Wireless Intrusion Detection And Prevention System For IEEE 802.11 Based Wireless Sensor Network

C Siva BalajiYadav and Dr R.Sheshadri
Department of Computer Science and EngineeringSri Venkateswara University, Tirupati.
Corresponding Author:C Siva BalajiYadav

Abstract: IEEE 802.11 is a major key technology used in most of the sensor network. Increasing in sensor devices and rise of Internet of Things (IoT) technology allows excessive amount of device communication through Wi-Fi network. Due to open air communication as medium the Wi-Fi frames are prone to attacks such as DDoS, MiTM, Rogue Access Point etc. Most of the DDoS attacks against wireless network is due to deauthentication frames created by the attacker against the legitimate client and AP. This Deauthentication attacks are the major problem of the 802.11 standard. Hence to mitigate the problem, a novel Wireless Intrusion Detection and Prevention System (WIDPS) is designed and developed. The proposed WIDPS is lightweight when compared to state of the art techniques and detects the attack with high accuracy & low false positive rate. The proposed IDPS uses minimalistic technique which can be easily adopted and deployed on any open and encrypted networks.

Keywords: Wireless Intrusion Detection and Prevention System, DDoS, MiTM, 802.11 frames, Wi-Fi, IoT.

I. Introduction
IEEE 802.11 based Sensor network is more successful in recent days when the technology IoT arises due to its low cost operational hardware and its deployment. Due to its popularity among the sensor technologies, 802.11 networks are mostly targeted by large number of attacks. In general, IEEE 802.11 framing consists of three major frames namely Data frame, Control frame and management frame. Out of three frames, data frame is secured by means of security key using cryptographical algorithm such as DES, Triple DES, AES and RC4 etc but management and control frame is still open. Various authentication based protocol schemes have been included in recent years which includes WEP, WPA, WPA-PSK,WPA2, WPA2-PSK, EAP, 802.11i, 802.1x etc [1-4].

A typical attack targeted against most of the wireless network is Deauthentication and Disassociation based DDoS. A deauthentication DDoS attack is bombarding all the connected clients from its associated AP and vice versa[10-13]. According to the report from Kaspersky laboratory there is only a weakest point of security standards in IEEE 802.11 based sensor network as of this date [5]. Along with the weakest security protection general users of Wi-Fi technology who access the network are not worrying much about the protection of access points.

According to the 2016 research report given Kaspersky, most of the IoT developers do not care about the security standards and 34% among them really don't use any preventive measure as well as the defensive measures against the IoT devices connectivity based attacks. According to the report 80% of the devices are Wi-Fi connected and general logging of data is on cloud and only 10% care about the general encryption standard for the communication channel which makes the least protection against integrity and authorization based attacks. Figure 1 shows the overview about the deauthentication attack [6][9][10].

In this paper, we focus more on building a novel solution against DDoS attacks on both forms (Deauthentication and Disassociation). Here we propose the IDPS solution for the same using hidden Markovian model.

The paper is organized as follows: Section II presents the security goal, literature review and some related works about the security issues and mitigation techniques in WSNs. Section III gives the brief explanation about the proposed WIDPS. Section IV dealt with the experimental results and The performance analysis of the proposed LWIDPS with the state of the art methods is given in the penultimate section. Finally the paper is concluded in section VI.

Motivation
From the general public information which is available online, some of the case studies are reported here which includes attacks and strategic incidents of Wi-Fi and some notable reports are follows:

- Recent attack over personal hotspots of clients staying over the hotel forcing the clients to pay the ransom to access the hotel's Wi-Fi network [7][8].

**Deauthentication attack - Attack description**

Figure 2 shows the deauthentication attack and its frame exchange procedure. The nature of AP is using open plain text mechanism for management frames. AP is not liable to verify its authenticity and process when the attacker initiates the deauthentication spoofed frames which leads to initiate deauthentication request against all the connected clients resulting the clients to terminate their connection from the associated AP. Once the client is targeted and redirected with high number of deauthentication frames then the client has to initiate reauthentication for its next level association. This makes the client to lose connectivity at any point of range.

**Attack description**

Deauthentication payloads sends a disassociation packets to all connected clients simultaneously resulting to disassociate the connected client reporting with the reason as follows:

- Recovering a hidden ESSID.
Wireless Intrusion Detection And Prevention System For IEEE 802.11 Based Wireless Sensor

- ESSID which is not being broadcast.
- Cloaked BSSID
- Forcing client to reauthenticate
- Capturing WPA/WPA2 handshakes
- Generate ARP requests

In operating system such as windows whenever the wireless client gets disconnected the ARP table will be flushed.

**Proposed System**
The proposed WIDPS is fully functional based on state transition models and Finite State Machine.

**Transition model for states**
State transition model is processed for all the states and given to FSM as input sequences. The state transition is modeled based on assumptions of FSM. In detection phase, if the states with computed KDE values are subjected to any deviation in the HMM model (as shown in Fig.3). The resulting values of state resulting in \( \xi \) parameter denote “DDoS attacks”.

Initial state probability is defined as

\[
\Pi = \{ p_i = P(q_i \text{ at } t = 1) \} \quad \text{1}
\]

Where \( p_i \) is defined as probability

**Coloring Model**
Coloring model is one of abstract mathematical model used to represent various states by modeling state transition when an anonymous or abnormal event occurs. During event processing, when the state transition occurs with resulting \( \delta, \xi \) values, then the Transition probabilities and prediction pattern of the states will change the colors as defined in the hypothesis 1 and hypothesis 2

**Hypothesis 1**: If the resulting values are \( \epsilon, \xi \), then there will be a DDoS attack and the states are changed to different color which results in attack.

**Transition probabilities**

\[
A = \{ a_{ij} = P(q_j \text{ at } t + 1 | q_i \text{ at } t) \}, \quad \text{where } P(a | b) \text{ is the conditional probability of } a \text{ given } b, t = 1, \ldots , T \text{ is time, and } q_i \text{ in } Q. \quad \text{Informally, } A \text{ is the probability that the next state is } q_j \text{ and given that the current state is } q_i. \\
\]

**States**

\[
S = \{ o_k \}, \quad k = 1, \ldots , M.
\]

**Hypothesis 2**: If the resulting value is ‘\( \delta \)’, then there might be an attack/anomaly or may not be an attack. **Prediction pattern**

\[
B = \{ b_{ik} = b_i(o_k) = P(o_k | q_i) \}, \quad \text{where } o_i \text{ in } O. \quad \text{Informally, } B \text{ is the probability that the output is } o_i \text{ given that the current state is } q_i \text{ where the prediction may or may not be an anomaly.} \\
\]

**States**

\[
S = \{ o_k \}, \quad k = 1, \ldots , M.
\]

Validate the color models by correlating the KDE values for both the phases (Learning and detection). When the flow and change of states is down towards the transition, then the deviation is calculated in the HMM model.

**Experimental Setup**
The proposed methodologies were tested in a fully functional experimental setup created for testing the proposed methods. The experimental setup is built with a server which runs windows operating system and 4 client machines running both windows and linux operating system. Here a small network is created and the
experimentation is carried out. Inetsim is used to isolate fake internet services inorder to perform network level attacks and to test the system capabilities.

**Attack Scenario**

Attack scenario (Figure 4-6) is built using various attack payloads which were available in parrot operating system. Parrot Operating System is an open source OS used widely for pentesting. The above mentioned OS is considered and possible attacks were launched using that OS. Client machine 4 is configured in such a way that the above mentioned scenario. Figure 4 – 6 represents the screenshot of various attacks launched to test the performance of the proposed methodologies.

![Figure 4 Screenshot – HTTP flooding](image1)

![Figure 5 Screenshot – UDP flooding](image2)

![Figure 6 Screenshot – DDoS](image3)

**Detection Scenario**

The python agent module running in the server starts to tap all the interface in promiscuous mode in order to ensure all the interfaces were getting tapped by the proposed security systems. Figure 7 – 10 shows the screenshot for detection and prevention results of the proposed WIDPS.
Performance metrics

The performance metrics of the proposed security system is evaluated based on the number of correctly classified predicts and wrongly classified predictions. It is measured based on True positive and false positive rate. The receiver operating characteristics were plotted in order to ensure the performance and rate of accuracy. The ROC curve plotted here ranges from the cutoff point where the mean area varies for various thresholds. In order to measure the performance, thresholds were varied and operated in different functional levels. Figure 11 represents the various ROC curve plotted for different mean area and functional operation rates.
Hence this paper is concluded by proposing a new model for detecting anomalies using Wireless Intrusion Detection and Prevention System. The proposed model has better accuracy and results are promising. The proposed WIDPS is capable to detect any sort of DDoS attack at layer 2 whereas the work concentrates only on layer 2 based DDoS attacks. In future the work can be extended to support for other supplementary security tools like firewalls, anti-virus and online spam filters etc. The model proposed in this work can be deployed in any real time or near real time security solutions in order to detect advanced deauthentication and dissociation based DDoS attacks.

II. Conclusion

Figure 1.1 ROC curve for functional mean area level at 1

Reference

