Context aware Wireless Intrusion Detection System for IEEE 802.11 based Wireless Sensor Networks

Siva Balaji Yadav.C\textsuperscript{1} and R.Seshadri, PhD\textsuperscript{2}

\textsuperscript{1}(Computer Science and Engineering, SV University, Tirupati, India)
\textsuperscript{2}(SVU Computer center, SV University, Tirupati, India)

Abstract

In recent decades the launch of cyber attacks against wireless network is more than the wired networks. This is due to the presence of Layer 2 vulnerabilities in IEEE 802.11 protocol standards. Most of the attacks against the wireless networks are targeting layer 2 vulnerabilities which are more susceptible to DoS, MiTM and replay attacks etc. In this paper, we focus only on the problem of DDoS against IEEE 802.11 and a novel Intrusion Detection System is designed to detect such DDoS attacks. The key idea used in the proposed IDS is to apply Kernel Density Derivative Estimator to study the steady state probabilities (density) of each Station (clients) in the network. Then correlation is applied to the steady state probabilities to find the correlativity of each packet generated from different nodes which in turn gives the results of malformed packets (Deauthentication-DDoS). The primary focus of this work is on the particular scenario where the attacker injects the malformed frames on the target network (Broadcast Spoofed Deauthentication DDoS). A strong analysis is made by experimenting the attacks in the live testbed. The experiments carried out are in house and purely deployed in the live testbed using Parrot Operating system. From the observation it is clearly observed that the proposed IDS is optimal enough with the good results of more than 94% in detection rate.

Keywords: WIDS, IDS, Parrot Operating system, HMM, markov chain, Intrusion
I. INTRODUCTION
Recent advancement in wireless technologies is increasing from last decade. This is due to increase in usage of pervasive devices, mobile gadgets, cloud connected components etc. The popularity of the technology leads the operational free lower cost devices. Due to the popularity and increase in usage leads these wireless technologies prone to attacks. Existing data frame security standards such as WEP, WPA, WPA2 etc can provide authentication based security cryptographic standard [1]. However attacks over data and control plane are still possible in Wi-Fi networks.

The most prominent feature available in IEEE 802.11 network is it can operate in both adhoc and infrastructure mode. This paper focus on the IEEE 802.11 network which operates only in infrastructure mode with dedicated access point. The basic working operation of the AP and Stations in IEEE 802.11 are listed into Authentication, Association, Disassociation, Disconnection, Deauthentication etc. i) Authentication: Authentication is the initial step for each sensor node operating in IEEE 802.11 standards. Initially client has to send connect request to the AP using authentication frame with Initialization vector (IVs) to establish connection with the Access Point for the successful data exchange. ii) Association: Association is the second step carried out by the sensor nodes to associate itself with the AP after authentication. Address allocation, node registration etc are carried out in this phase. iii) Disassociation: Disassociation is the step carried out by the wireless client to initialize the disassociation of the client from the AP. Here the client sends disassociation frames to AP to disassociate itself. Disassociation with all connected clients can happen only if any firmware level upgradation is carried out in AP. iv) Disconnection: Disconnection is the process where the AP sends disassociation request to the client to disconnect from the AP. v) Deauthentication: Deauthentication frame (as shown in Figure 1a - 1c) is initiated from the client if the station needs to leave the network gracefully. Likewise, the AP also sends deauthentication frame if it needs to disconnect from the client at the particular time interval [2-10].

![Figure. 1a Pre-attack - Deauthentication Attack scenario](image-url)
The two major frames known as Deauthentication and Disassociation frames are used for entire handshake of IEEE 802.11 network. These two frames are responsible to perform association and connection of AP with Stations (STA)[11]. But the hard fact is these two frames are not encrypted enough hence the attacker make use of these frames for successful launch of attacks. Attacker can easily masquerades any of these frames by tapping layer 2 protocols (DLL)[12]. These masquerades result in MAC address based spoofing and attacks against AP and clients by initializing n number of deauthentication and disassociation frames. Once these frames are flooded against client and AP, based on the level of payload and packet generation, AP and STA never gets connected. Additionally all the STA needs an reauthentication in order to connect with AP. Figure 2 shows the attack scenario of how an attacker can easily...
launch a powerful DoS over any IEEE 802.11 network by spoofing disassociation and deauthentication frames [13-20].

Figure. 2 Deauthentication and Disassociation attack scenario.

Present day methods used to mitigate the deauthentication and disassociation based DDoS attack includes cryptography and newer standards for protocol by modifying the entire protocol stack. Cryptography techniques include additional hardware and softwares for special tasking and computing the keys [13][16][18]. Specific server should be deployed to monitor the key distribution and management. However protocol stack level upgradation is very expensive tasks and increases administrative over heads. Upgradation of firmware in critical application deployment is a harder task and time consuming [14 -15][17][22][23-25]. From the observation, it is not feasible to adopt the existing mitigation technique. Hence in this paper, novel software based Intrusion Detection System has been proposed. The proposed Wireless IDS does not suffer any critical impact which are listed above. The summary of the contribution is listed below

- A novel Context aware Wireless Intrusion Detection System is proposed and operable in both legacy standards (cryptography implemented networks) and non-legacy network
- The proposed IDS is purely software based and does not require any additional hardware or firmware updation and can be easily deployable in both client and server side.
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 CAWIDS. Section IV dealt with the experimental results and the performance analysis of the proposed CAWIDS with the state of the art methods is given in the penultimate section. Finally the paper is concluded in section V.

II. MOTIVATION

Here, we initially discuss about the basics of Wi-Fi and its operating characteristics and followed by attacks and its attack definitions.

Basic Terminologies

In general, Wi-Fi network consists of many wireless clients such as mobiles, laptops, tablets etc and an Access point which might be a wireless router. All the communication will take place by means of AP where the AP is connected to a backbone network of any ISP. Initial stage is client needs to authenticate itself with AP in order to associate with the AP and to join the network. The procedure is same for all the wireless clients which are seeking to form a network.

Deauthentication Attack

Deauthentication attack is launched over the deauthentication frames due to its plain text in nature. Hence spoofing of these plain-text frames is easier when compared to encrypted data frames. These management frames are responsible for fast processing and to proceed with handshaking mechanism with AP to all connected clients. Due to its open plain text nature, AP is not liable to verify its authenticity and process the deauthentication spoofed frames. This leads to initiate deauthentication request against clients resulting the clients to terminate its connection with 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. As per the existing standards of IEEE 802.11, deauthentication request is just a notification not a request. Figure 1 and Figure 2 clearly shows the actual working mechanism of deauthentication attack launched against a wireless network [5-20].

State of the art methods

Many researchers proposes various methods for mitigating the Deauthentication based
DDoS attack in Wi-Fi network. Some of the state of the art methods have been reviewed and presented here in this section.

**Entropy based WIDS**

Kamalanaban et al proposed a novel Wireless Intrusion Detection System using Entropy based approach. Here the authors concentrate on calculating entropy for all the frames which is going in and around the network. The key advantage of the stated method is better but requires high computation. The author also addresses some basics level channel switching and it detection mechanism where their IDS is capable to detect Deauthentication DDoS attack at any channel in multiple networks. The only challenge possessed by the WIDS stated by the author is overhead of processing and execution time [12].

**Cryptography based methods**

Bellardo proposed a encryption method to encrypt all the frames which is going in and around the network. The method proposed by the author is robust enough but needs special upgradation of firmware and hardware as well in both client and server [25].

**III. PROPOSED IDS**

In this paper, a new context aware IDS has been developed to detect Deauthentication DDoS attacks. The proposed IDS is robust and context aware in nature due to its learning capabilities of real time live feed of network data and cross correlating it with the addressed pattern in order to detect the DDoS and wireless anomalies. Robustness of the behavior model proposed in this paper is initially to learn the network traffic patterns using KDDE function, where Kernel Density function is used to estimate the PDF of a complete randomness. Here in KDDE, Parzen–Rosenblatt window method is used for estimating the density values. The KDDE is a kernel function which works on basis of neural model which is clearly figured in the equation (1). Each input is tested with the possible output and the learned data is computed with KDDE values. Firstly in learning phase all the network parameters are learnt and profiled specifically with KDDE values and approximate KDDE values are computed. Secondly in detection phase the KDDE values of the live feed are compared with learnt KDDE values and correlation is applied in order to detect the intrusions [3].

$$\text{MISE}(h) = E \int (\hat{f}_h(x) - f(x))^2 dx.$$  

-------------------------- 1
fig 3. Architecture of Proposed Context aware WIDS

Here, KDDE values are computed for learning phase using specific network patterns such as IP, port, Link, interface (ETH#, WLAN#), BOOTIF (MAC) and other system parameter such as NET CONSOLE, CPU utilization, Memory usage, Memory utilization, Incoming Packet buffer, Outgoing Packet buffer, Cached Bytes etc. Network packet analyzers are used to analyze the network packets. Packet capturing interface is widely used to capture all the packets and network data collector acts as the serialization interface for all the network inputs.

Learning phase

In this phase, the values have been collected from the network parameters which are related to the network for each connected host. Each host are profiled into system and network parameters and each value are utilized to compute KDDE. A detailed process was illustrated in the algorithm 1 which runs in all hosts for 5 working days with all network and system credentials
Algorithm 1 Learning phase

Begin

Initiate learning and profiling
Profile each host
Collect network credentials
Do feature selection
Compute KDDE

Compute KDDE parameters with appropriate values

End

Detection phase

In this phase as off the learning phase is cloned to compute KDDE values for the hosts of same parameters in several time periods. Then the Comparison process is carried out for the present KDDE values with the learnt KDDE values.

Hypothesis

According to the hypothesis, the correlation values lies between 0 and 1. KDDE value computed is always lies between 0 to 1. If the values are nearest circumstance of 1, then the relationship possessed by the parameters is in strong relationship. If the threshold value falls <0.5, then it is abnormal frame or Deauthentication frame

Correlation phase

Based on the hypothesis defined above the cross correlation values are computed. The detection phase is exhibited by considering, analyzing and comparing all the defined network and system parameters. According to the discussion defined in previous section’s anomalies are the specific event based, so that the proposed methodology computed here yields the promising results by utilizing the network parameters for identification.
Algorithm 2 Detection phase

Use learnt data

Procure the live feed

Do feature selection

Compute KDDE

Use KDDE values of Learnt data and live feed

Check all the frame: include (control, management and data frames)

Apply cross correlation

Compare cross correlation value for each network parameter

If the threshold (correlation) < 0.5 then

Caption: Intrusion detection

Trigger Alarm

End

IV. EXPERIMENTAL RESULTS

The correlation coefficient values of the two collective samples were linearly inclusive with +1 or -1 which in term shows the deviation range and the proposed methodology yields the promising results by detecting intrusions in near real time (Fig 4 - Fig 21). Here the correlation values are compared between kernel density function values along with the trained values. Then the range of threshold is isolated and correlativity is computed by correlating various system and network parameters.

Using this method all the attacks performed during certain time periods were identified/detected and experimentally promising results were achieved. The cross correlation values of attack sequence are clearly defined in the Table 1 for various attributes like CPU utilization, RAM utilization, outgoing packets, incoming packets etc.,.
**Figure 4** Kernel Density Estimation for Incoming bytes (Learning phase)

**Figure 5**: Kernel Density Estimation for Incoming packets (Learning phase)
Figure 6: Kernel Density Estimation for Outgoing bytes (Learning phase)

Figure 7: Kernel Density Estimation for Outgoing packets (Learning phase)
Figure 8 Kernel Density Estimation for RAM Buffered (Learning phase)

Figure 9 Kernel Density Estimation for RAM Used (Learning phase)
Figure.10 Kernel Density Estimation for Incoming bytes (Detection phase)

Figure.11 Kernel Density Estimation for Incoming Packets (Detection phase)
Figure 12 Kernel Density Estimation for Outgoing bytes (Detection phase)

Figure 13 Kernel Density Estimation for Outgoing Packets (Detection phase)
Figure 14 Kernel Density Estimation for RAM buffered (Detection phase)

Figure 15 Kernel Density Estimation for RAM Used (Detection phase)
Figure 16 Kernel Density Estimation for Incoming bytes (Correlation phase)

Figure 17 Kernel Density Estimation for Incoming Packets (Correlation phase)
Figure 18 Kernel Density Estimation for Outgoing Bytes (Correlation phase)

Figure 19 Kernel Density Estimation for Outgoing Packets (Correlation phase)
Figure 20 Kernel Density Estimation for RAM Buffered (Correlation phase)

Figure 21 Kernel Density Estimation for RAM used (Correlation phase)
The proposed model can be deployed in both client and server side to detect any form of wireless attack. Currently it is tested by deploying in both client and server. The real time implementation result is also given. A command line console is given to display the alerts from the proposed model. Figure states the attack detection and alert scenario where the alert consists of Target MAC address, AP with which the client is connected and attacker’s MAC.

V. CONCLUSION

This paper is concluded by proposing a novel Wireless Intrusion Detection System. The proposed Context aware WIDS is evaluated and some of the active time stamps are estimated and tabulated in Table I. In detection the Cross correlation values for network and system parameters are estimated along with the time stamp and deviation range of the values are mentioned in the Figures 4 -15 for network and host parameters. The experimental results demonstrated in the Figure 16 - 21 shows the results of correlation which shows the optimality of the proposed algorithm in detection. In future, the proposed IDS is extended to detect the covert communications in WSN.

Table I: Cross correlation values of attacking sequence

<table>
<thead>
<tr>
<th>S.No</th>
<th>Time</th>
<th>CPU</th>
<th>RAM</th>
<th>Outgoing packets</th>
<th>Incoming packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1:16:59</td>
<td>1179339978</td>
<td>892986</td>
<td>896046</td>
<td>636809</td>
</tr>
<tr>
<td>2</td>
<td>1:17:10</td>
<td>1179339978</td>
<td>896119</td>
<td>896046</td>
<td>636809</td>
</tr>
<tr>
<td>3</td>
<td>1:18:28</td>
<td>1179611728</td>
<td>898952</td>
<td>898952</td>
<td>639716</td>
</tr>
<tr>
<td>4</td>
<td>1:19:26</td>
<td>1179791914</td>
<td>898231</td>
<td>901233</td>
<td>641997</td>
</tr>
<tr>
<td>5</td>
<td>1:20:27</td>
<td>1179972352</td>
<td>900347</td>
<td>903479</td>
<td>644243</td>
</tr>
<tr>
<td>6</td>
<td>1:21:27</td>
<td>1180153141</td>
<td>902466</td>
<td>905726</td>
<td>646491</td>
</tr>
<tr>
<td>7</td>
<td>1:22:27</td>
<td>1180376311</td>
<td>904659</td>
<td>908039</td>
<td>648815</td>
</tr>
<tr>
<td>8</td>
<td>1:23:11</td>
<td>1211149803</td>
<td>926499</td>
<td>937182</td>
<td>664802</td>
</tr>
<tr>
<td>9</td>
<td>1:24:4</td>
<td>1262468314</td>
<td>962392</td>
<td>937182</td>
<td>664802</td>
</tr>
<tr>
<td>10</td>
<td>1:25:26</td>
<td>1380740088</td>
<td>1043522</td>
<td>1022047</td>
<td>709688</td>
</tr>
<tr>
<td>11</td>
<td>1:26:22</td>
<td>1420838212</td>
<td>1071513</td>
<td>1071466</td>
<td>735810</td>
</tr>
</tbody>
</table>

The proposed model can be deployed in both client and server side to detect any form of wireless attack. Currently it is tested by deploying in both client and server. The real time implementation result is also given. A command line console is given to display the alerts from the proposed model. Figure states the attack detection and alert scenario where the alert consists of Target MAC address, AP with which the client is connected and attacker’s MAC.
REFERENCES


[4] Yu-Xin Ding, Min Xiao, Ai-Wu-Liu “Research and implementation on snort-based hybrid intrusion detection system”, in proceedings of the Eighth International Conference on


