strength of the password you use determines the strength of this tunnel that protects you, your personal

data, and your information. However, it will not be discovered when you connect to public open networks that do not have a password and do not have this tunnel. The hacker can then obtain your information as it passes through the network through some means.

But the knowledgeable hacker would consider something new in technology. Of course not; this is a tough traditional technique that a hacker is currently employing, but he is doing the best he can. It builds a fake free Wi-Fi network to confuse users into thinking it's a secure hotspot [6]. Users make direct contact through it, completely oblivious to the fact that they are its ready prey for penetration. Users can use the internet as usual in this case. If they purchase over the internet. Enter the information with bank card, and all of information and data will be sent to the hacker who created the fake Wi-Fi hotspot [7].

The question that arises in this situation. Is it possible for a hacker to overcome the site's high-encryption HTTP protection? The encryption Https is a little tricky to crack. But we keep in mind that this is a hacker's profession, and he will undoubtedly be able to overcome it. It makes use of tools that make decoding the HTTP protocol an ease. User's information will be sniped in this case without even realizing it [8].

1.1. Related Work

Man-In-The-Middle (MITM) attacks are well known attacks in computer security MITM attacks are mapped at the Open Systems Interconnection (OSI) layers of two mobile communication architectures, namely the Global System for Mobile Communications (GSM) and Universal Mobile Communications (UMTS), in a detailed survey. By your OSI sheet in addition, Glass et al. Examine the impact of MITM attacks on ad hoc and cellular mobile networks' MAC layers [28]. The authors took advantage of the network's optimistic accept property to reveal and recognise compromised nodes engaged in MITM attacks, resulting in high detection rates and no false positives. Similarly, Kaplanis looked at MITM attacks on WiFi networks in [29]. The lack of encryption over the data link layer, according to the author, offers a perfect medium for attackers to conduct MITM attacks.

The author also offers a solution for dealing with MITM attacks on WiFi networks. MITM attacks are investigated on both wired and wireless technologies in general.

MITM attacks on wired networks were proposed by Stricot-Tarboton et al. [25] and Chen et al. [26]. Through MITM's classification of HTTPS, it categorizes attackers into four categories: status, target, actions, and vulnerability. On the other hand, the focus was on a statistical model of MITM attacks on network adapter Secure Sockets Layer (SSL) protocols [27].

2. TYPES OF WIRELESS ATTACKS

WiFi networks are susceptible to a wide range of attacks. As a result, it's critical to be aware of them so that we can take the necessary steps to prevent and minimize their impact.
Bellow we will find out in-depth information on these attacks:

2.1. Rogue Wireless Devices

A rogue wireless device, also known as an access point, is an unauthorized WiFi device that is not managed by the network administrators. They provide a way into the network for potential attackers. If an attacker has direct access to the wired network, this type of device may be

maliciously installed, but they are more often than not added by employees who are unaware of the risks [9].

2.2. Peer-to-peer Attacks

Devices connected to the same access point may be vulnerable to attacks from other access point devices. Most service providers offer a feature called "Client Isolation," which prevents clients connected to the access point from communicating with one another [10].

2.3. Eavesdropping

Wireless communications are controlled in this area. Snooping can be divided into two categories. Casual snooping, also known as WLAN discovery, is when a wireless client actively searches for available wireless access points. Malicious snooping is the unlawful kind of snooping. Someone is attempting to listen in on data exchanged between customers and the access point. As a result, it is critical to encrypt these networks, as anything not encrypted can be intercepted [11].

2.4. Encryption Cracking

The attacker tries to break the network's encryption. WEP networks are the most vulnerable to this, as they can be cracked in as little as five minutes. It's critical to use the most secure encryption possible, and to avoid using WEP whenever possible [12].

2.5. Authentication Attacks

An attacker scrapes a frame exchange between a client’s authenticating with the network and then runs an offline dictionary attack on it.

With this kind of information, and depending on the password's strength, it may only be a matter of time before they crack it and gain access. As a result, you must keep your login credentials as safe as possible.

2.6. MAC Spoofing

Spoofing a MAC address is remarkably easy. As a result, using MAC filtering to control which devices are allowed to connect to the network is not at all secured. However, it should be used in conjunction with other security measures to create a more secure network architecture in the long run [13].

2.7. Management Interface Exploits

When we use devices like wireless controllers, which allow us to control access points via web interfaces or console access, this type of attack can become a challenge. Because default login credentials are widely available on the internet, it's critical to secure all devices to prevent unauthorized access [14].

2.8. Wireless Hijacking

When an attacker configures their laptop to broadcast as a wireless access point with the same SSID as a public hotspot, this happens. They then sit back and wait for new tourists to connect to

it, believing it to be a legitimate public hotspot. This exposes them to peer-to-peer attacks and allows them to monitor the murderer's network activity [15].

2.9. Denial of Service

DoS attacks can happen at various layers. Layer 1 attacks, also known as RF jamming attacks, can be both intentional (attacker intentionally producing a signal to cause interference) and unintentional (devices like microwaves or wireless phones causing interference). Layer 2 attacks can happen in a variety of ways. An attacker might, for example, flood and AP with forged association and disassociation requests. There are solutions available that can detect these types of attacks and allow you to take action to prevent them.

2.10. Social Engineering

Scripts, software, and tools are not used in the majority of successful hacks, contrary to popular belief. The majority of them are caused by social engineering. This is a method of solving problems to reveal sensitive information, such as computer passwords or information that will assist attackers in narrowing down possible passwords. The best way to deal with this potential threat is to make sure that everyone is aware of security processes such as changing passwords regularly and not sharing personal information [16].

3. ATTACKER HIATUS

In this section, we will see how an attacker can use hiatus for arriving to his target. Bellow we discuss kind of hiatus can attacker used.

3.1. Delay Attack

Attack speed is stored in the game's data files in two ways.

The old method was as follows: The base attack cooldown is 1.6 seconds globally (this is the time between the start of one attack to the start of another attack, as well as the time between one hit to the next hit). Note that Riot calls attack cooldown "attack delay," but we think that's unclear with the windup time, so we call it attack cooldown [17].

Each champion has a different "attack cooldown offset percent," which the wiki wrongly refers to as "attack offset" or "attack delay." This value, which is equal to 1.6 * (1 + attack cooldown offset), is used to calculate the champion's base attack cooldown. The majority of attack cooldown offsets The majority of attack cooldown offsets are 0 or negative, resulting in attack speeds of 0.625 or higher. Positive offsets result in attack speeds that are less than 0.625. (like Annie).

The inverse of the champion's base attack cooldown is then used to determine their base attack speed, which is then visually rounded off. It's important to remember that even though the game processes attack at a different speed than how it's shown, the results are the same. The attack speed maximum and minimum caps of 2.5 and 0.2 are also determined in terms of their inverses, with a 0.4 and 5.0 second cooldown time, respectively.

Bonus attack speed boosts attack speed while lowering attack cooldown in a 1:1 ratio. Because they scale inversible, the new attack speed will be X% faster than the base attack speed, and the base attack cooldown will be X% longer than the new attack cooldown [18].

The global base attack cast percent = 0.3 or 0.333 (meaning the attack would cause 30 percent or 33 percent of the time/cooldown, so the global base windup time will be 1.6 * 0.3 = 0.48). Because 0.3 is specified explicitly in a global vars file and the default offset percent is -0.3 (which would result in a default windup time of 0), we specify two values here: 0.333 provides more precise results with manual frame timings (this will be discussed a little more later).

Each champion has their own "attack cooldown cast offset percent," which is used to calculate the base attack windup/cast time, which is calculated as base attack cooldown * (0.3 + cast offset percent). Almost every character in the game has a negative cast offset (I can't think of any with a positive value), and most champions' base attack cast time is between 0.2 and 0.4 seconds.

Some champions set a value for their "attack cooldown cast offset percent attack speed ratio," which determines how much of their attack speed goes toward minimizing windup time. 1.0 is the default value. Thresh, for example, overrides this value to 0.25, which explains why "only 25% bonus on windup" is mentioned. This value has no effect on total attack speed. The full list of champions with a non-1.0 value can be found here.

There's also a safeguard in place to prevent the attacks from being accidentally canceled. Attempting to cancel the attack windup will not work because we have a two-frame buffer consisting of the frame that an attack will fire and the frame shortly before that. This buffer is approximately 0.0667 seconds since the server runs at 30 frames per second.

The following has changed with the second method: base attack speed is no longer obtained from the base attack cooldown. Instead, the base attack speed is specifically determined, and the base attack cooldown is derived from that. The removal of the "attack cooldown offset" value from the Riot API, which was later replaced with the explicit base value, is what the wiki refers to when it says the mechanic has shifted (although only the representation changed, the actual mechanics are identical).

Furthermore, the "base" and "ratio" values for base attack speed were separated. "Base" refers to your attack speed at level 1, and "ratio" refers to how bonus attack speed is compounded before being added to the base to calculate your max. The base and ratio are the same with most champions, but champions who receive bonus attack speed at level 1 have the bonus attack speed programmed into their base score, so the level 1 bonus does not count as real bonus attack speed. For eg, Yasuo has a ratio of 0.67 but a base of 0.697 (effective bonus of 4%, but does not scale with bonus attack paces, such as his Q cooldown or Stormrazor's proc cooldown).

A marginally unnecessary explicit specification of the base attack cooldown is also included, which is only relevant for characters with an overriding level 1 attack speed.

Only on newer champs/VGUs is attack windup now specifically specified as an "attack cast time" value. Despite being changed to the new method for their base attack speed/cooldown, older champions still use the old method for this value. This, like the base attack cooldown upgrade, may be changed in the future.

But how long does it take from the time the attack is issued/queued before it is finally realized? Will this be 0.3 seconds and a 1.3 second attack cooldown in the previous case, or 0.4 and 1.2, or 0.2 and 1.0, or whatever? It wouldn't matter if you continued fighting for a long time without giving other orders, but with so many attacks resets in the game, it's necessary to consider how much time this will save. Although it's clear that this attack cooldown issue can't be entirely abused by canceling after the attack with a movement order and then immediately giving another attack command, it does seem that this kind of stutter stepping cuts the effective total time by a

significant amount, it seems that stutter stepping decreases the successful overall time between attacks by at least a small amount [19].

Attack delay, also known as attack speed offset, was used to measure a champion's "base attack speed [21]." The following was the formula for this calculation [22][23]:

$AS_{base} = 0.625 / 1 +$ attack delay. (3.1)

A lower base attack speed (i.e. attacks per second) correlated with a lower attack latency, making bonus attack speed more successful.

Attack pause, contrary to common belief, has little to do with how "nice" an attack feels. Other secret variables were used to decide when an attack's wind-up is considered complete, as well as when an attack is considered to have struck - for example, some projectile-based attackers can press to move the moment the projectile is airborne, while others can "cancel" the attack at any time before the projectile hits. These variables may not be viewed or accessed.

Attack delay speed % should be converted to decimal (divide by 100) after that will multiply by level. Each delay speed example illustrate in table 1.

Table 1. Attack delay and base attack speed

	Attack delay	**Decimal**	**Precise fraction**
Standard base attack speed	0	0.625	0.625 ÷ 1
Low base attack speed	0.3	0.481	0.625 ÷ 1.3
High base attack speed	-0.1	0.694	0.625 ÷ 0.9

3.2. Dropping Attack

A router that is supposed to pass packets only discards them in a denial-of-service attack. This normally happens when a router is hacked, which can happen for a variety of reasons. A denial-of-service attack on the router using a known DDoS tool is one cause listed in the study [4]. The packet drop attack is difficult to track and avoid when packets are routinely dropped from a lossy network.

4. SIMULATION PARAMETER

Our simulation was a process attack model using Omnet++ with NETA as shown in figure 1, under windows operating system with core i5 processor and 8GB RAM. The network we have to simulate will have 100 smartphones with the small geographical area.

4.1. Data Queue Length

Is a direct measurement of the number of requests present at the time that the performance data is collected. It also includes requests in service at the time of the data collection.

4.2. Drop Packet by Queue

Packet loss in a network is usually caused by network congestion, in which packets are lost as traffic arrives at a particular router or network section at a rate that exceeds the rate at which it can be sent through for an extended period of time. A bottleneck occurs when a single router or

connection restricts the ability of the entire transport path or network travel in general. Retransmission of packets is needed for efficient packet delivery since it is required to retrieve accurate information at the destination. However, due to the extra time required for retransmission, this protocol increases latency.

4.3. Loss Rate

For real-time flows like video and VoIP, the PLR (packet loss rate) is a valuable output metric. The number of packets missed or skipped during transmission must be kept low and certain data packets are guaranteed such data rates for quick and seamless transmission. Number of packet losses of 5% to 10% of the overall packet stream would have a major impact on the consistency. For streaming audio or video, less than 1% packet loss is "fine," and 1-2.5 percent is "acceptable," according to another.

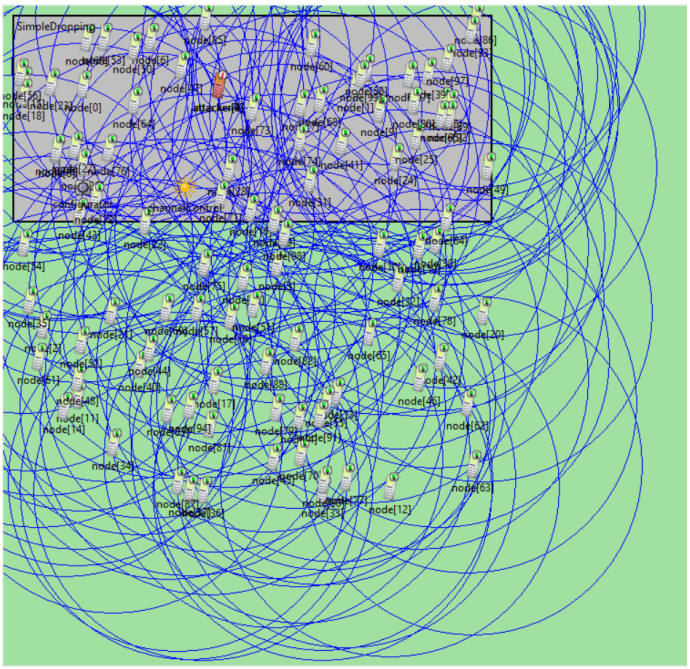

Figure 1. Network in NETA Simulation

5. PERFORMANCE EVALUATION METRICS

We applied the following assessment criteria to assess the stability of wireless networks in the presence of attackers, which can evaluate MITM attacks in networks. There are the following:

E2ED: This metric is similar to network QoS, and it indicates the delay induced by valid node packets being exchanged with neighboring nodes [20]. The discrepancy between packet generation time and packet receipt time, measured as follows:

$$E2ED = Packet_{reception} - Packet_{generation} \quad (5.1)$$

Content Delivery Ratio (CDR): The content delivery ratio indicates the number of messages successfully received by legal vehicles [4]. If M_R is the number of messages sent and M_{PRE} is the number of messages predicted to be received within the network, then CDR is [24]:

$$CDR = M_R / M_{PRE} \quad (5.2)$$

If 'N' is the cumulative number of vehicles sending 'M_{TRANS}' messages, MPRE is measured as follows:

$$M_{PRE} = N \times M_{TRANS} \quad (5.3)$$

Packet Loss Ratio (PLR): Packet loss ratio indicates how many packets are missing as a result of MITM nodes. Where the M_T is the total number of messages and the M_L is the number of messages lost, the PLR is measured as follows:

$$PLR = M_L / M_T \quad (5.4)$$

M_T MT contains all legal and malicious nodes, as well as messages. Let M_R is the number of received messages at legitimate nodes and M_L is the amount of messages lost at the MITM nodes, then M_T is given as:

$$M_T = M_R + M_L \quad (5.5)$$

Number of Compromised Messages: This statistic shows the number of messages from the malicious node that has been compromised (either tampered with or delayed).

A number of Dropped Messages: The number of messages dropped is a metric specified for MITM, which drops messages obtained from valid nodes. This statistic depicts the number of messages lost by network attackers.

6. RESULTS AND DISCUSSION

In this part, we first present the simulation results of three MITM attacks in wireless networks (message delayed, message dropped). Then we discussed some of the potential options for dealing with MITM threats.

6.1. Simulation Results

The purpose of this section is to analyze the outcomes of the MITM attack. Each simulation scenario is run ten times with a different seed value each time to ensure a specific initial system assignment in the network. Furthermore, for each simulation scenario, the simulation results presented below are the average of ten runs.

6.1.1. Message Delay Attacks

In the presence of MITM, end-to-end delay (E2E) delays packets by 2 seconds as shown in figure 4. The network is challenged with malicious nodes that delay valid packets, the E2E delay increases. In figure 2 and figure 3 an ideal world, legitimate nodes would receive such messages with minimal delay; however, MITM attackers who can delay messages prevent legitimate nodes from receiving messages on time. Furthermore, when the attackers are distributed across the network, this indicates that the E2E delay increases. As a result, in the case of attackers in the network architecture, the network encountered low E2E delays. Furthermore, as opposed to a network with a network of malicious nodes, a network with dispersed attackers reaches about 47.94 percent of high E2E delays for 10% of malicious nodes. When half of the malicious nodes are inserted into the network, the delay rises to 73.44 percent.

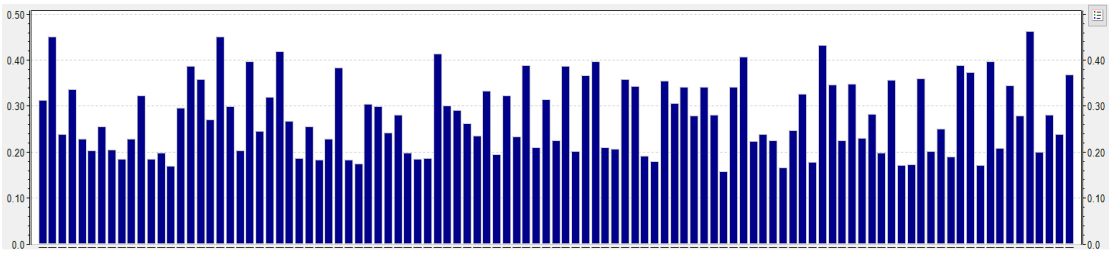

Figure 2. loss Rate time average on 100 node

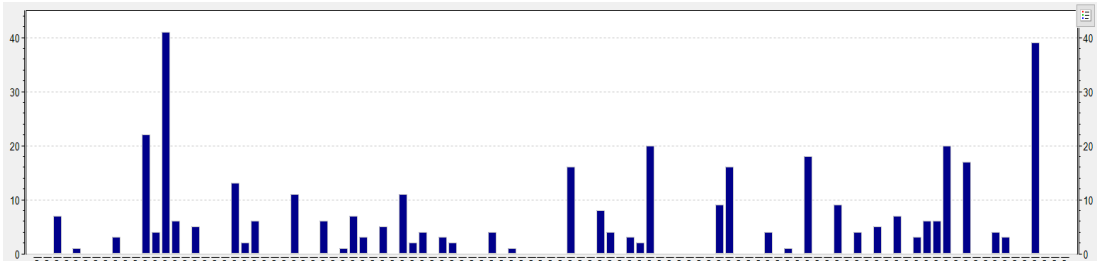

Figure 3. Average count of number to drop packet by queue in 100 node.

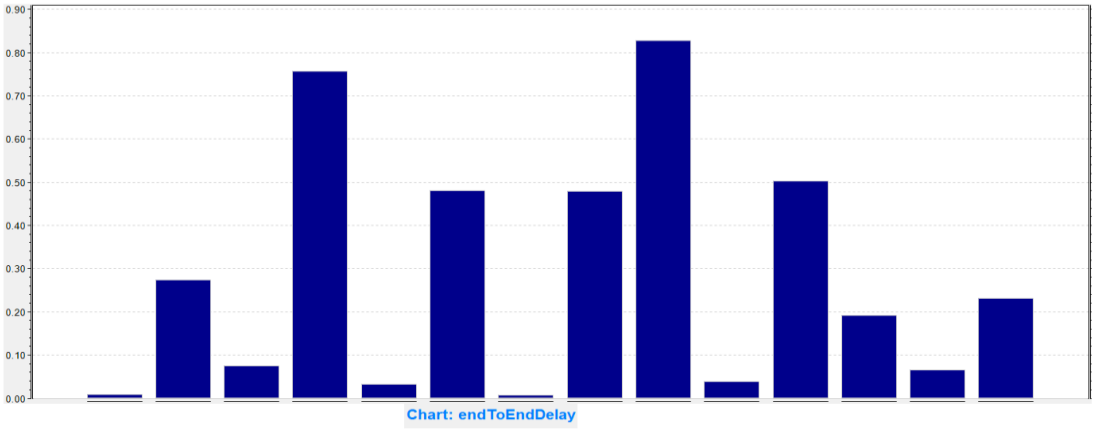

Figure 4. End-to-end delay (E2E) delays packets.

6.1.2. Message Drop Attacks

Figure 5 shows the number of messages dropped by malicious nodes, indicating that as the number of malicious nodes in the network grows, so does the number of messages drop. Both dispersed and fleet attacker patterns have a significant effect on the network in terms of the number of messages lost, i.e., both distributed and fleet attackers lose almost identical numbers of messages. Due to the collaborative aspect of attack starting, the network with fleet attackers achieves a somewhat higher packet drop rate than the network with distributed attackers. When the number of such attackers grows, so does the pace at which messages in the network are dropped.

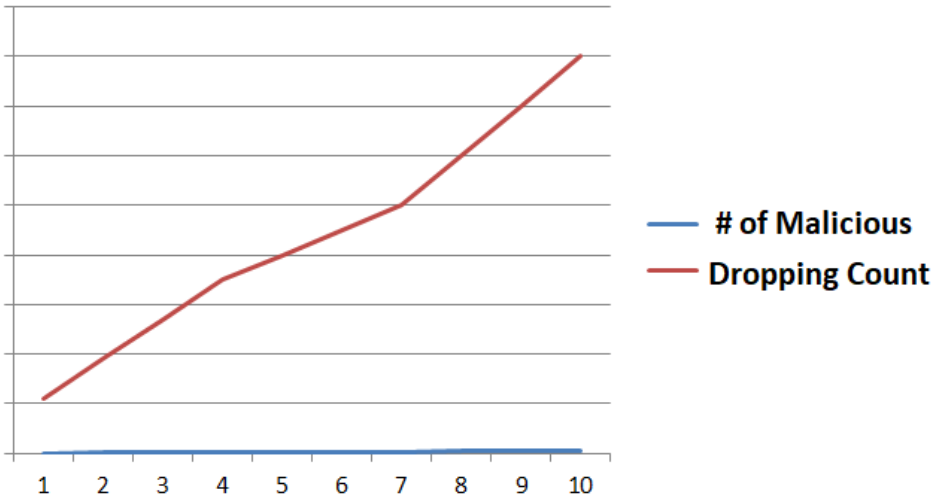

Figure 5. Dropped Messages

6.2. Discussion

Both types of MITM attacks have a high effect on networks, resulting in high E2E delays, poor content transmission ratios, higher packet losses, and the dissemination of a large number of infected packets, as seen in the preceding sections. The network is affected by distributed malicious attackers in terms of E2E delays, as can be observed. The network is influenced by the fleet MITM attackers in terms of stolen messages and PLR. As a result, when designing a network security approach, these MITM characteristics should be considered before integrating into the actual network.

7. CONCLUSION

This paper examined MITM attacks in wireless networks in depth. We tested three types of MITM attacks in a wireless network to see how they affected the network. According to the findings, these attacks have a significant impact on the network in terms of traffic distribution, end-to-end latency, infected packets, and packet losses. Furthermore, as opposed to dispersed attackers, the attacker model with fleet configuration has low network efficiency in terms of sacrificing message quality. The key cause for this low performance is that fleet attackers put a large number of network infrastructure and contact channels at risk, causing network congestion, while distributed attackers only have a minor effect on resources.

We will continue this study in the future by analyzing the effects of MITM attack models in different scenarios of wireless network styles dependent on node mobility.

REFERENCES

[1] Burchfiel, J., Tomlinson, R., & Beeler, M. (1975, May). Functions and structure of a packet radio station. In Proceedings of the May 19-22, 1975, national computer conference and exposition (pp. 245-251).

[2] Toor, Y., Muhlethaler, P., Laouiti, A., & De La Fortelle, A. (2008). Vehicle ad hoc networks: Applications and related technical issues. IEEE communications surveys & tutorials, 10(3), 74-88.

[3] Bauwens, J., Jooris, B., Giannoulis, S., Jabandžić, I., Moerman, I., & De Poorter, E. (2019). Portability, compatibility and reuse of MAC protocols across different IoT radio platforms. Ad Hoc Networks, 86, 144-153.
[4] Chaqfeh, M.; Lakas, A. A Novel Approach for Scalable Multi-hop Data Dissemination in Vehicular Ad Hoc Networks. Ad Hoc Netw. 2016, 37, 228–239
[5] Shi, Y., Ross, A., & Biswas, S. (2018). Source identification of encrypted video traffic in the presence of heterogeneous network traffic. Computer Communications, 129, 101-110.
[6] Williams, R., Samtani, S., Patton, M., & Chen, H. (2018, November). Incremental hacker forum exploit collection and classification for proactive cyber threat intelligence: An exploratory study. In 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 94-99). IEEE.
[7] Wang, J., Juarez, N., Kohm, E., Liu, Y., Yuan, J., & Song, H. (2019, April). Integration of SDR and UAS for malicious Wi-Fi hotspots detection. In 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS) (pp. 1-8). IEEE.
[8] Phung, C. V., Dizdarevic, J., Carpio, F., & Jukan, A. (2019, May). Enhancing rest http with random linear network coding in dynamic edge computing environments. In 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 435-440). IEEE.
[9] AMIR, A. Z. B. (2018). A study on Rogue Wireless Devices with Detection of Mousejack Attacks and Vulnerabilities.
[10] Vanhoef, M., Bhandaru, N., Derham, T., Ouzieli, I., & Piessens, F. (2018, June). Operating channel validation: preventing Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks. In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (pp. 34-39).
[11] Chittamuru, S. V. R., Thakkar, I. G., Pasricha, S., Vatsavai, S. S., & Bhat, V. (2020). Exploiting Process Variations to Secure Photonic NoC Architectures from Snooping Attacks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.
[12] Rupprecht, D., Kohls, K., Holz, T., & Pöpper, C. (2019, May). Breaking LTE on layer two. In 2019 IEEE Symposium on Security and Privacy (SP) (pp. 1121-1136). IEEE.
[13] Ullas, S. U., & Sandeep, J. (2019). Reliable Monitoring Security System to Prevent MAC Spoofing in Ubiquitous Wireless Network. In Advances in Big Data and Cloud Computing (pp. 141-153). Springer, Singapore.
[14] Maithili, K., Vinothkumar, V., & Latha, P. (2018). Analyzing the security mechanisms to prevent unauthorized access in cloud and network security. Journal of Computational and Theoretical Nanoscience, 15(6-7), 2059-2063.
[15] Tochner, S., Zohar, A., & Schmid, S. (2020, October). Route Hijacking and DoS in Off-Chain Networks. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (pp. 228-240).
[16] Alharthi, D. N., Hammad, M. M., & Regan, A. C. (2020, March). A taxonomy of social engineering defense mechanisms. In Future of Information and Communication Conference (pp. 27-41). Springer, Cham.
[17] Metz, L. A. E. P. (2020). An evaluation of unity ML-Agents toolkit for learning boss strategies (Doctoral dissertation).
[18] Shringarputale, S., McDaniel, P., Butler, K., & La Porta, T. (2020, November). Co-residency Attacks on Containers are Real. In Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop (pp. 53-66).
[19] Xia, W., Cong, W., Wei, Y., & Li, C. (2020). Critical angle of attack and the corresponding impact cavity for non-circuitous trajectory of water entry of circular cylinder. Applied Ocean Research, 103, 102322.
[20] Huang, Y., Kuo, H. K., Thomas, S., Kons, Z., Audhkhasi, K., Kingsbury, B., ... & Picheny, M. (2020, May). Leveraging unpaired text data for training end-to-end speech-to-intent systems. In ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 7984-7988). IEEE.
[21] Verma, S., Hamieh, A., Huh, J. H., Holm, H., Rajagopalan, S. R., Korczynski, M., & Fefferman, N. (2016, August). Stopping amplified dns ddos attacks through distributed query rate sharing. In 2016 11th International Conference on Availability, Reliability and Security (ARES) (pp. 69-78). IEEE.

[22] A. Guruswamy, R. S. Blum, S. Kishore and M. Bordogna, "On the Optimum Design of L-Estimators for Phase Offset Estimation in IEEE 1588," IEEE Transactions on Communications, Vol. 63 , No. 9, pp. 5101 – 5115, Dec. 2015.

[23] Karthik, A. K., & Blum, R. S. (2016). Estimation theory based robust phase offset estimation in the presence of delay attacks. arXiv preprint arXiv:1611.05117.

[24] Tsigkari, D., & Spyropoulos, T. (2020). An approximation algorithm for joint caching and recommendations in cache networks. arXiv preprint arXiv:2006.08421.

[25] Stricot-Tarboton, S.; Chaisiri, S.; Ko, R.K.L. 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. [CrossRef]

[26] Chen, Z.; Guo, S.; Duan, R.; Wang, S. Security Analysis on Mutual Authentication against Man-in-the-Middle Attack. In Proceedings of the First International Conference on Information Science and Engineering, Nanjing, China, 26–28 December 2009; pp. 1855–1858. [CrossRef]

[27] Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man In The Middle Attacks. IEEE Commun. Surv. Tutor. 2016, 18, 2027–2051. [CrossRef]

[28] Glass, S.M.; Muthukkumarasamy, V.; Portmann, M. Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks. In Proceedings of the International Conference on Advanced Information Networking and Applications, Bradford, UK, 26–29 May 2009; pp. 530–538.

[29] Kaplanis, C. Detection and Prevention of Man in the Middle Attacks in Wi-Fi Technology. Master's Thesis, Aalborg University, Aalborg, Denmark, 2015.