JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AN APPROACH TO IDENTIFY DENIAL OF SERVICE (DOS) ATTACKS IN REAL-TIME ON THE MAC LAYER OF IEEE 802.11 WIRELESS NETWORKS

[1] SriiRohit P, [2] S.M.Saravana Kumar,
[1] Student, [2] Assistant Professor
[1]Department Of Computer Science with Data Analytics,
[1]PSG College Of Arts and Science, Coimbatore , India

Abstract: The paper introduces an approach to identify attacks in real-time on the Media Access Control (MAC) layer of IEEE 802.11 wireless networks. These attacks involve malicious nodes tampering with MAC protocol parameters such as the Distributed Interframe Space (DIFS) or Short Interframe Space (SIFS) or flood the network thereby consuming the entire bandwidth. The proposed detection method involves the collection of various metrics, including throughput and delay, with a change point detection technique being utilized. These simulated attacks were implemented using the GNS-3 2.2.38 network simulator.

IndexTerms **- Change Point Detection , Denial of Service Attacks, IEEE 802.11 Wireless Networks, MAC Layer Attacks.**

I.INTRODUCTION

The IEEE 802.11 includes two main components: the physical layer (PHY) and the media access control (MAC) layer[1].
The MAC protocol is responsible for regulating access to the wireless medium and ensuring that multiple devices can share the same frequency band without causing interference. One of the most significant vulnerabilities in IEEE 802.11 is the use of the Wired Equivalent Privacy (WEP) protocol for encryption. In particular, WEP uses a small 24-bit Initialization Vector (IV) that is sent in plain text along with the encrypted data, making it easy for attackers to guess the IV and decrypt the data.

Another vulnerability in IEEE 802.11 networks is the lack of authentication mechanisms. In open networks, anyone can connect to the network without any authentication, which can lead to unauthorized access and potentially malicious activities on the network [2]. Even in networks that use authentication mechanisms such as Wi-Fi Protected Access (WPA) or WPA2, there have been vulnerabilities that can be exploited by attackers 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 device manufacturers or software developers. For example, attackers can exploit buffer 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 cyberattack that can be launched against IEEE 802.11 networks,[3] which are the most commonly used wireless networks in the world. The attacker overwhelmed the network's resources to crash it by flooding SYN packets to the target network. The initiation of data transmission between nodes is signaled by a SYN packet. To acknowledge the request and start the session, a device sends a SYN-ACK packet in response to receiving a SYN packet. During a SYN flood attack, the attacker storms the target network with SYN packets but doesn't respond to the SYN-ACK packets that are received in response. This prevents the target network from responding to valid requests from other devices because it prompts it to exhaust all of its resources trying to create the communication session[4].

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 monopolize network resources or obstruct certain communications using this technique.

The Shortest DIFS (Distributed Inter-Frame Space) is a type of DoS attack that targets wireless networks using the IEEE 802.11 standard. In this attack, an attacker exploits a vulnerability in the DIFS mechanism of the network, which is used to manage the timing of wireless transmissions. The attack works by sending a series of specially crafted frames that trigger collisions between legitimate frames, causing the network to become congested and effectively shutting it down. By using a very short DIFS interval, the attacker can ensure that their frames are always transmitted before any legitimate frames, effectively blocking all legitimate traffic[5]. This attack can be 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: 1) SYN flood Attack and 2) Shorter DIFS Attack. We employ a detection technique on the data that we have collected to identify sudden shifts in the data that can be attributed to the 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-authentication attacks involve sending fake de-authentication frames to a wireless client, which leads to the disconnection of the client from the network. In [2], the author evaluated the performance of the proposed mechanism using a real-world testbed consisting of several Wi-Fi access points and clients. The paper gives a thorough evaluation of several detection techniques for SYN flooding attacks in [3]. The authors of [4] used a simulation model to assess the performance of their suggested mechanism. In [5], the paper analysis 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 identifies various types of MAC layer misbehavior that can occur 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 the network 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. [8], the paper examines the issue of MAC layer misbehavior attacks in MANETs. A node may purposefully break the MAC protocol in such attacks in order to disrupt network operations or gain an edge over other nodes. The study tackles the topic of MAC layer attacks in ad hoc networks and provides a distributed solution for detecting and preventing such misbehavior in [9]. In[10], The paper focuses on the analysis of attacks in reservation-based MAC 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 node's behavior and determine whether they are selfish or cooperative.

III. REAL-TIME DETECTION

A. System Model

A network intrusion by an attacker can cause abnormal delay and throughput measurements. The change in the distribution of delay and throughput is different from network congestion because only one node triggers it in the case of an attack, whereas it is 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[6]. 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 by misbehaving nodes. The time series will be assumed to follow one distribution prior to the transition point and a different distribution thereafter.
Let's have a look at two density functions. where is the pre-change density function $f(.)$ and the post-change density function $g(.)$.

The alternative hypothesis is stated as

H_μ: $\{x_1, x_2, \ldots, x_\mu\} \sim f$

$\{x_{\mu+1}, x_{\mu+2}, \ldots, x_n\} \sim g$

the null hypothesis is :

H_0: $\{x_1, x_2, \ldots, x_n\} \sim f$
With no change occurring, then H_0 is true; else H_μ is true

B. Detection Algorithm

The algorithm evaluates detection statistics and contrasts them with a threshold for detection that is established based on current, real-time data. [7].
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 of the sample variance, σ^2, and also in the bounds for the loop that iterates over the windows of data points. The method specifically proceeds from t=0 to t=n-2m, where m is the window size, in order to evaluate all potential windows of size m in the time series. 'x' denotes the time series dataset's values. 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. The process involves selecting a set of 'm' sequential data points from the time series, labelled as 'window 1,' followed by the next set of 'm' data points, named 'window 2.' We then determine the summation of the x-values within both windows.

$Y_1(t) = \sum_{i=t+1}^{t+m} X_i$ and $Y_2(t) = \sum_{i=t+m+1}^{t+2m} X_i$

$D(t) = | Y_1(t) - Y_2(t) |$ Firstly, Φ(z), is defined as:

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

where a is a standard normal variable with mean 0 and variance 1.
To calculate a detection threshold, DT_h, based on a desired false alarm rate, ε:

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

The function Φ(z) represents the probability that a random variable, following a standard normal distribution.

To calculate the value of z, we first need to compute the sample mean and variance of the dataset:

$\bar{x} = (1/n) * \Sigma_i X_i$

for I ranging from 1 to n

$\sigma^2 = (1/n) * \Sigma_i (X_i - \bar{x})^2$

Then, we can use these values along with the window size, m, to calculate z:

$$z = \Phi^{(-1)}(1-\varepsilon) * \sqrt{(2m \div n)} * \sqrt{1 + m \div 2n} * (\sqrt{\sigma^2 \div m}$$

Finally, we can calculate the detection threshold, DT_h, as:

$DT\_h = \bar{x} \pm z * (\sigma / sqrt(n))$
Now, as we move through the time series dataset, we can compare the mean value of each consecutive window of size m to the detection threshold, DT_h. If the absolute difference between the two means is greater than DT_h, we can report a change point at the midpoint of the two windows.

IV. SIMULATION

A. Simulation Setup

To study the performance of nodes GNS-3 Network simulator is used. 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[8]. The attacker node uses Kali Linux and the server node uses Windows Server , where all these are virtual machines. In Fig.1 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 .

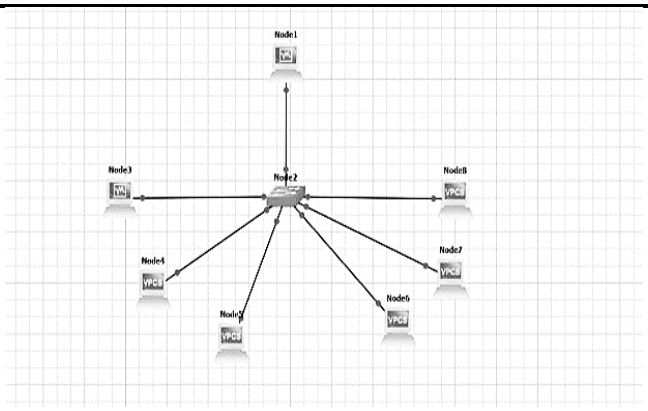

Fig.1: Simulation Setup in GNS3

B. Simulation Result

SYN Flood Attack: In this simulation, we consider a SYN flooding attack. 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[9]. This process ties up the server's resources, preventing it from establishing legitimate connections with other nodes thereby keeping the channel busy all the time. In a network attack scenario, the attacker sends an excessive number of packets, but the network's rules for packet timing and backoff time remain the same. A parameter θ can be introduced to hold the value of frequency at which the attacker sends these packets affecting the overall performance of the network. Legitimate nodes' throughput and channel utilization decrease as θ increases, and we can analyze the network's delay and throughput performance by adjusting θ. The decision to incorporate θ into the algorithm depends on the context. If θ is a significant factor in the network attack scenario, it is worthwhile to adapt the algorithm to consider θ. However, if the main objective is solely to detect changes in the time series data without direct consideration of θ, we can focus on the core change point detection algorithm as described earlier.

Depending on the specific network attack scenario and its characteristics, you may need to adapt the algorithm to consider the attacker's packet frequency (θ) as a part of the analysis.

Shorter DIFS Attack: A succession of deliberately constructed frames are sent in the course of the attack, causing genuine frames to collide and effectively shutting down the network as a result [11]. 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.

If the Distributed Inter-Frame Space (DIFS) is shortened, an attacker can seize control of the channel by submitting a Request-to-Send (RTS), effectively blocking other data flows from transmitting. This leads to fluctuating throughput, with the average throughput decreasing over time. To determine the impact of the selfish node on performance, a time series of average throughput can be analyzed using a change point detection technique. [12]. Incorporating θ into the analysis of a Shorter DIFS attack allows you to explore the connection between attack behavior and its impact on network performance. Just as with other attacks, understanding this relationship can help in developing strategies to detect, prevent, and mitigate the effects of the attack on the network.

V. CONCLUSION

This paper addresses the different types of attacks that occur in IEEE 802.11 networks. We have studied different attacks and observed that the shorter DIFS has more effect on wireless networks. In this paper, we have used a change point detection algorithm to identify any suspicious behavior in real time. Future research will focus on identifying the misbehaving node and developing efficient countermeasures to lessen the harm that the node is causing.

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

[4] Jamal, Tauseef & Alam, Muhammad & Umair, Mussadiq. (2017). Detection and prevention against RTS attacks in wireless LANs. 152-156. 10.1109/C-CODE.2017.7918920.

[5] 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.