AN APPROACH TO DETECT REAL-TIME MAC LAYER DOS ATTACKS IN IEEE 802.11 WIRELESS NETWORKS

Abstract

This paper suggests a method to detect real-time attacks on MAC layer in IEEE 802.11 networks. The malicious nodes manipulate the MAC protocol parameter such as DCF Interframe Space (DIFS), Short Interframe Space (SIFS) or floods the network with huge volume of packets capturing the entire network bandwidth. The detection method requires collecting throughput, delay and change point detection algorithm is used. All these attacks are simulated in GNS-3 network simulator.

Keywords: IEEE 802.11 Wireless Networks, Denial of Service Attacks, MAC Layer Attacks, Change Point Detection

Authors

SM Saravanakumar
Assistant Professor
Department of Computer Science
(Data Analytics)
PSG College of Arts & Science
Coimbatore, Tamil Nadu, India.
smskpsgcas@gmail.com

P Srii Rohit
BSc Computer Science with Data Analytics
PSG College of Arts & Science
Coimbatore, Tamil Nadu, India.

Dr. T.Revathi
Associate Professor
Department of Computer Science
PSG College of Arts & Science
Coimbatore, Tamil Nadu, India.

I. INTRODUCTION

IEEE 802.11 is a set of standards that govern wireless local area network (WLAN) communication. The IEEE 802.11 standard includes two main components: the physical layer (PHY) and the media access control (MAC) layer. The MAC protocol isresponsible for regulating access to the wireless medium and ensuring that multiple devices can share the same frequency band without causing interference. One of the mostsignificant vulnerabilities in IEEE 802.11 is the use of the Wired Equivalent Privacy (WEP) protocol for encryption. WEP was theoriginal encryption protocol used in IEEE 802.11 networks, but it has been shown to bevulnerable to attacks that can easilycompromise the security of the network. In particular, WEP uses a small 24-bitInitialization Vector (IV) that is sent in plaintext along with the encrypted data, making iteasy for attackers to guess the IV and decryptthe data.

Vulnerability in IEEE 802.11 networks is the lack of authentication mechanisms. In open networks, anyone can connect to the network without anyauthentication, which can lead to unauthorized access and potentiallymalicious activities on the network. Even in networks that use authentication mechanismssuch as Wi-Fi Protected Access (WPA) or WPA2, there have been vulnerabilities discovered that can be exploited by attackers to bypass authentication and gain access to the network. IEEE 802.11 networks can be vulnerable to attacks that exploit weaknesses in the implementation of the protocol by the device manufacturers or software developers.

For example, attackers can exploit buffer using the IEEE 802.11 standard. In overflow vulnerabilities, format string vulnerabilities, or other programming errors to execute malicious code on the device or gain unauthorized access to the network.

A SYN flood attack is a type of cyber attack that can be launched against IEEE 802.11 networks, which are the most commonly usedwireless networks in the world. In this type ofattack, the attacker sends a large number of SYN packets to the target network, with the aim of overwhelming the network's resourcesand causing it to crash. The initiation of a data transmission between nodes is signalled by a SYN packet. To acknowledge the request and start the session, a device sends a SYN-ACKpacket in response to receiving a SYN packet. When conducting a SYN flood attack, the attacker floods the target network with SYN packets but never replies to the SYN-ACK packets that are received in return. This prevents the target network from respondingto valid requests from other devices because it prompts it to exhaust all of its resources trying to create the communication session.
In a CSM attack, the attacker delivers falsified signals that interfere with the CSMA/CA protocol, forcing the wireless nodes to excessively delay or postpone their transmissions. This reduces network performance or completely disrupts the network. The attacker might potentially monopolise network resources or obstruct certain communications using this technique.

The Shortest DIFS (Distributed Inter-Frame Space) attack is a type of denial-of-service (DoS) attack that targets wireless networks attack, an attacker exploits a vulnerability in the DIFS mechanism of the network, which is used to manage the timing of wirelesstransmissions. The attack works by sending aseries of specially crafted frames that triggercollisions between legitimate frames, causingthe network to become congested and effectively shutting it down. By using a veryshort DIFS interval, the attacker can ensure that their frames are always transmitted before any legitimate frames, effectively blocking all legitimate traffic. This attack canbe particularly effective in networks with a high density of wireless devices, as the congestion caused by the attack can quickly spread throughout the network.

Here, We Focus on Two Types of Attacks**,**

- SYN flood Attack
- Shorter DIFS Attack.

We collect the delay and throughput and apply change point detection method to detect abrupt changes caused by these DoS Attacks

II. RELATED WORK

In [1], the paper proposes a machine learning-based approach for the detection of de-authentication Denial of Service (DoS) attacks in Wi-Fi networks. De-authenticationattacks involve sending fake de- authentication frames to a wireless client, which leads to disconnection of the client from the network.In [2], the author evaluatedthe performance of the proposed mechanismusing a real-world testbed consisting of several Wi-Fi access points and clients. The results showed that the proposed mechanismwas able to accurately detect MAC layer DoS attacks in real-time, while maintaining a low false positive rate. In[3],the paper provides acomprehensive review of various detection mechanisms for SYN flooding attacks. SYN flooding attacks are a type of Denial of Service (DoS) attack that exploit the vulnerability of the Transmission Control Protocol (TCP) to overload a target server with a flood of connection requests.In [4], theauthors evaluated the performance of their proposed mechanism using a simulation model. The results showed that the proposedmechanism was able to effectively detect andprevent RTS attacks in wireless LANs.In [5],the paper presents a simulation-basedanalysis of various Request to Send/Clear to Send (RTS/CTS) Denial of Service (DoS) attack variants in IEEE 802.11 wireless networks.In [6], the author identify various types of MAC layer misbehavior that canoccur in wireless networks, including selfish behavior, where nodes do not cooperate with the MAC protocol and transmit data whenever they want, and malicious behavior,where nodes intentionally disrupt thenetwork by sending false control packets or generating interference.In[7], the paper proposes a novel approach to detect MAC layer misbehavior in wireless networks by analyzing the time series data of packet transmission. In [8], the paper addresses the problem of MAC layer misbehavior attacks in mobile ad-hoc networks (MANETs) and investigates their impact on the network performance. In such attacks, a node may deliberately violate the MAC protocol to disrupt the network operations or gain anadvantage over other nodes.In[9], The paper addresses the problem of MAC layer misbehavior in ad hoc networks and proposes a distributed approach to detect and prevent such misbehavior. The authors focus on misbehavior attacks that violate the carrier sense multiple access with collision avoidance (CSMA/CA) protocol, such as the hidden terminal problem and the exposed terminal problem.In[10], The paper focuses on the analysis of denial-of-service (DoS) attacks in reservation-based MAC protocols, such as the IEEE 802.11 and the IEEE 802.16 standards. The authors identify thevulnerabilities in these protocols that can be exploited by attackers to launch DoS attacks,and propose a framework for analyzing the impact of such attacks on the performance ofthe protocols. In [11], The paper addresses the problem of selfish exploitation of carrier sensing in 802.11 networks, which occurs when a node transmits data without first sensing the wireless medium for ongoing transmissions. Such behavior can lead to collisions and degradation of network performance, especially in high-traffic scenarios. In [12], The authors propose a novel detection and defense mechanism that utilizes a game-theoretic approach to identify selfish nodes and encourage cooperation among nodes. The proposed mechanism uses a reputation system to evaluate nodes' behavior and determine whether they are selfish or cooperative.

III. REAL TIME DETECTION

1. **System Model:** A network intrusion by an attacker can cause abnormal delay and throughput measurements. The change in distribution of delay and throughput is different from network congestion because only one node triggers it in the case of an attack, whereas itis caused by all nodes in the case of congestion. To study this phenomenon, you suggest collecting cumulative end-to-end delay measurements between sender and receiver. It is important to use cumulative measurements to avoid false alarms, as the traffic in 802.11 networks can be unpredictable due to contention. By using these cumulative measurements, an algorithm can differentiate between an attack and network congestion thus preventing false alarms. Change point detection problems are any rapid changes in the time series brought on bymisbehaving nodes. A time series is acollection of data points (x1, x2,..., xt...) thatdescribe a stochastic process. A presumptionwill be made that the time series follows one distribution prior to the change point and a different distribution thereafter. Let's have a look at two density functions. where is the pre-change density function and the post-change density function. The change point will be at the intersection of the pre-change density function *f* (.) and the post-change density function *g* (.).The alternative hypothesis is stated as

$$H_\mu: \quad \{x1, x2, \ldots, x\mu\} \sim f$$

$$\{x\mu+1, x\mu+2, \ldots, xn\} \sim g$$

While the null hypothesis is formulated as:

$$H0: \quad \{x1, x2, \ldots, xn\} \sim f$$

If no change has occurred, then H0 istrue; if a change has occurred, then Hμ is true.

2. **Detection Algorithm*:*** This algorithm compares detection statistics with a detection threshold that is decided based on real-time data , and not thepreset values.

   In the context of this algorithm, 'n' refers to the total number of data points in the time series dataset. It is used in the computation ofthe sample variance, σ^2, and also in the bounds for the loop that iterates over the windows of data points. Specifically, the algorithm moves from t=0 to t=n-2m, where m is the window size, so that it can consider all possible windows of size m in the time series. ‘x' refers to the values of the timeseries dataset. The algorithm computes the sum of the x-values in each window of size m, as well as the sample variance of the x- values in the dataset. Taking ‘m’ consecutive data points from the time series—call it window 1, and the next ‘m’ data points— call it window 2. Then we compute the sum of the x’s in the two windows.

$$Y_1(t) = \overset{t+m}{\underset{i=t+1}{}} Xi \text{ And } Y_2(t) = \overset{t+2m}{\underset{i=t+m+1}{}} Xi$$

$$D(t) = | Y1(t) - Y2(t) |$$

Firstly, the equation for the cumulative distribution function (CDF) of a standard normal distribution, $\Phi(z)$, is defined as:

$$\Phi(z) = P(a \leq z)$$

where a is a standard normal variable with mean 0 and variance 1.

This algorithm works by computing a detection threshold (DT_h) using the following equation:

$$1 - \Phi(z) = \varepsilon$$

where $\Phi(z)$ is the cumulative distribution function (CDF) for a standard normal distribution and ε is the desired false alarm rate. Once the value of z has been determined, the detection threshold is calculated as:

$$DT\_h = z / \mathrm{sqrt}(2m\sigma)$$

where σ is the square root of the sample variance and m is the window size.

Then, as the algorithm moves through the time series dataset, it computes the sum of the x-values in two consecutive windows of size m and checks whether the difference between these two sums exceeds the detection threshold DT_h:

$$D(t) \geq DT\_h$$

If this condition is satisfied, the algorithm reports that a change point has occurred at the midpoint of the two windows:

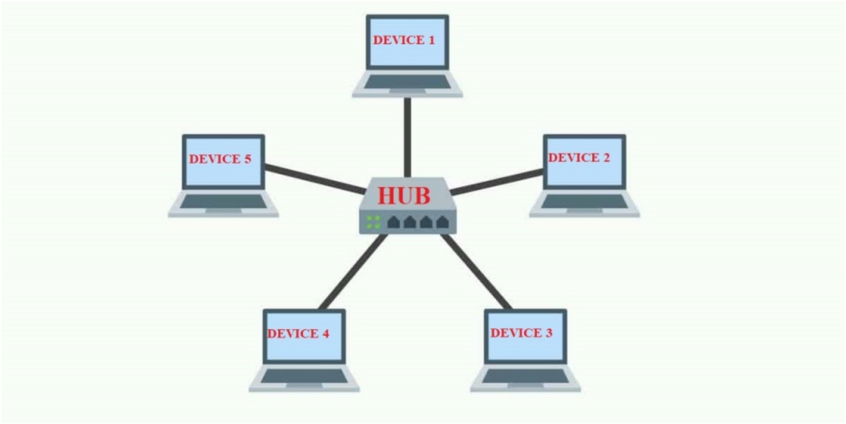
$$\tilde{\mu} = t + m$$

This process is repeated as the algorithm moves through the dataset, checking for change points in subsequent windows.

IV. SIMULATION

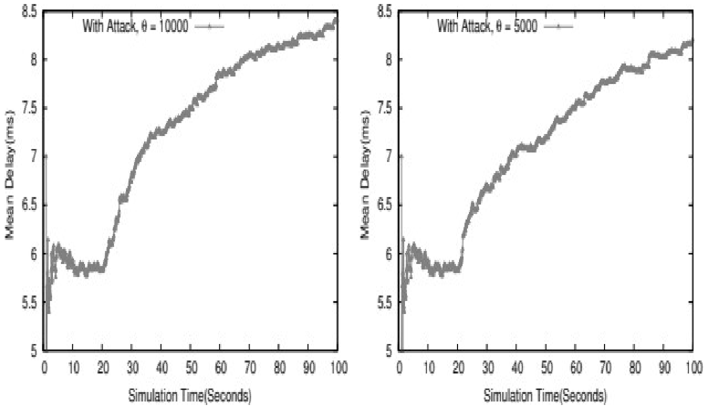
1. **Simulation Setup:** To study the performance of nodes we used GNS-3 Network simulator. We considered 8 nodes in a grid of 100x 100. Out of all nodes, there are one server node, one attacker node and all others are normal nodes. The attacker node uses Kali Linux and the server node uses Windows Server, where all these are virtual machines. In Fig the Node 1 is the server node and Node 3 is the Attacker Node. Here,

we focus on two important attacks : SYN Flood Attack and Shorter DIFS Attack



2. Simulation Result

- **SYN Flood Attack:** In this simulation, we consider SYN flooding attack as explained in Section I. The Attacker node (Node 3) sends continuous SYN (synchronization) packets to the server node (Node 1) initiating a handshake process to establish a connection. However , the attacker doesn't complete the process by sending an ACK packet in response to the server's SYN-ACK packet ,leaving the connection half-opened. This process ties up the server's resources , preventing it from establishing legitimate connections with other nodes thereby keeping the channel busy all time. Here, although the attacker sends too many packets, it still has DCF parameters such as DIFS, SIFS and back-off time same as normal nodes. This varies based on the frequency (θ) of SYN packets sent by attacker. The throughput and channel utilization of the legitimate nodes is inversely proportional to θ. We can measure delay and throughput performance by varying the θ distribution



- **Shorter DIFS Attack:** A succession of deliberately constructed frames is sent in the course of the attack, causing genuine frames to collide and effectively shutting down the network as a result. The attacker may make sure that their frames are always broadcast before any valid frames by employing a very low DIFS interval, thereby blocking all genuine traffic. The attacker node has shorter DIFS. Due to shorter DIFS , the attacker has better chance to send out RTS and reserve the channel thus preventing other flows from transmission. Although ,the throughput shows oscillation , the cumulative mean of throughput is decreasing therefore the throughput is still decreased over time. Applying the change point detection algorithm on the cumulative means time series can easily detect the performance change caused by the selfish node.

V. CONCLUSION

This paper addresses the different types of attacks that occurs in IEEE802.11 networks. We have studied about different attacks and observed that , the shorter DIFS has more effect on wireless network. In this paper , we have used change point detection algorithm to identify any suspicious behaviour in real- time. Future research will focus on extracting the change point detection result and identifying the misbehaving node and developing efficient countermeasures to lessen the harm that the node is causing.

REFERENCES

[1] M. Agarwal, S. Biswas, and S. Nandi, “Detection of de-authentication dos attacks in wi-fi networks: A machine learning approach,” in Systems, Man, and Cybernetics (SMC), 2015 IEEE International Conference on. IEEE, 2015, pp. 246–251.

[2] Dasari, Mallesham. (2017). Real time detection of MAC layer DoS attacks in IEEE 802.11 wireless networks. 939-944. 10.1109/CCNC.2017.7983259.

[3] Manna, Mehdi & Amphawan, Angela. (2012). Review Of Syn-Flooding Attack Detection

[4] Mechanism. International Journal of Distributed and Parallel Systems (IJDPS). 3. 99-117. 10.5121/ijdps.2012.3108.

[5] Jamal, Tauseef & Alam, Muhammad & Umair, Mussadiq. (2017). Detection and prevention against RTS attacks in wireless LANs. 152-156. 10.1109/C- CODE.2017.7918920.
P. M. D. Nagarjun, V. A. Kumar, C. A. Kumar and A. Ravi, "Simulation and analysis of RTS/CTS DoS attack variants in 802.11 networks," 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering, Salem, India, 2013, pp. 258-263, doi: 10.1109/ICPRIME.2013.6496483.

[6] Kyasanur, Pradeep & Vaidya, N.H.. (2003). Detection and Handling of MAC Layer Misbehavior in Wireless Networks. Proceedings of the International Conference on Dependable Systems and Networks. 173- 182. 10.1109/DSN.2003.1209928.

[7] M. X. Cheng, Y. Ling and W. B. Wu, "MAC Layer Misbehavior Detection Using Time Series Analysis," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1-7, doi: 10.1109/ICC.2018.8422724.

[8] Houssaini, Mohammed-Alamine & Aaroud, Abdessadek & Ali, Elhore & Ben-Othman, Jalel. (2015). Performance Analysis under MAC Layer Misbehavior Attack in Mobile Ad-Hoc Networks. Computer Technology and Application. 6. 10.17265/1934-7332/2015.01.006.

[9] Cardenas, Alvaro & Radosavac, Svetlana & Baras, John. (2004). Detection and prevention of MAC layer misbehavior in ad hoc networks. 17-22. 10.1145/1029102.1029107.

[10] Negi, Rohit & Rajeswaran, A.. (2005). DoS analysis of reservation based MAC protocols. IEEE International Conference on Communications (ICC'05). 5. 3632 - 3636 Vol. 5. 10.1109/ICC.2005.1495094.

[11] Pelechrinis, Konstantinos & Yan, Guanhua & Eidenbenz, Stephan & Krishnamurthy, Srikanth. (2009). Detecting Selfish Exploitation of Carrier Sensing in 802.11 Networks. 657-665. 657-665. 10.1109/INFCOM.2009.5061973.

[12] Li, Ming & Salinas, Sergio & Li, Pan & Sun, Jinyuan & Huang, Xiaoxia. (2015). MAC-Layer Selfish Misbehavior in IEEE 802.11 Ad Hoc Networks: Detection and Defense. IEEE Transactions on Mobile Computing.14.1203-1217.10.1109/TMC.2014.2348560.