IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. IV (Jan.- Feb. 2018), PP 30-36
www.iosrjournals.org

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.*

Date of Submission: 16-02-2018 Date of acceptance: 03-03-2018

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-PSKWPA2, 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 thenotable reports are follows

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

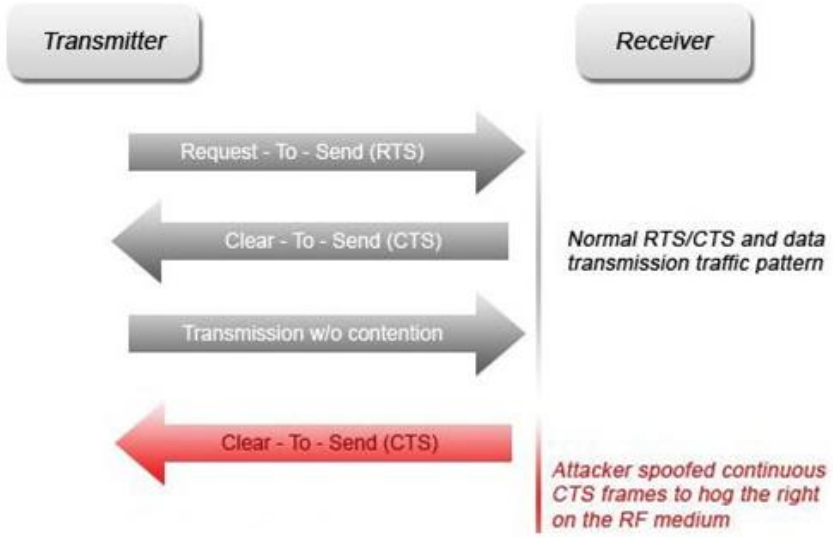

Transmitter
Receiver
Request - To - Send (RTS)
Clear - To - Send (CTS)
Normal RTS/CTS and data transmission traffic pattern
Transmission w/o contention
Clear - To - Send (CTS)
Attacker spoofed continuous CTS frames to hog the right on the RF medium

Figure 1. DDoS based spoofing attack

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.

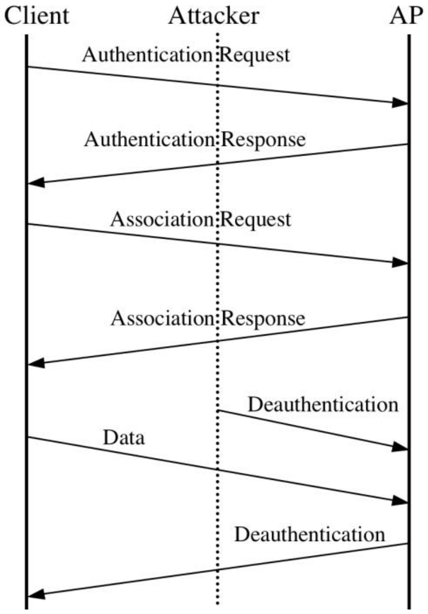


Figure 2. Deauthentication and disassociation procedure.

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.

- 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 toFSM 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 inξparameter denote "DDoS attacks".

Initial state probability is defined as

Initial state probabilities$\Pi = \{p_i = P(q_i \text{ at } t = 1)\}$---------- 1

Where p_i is defined as probability

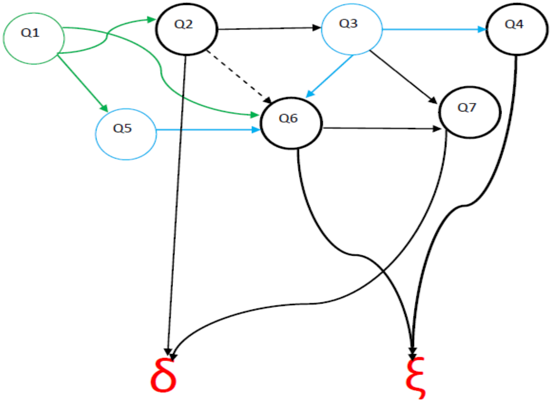


Figure 3. State transition diagram

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 δ, ξ 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'ξ', then there will be a DDoSattack and the states are changed todifferent color which results in attack.

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

States $S = \{o_k\}, k = 1, \ldots, M$.

Hypothesis 2: If the resulting value is 'δ', then there might be an attack/anomaly or may not be an attack.**Prediction pattern** $\boldsymbol{B} = \{b_{ik} = b_i(o_k) = P(o_k \mid q_i)\}$, where $o_k$in $\boldsymbol{O}$. Informally, $\boldsymbol{B}$ is the probability that the output is $o_k$given that the current state is q_i where the prediction may or may not be an anomaly.

States $S = \{o_k\}, k = 1...M.$

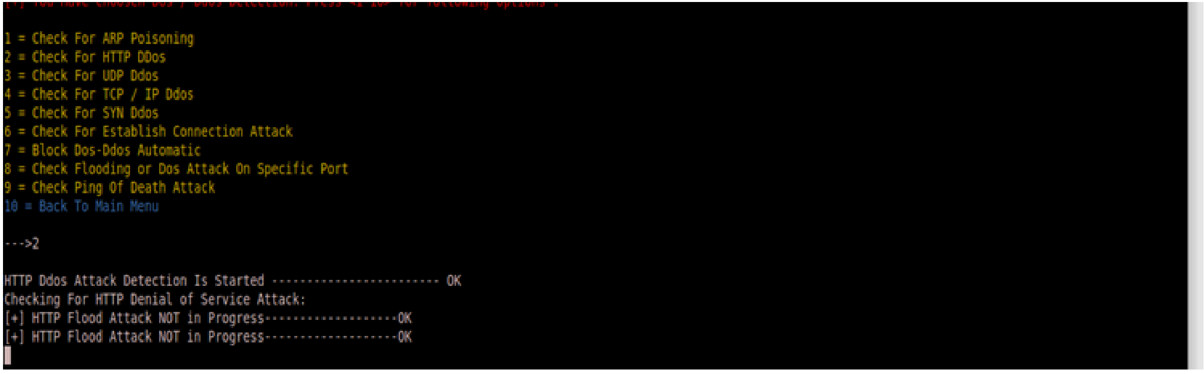
Validate the color models by correlating the KDE values for both the phases (Learning and detection). When the flow and change of states is down towards the transition, then the deviation is calculated in the HMM model.

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.

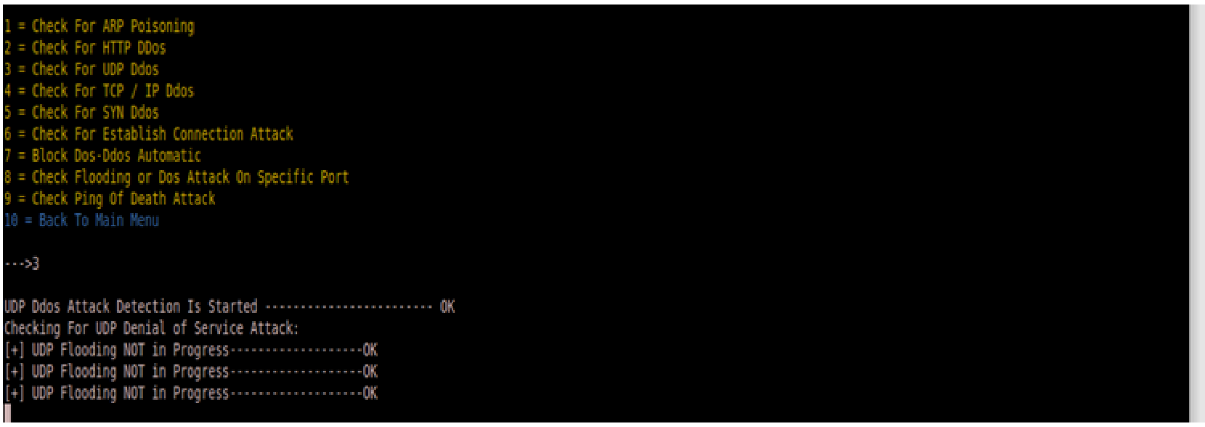
Attack Scenario

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 pentesing. 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.



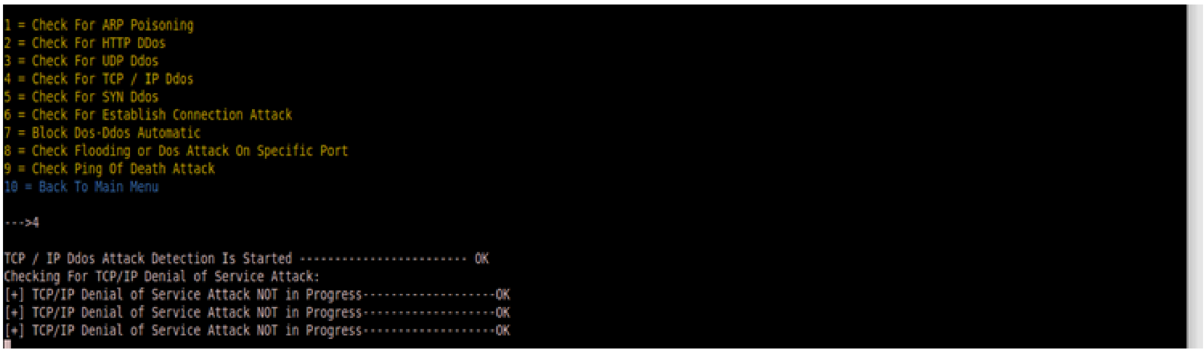
```
1 = Check For ARP Poisoning
2 = Check For HTTP DDos
3 = Check For UDP Ddos
4 = Check For TCP / IP Ddos
5 = Check For SYN Ddos
6 = Check For Establish Connection Attack
7 = Block Dos-Ddos Automatic
8 = Check Flooding or Dos Attack On Specific Port
9 = Check Ping Of Death Attack
10 = Back To Main Menu

--->2

HTTP Ddos Attack Detection Is Started ----------------------- OK
Checking For HTTP Denial of Service Attack:
[+] HTTP Flood Attack NOT in Progress-----------------OK
[+] HTTP Flood Attack NOT in Progress-----------------OK
```

Figure.4 Screenshot – HTTP flooding



```
1 = Check For ARP Poisoning
2 = Check For HTTP DDos
3 = Check For UDP Ddos
4 = Check For TCP / IP Ddos
5 = Check For SYN Ddos
6 = Check For Establish Connection Attack
7 = Block Dos-Ddos Automatic
8 = Check Flooding or Dos Attack On Specific Port
9 = Check Ping Of Death Attack
10 = Back To Main Menu

--->3

UDP Ddos Attack Detection Is Started ----------------------- OK
Checking For UDP Denial of Service Attack:
[+] UDP Flooding NOT in Progress-----------------OK
[+] UDP Flooding NOT in Progress-----------------OK
[+] UDP Flooding NOT in Progress-----------------OK
```

Figure.5 Screenshot – UDP flooding

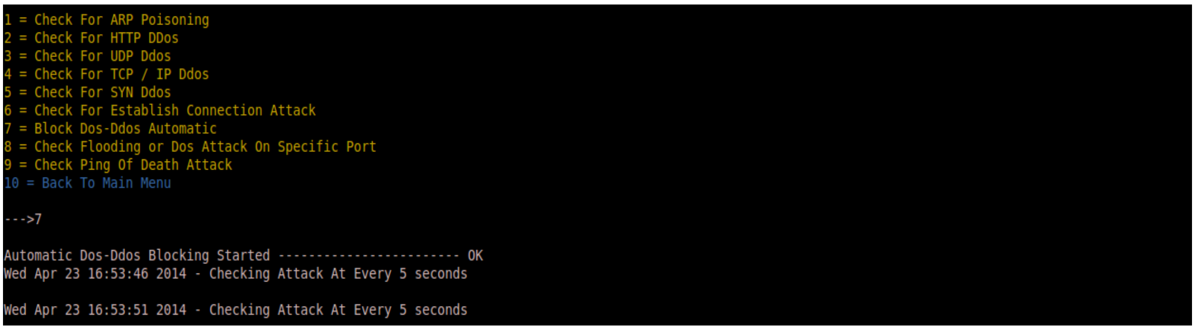


```
1 = Check For ARP Poisoning
2 = Check For HTTP DDos
3 = Check For UDP Ddos
4 = Check For TCP / IP Ddos
5 = Check For SYN Ddos
6 = Check For Establish Connection Attack
7 = Block Dos-Ddos Automatic
8 = Check Flooding or Dos Attack On Specific Port
9 = Check Ping Of Death Attack
10 = Back To Main Menu

--->4

TCP / IP Ddos Attack Detection Is Started ----------------------- OK
Checking For TCP/IP Denial of Service Attack:
[+] TCP/IP Denial of Service Attack NOT in Progress-----------------OK
[+] TCP/IP Denial of Service Attack NOT in Progress-----------------OK
[+] TCP/IP Denial of Service Attack NOT in Progress-----------------OK
```

Figure.6 Screenshot – DDoS

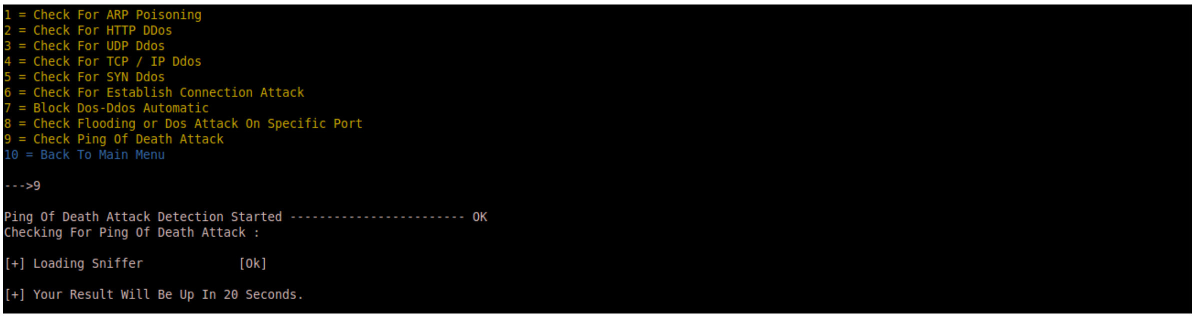
Detection Scenario

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.



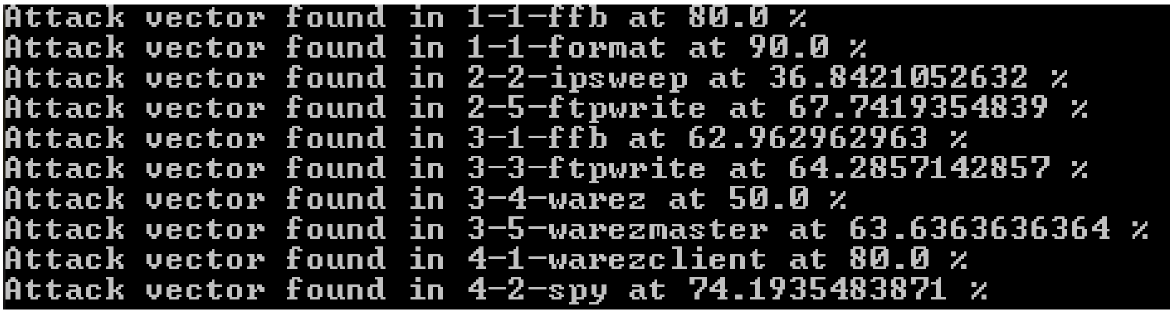
```
1 = Check For ARP Poisoning
2 = Check For HTTP DDos
3 = Check For UDP Ddos
4 = Check For TCP / IP Ddos
5 = Check For SYN Ddos
6 = Check For Establish Connection Attack
7 = Block Dos-Ddos Automatic
8 = Check Flooding or Dos Attack On Specific Port
9 = Check Ping Of Death Attack
10 = Back To Main Menu

--->7

Automatic Dos-Ddos Blocking Started ----------------------- OK
Wed Apr 23 16:53:46 2014 - Checking Attack At Every 5 seconds

Wed Apr 23 16:53:51 2014 - Checking Attack At Every 5 seconds
```

Figure.7 Screenshot – Attack detection console.



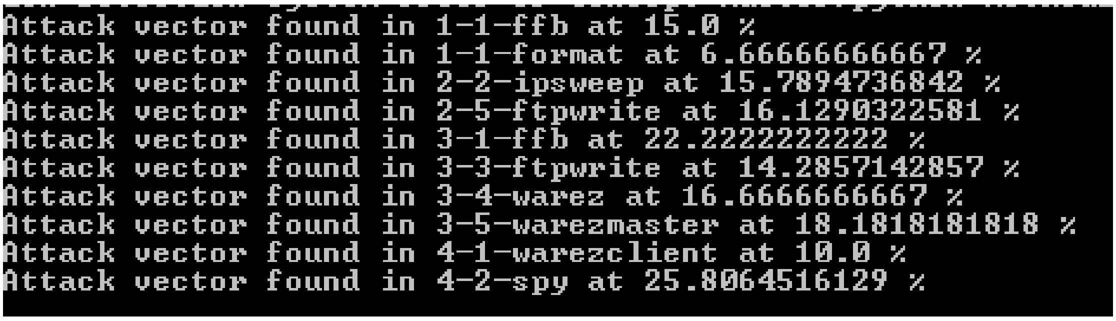
```
1 = Check For ARP Poisoning
2 = Check For HTTP DDos
3 = Check For UDP Ddos
4 = Check For TCP / IP Ddos
5 = Check For SYN Ddos
6 = Check For Establish Connection Attack
7 = Block Dos-Ddos Automatic
8 = Check Flooding or Dos Attack On Specific Port
9 = Check Ping Of Death Attack
10 = Back To Main Menu

--->9

Ping Of Death Attack Detection Started ----------------------- OK
Checking For Ping Of Death Attack :

[+] Loading Sniffer             [Ok]

[+] Your Result Will Be Up In 20 Seconds.
```

Figure.8 Screenshot - Result module



```
Attack vector found in 1-1-ffb at 80.0 %
Attack vector found in 1-1-format at 90.0 %
Attack vector found in 2-2-ipsweep at 36.8421052632 %
Attack vector found in 2-5-ftpwrite at 67.7419354839 %
Attack vector found in 3-1-ffb at 62.962962963 %
Attack vector found in 3-3-ftpwrite at 64.2857142857 %
Attack vector found in 3-4-warez at 50.0 %
Attack vector found in 3-5-warezmaster at 63.6363636364 %
Attack vector found in 4-1-warezclient at 80.0 %
Attack vector found in 4-2-spy at 74.1935483871 %
```

Figure.9 Screenshot - Result for detection and prevention statistics



```
Attack vector found in 1-1-ffb at 15.0 %
Attack vector found in 1-1-format at 6.66666666667 %
Attack vector found in 2-2-ipsweep at 15.7894736842 %
Attack vector found in 2-5-ftpwrite at 16.1290322581 %
Attack vector found in 3-1-ffb at 22.2222222222 %
Attack vector found in 3-3-ftpwrite at 14.2857142857 %
Attack vector found in 3-4-warez at 16.6666666667 %
Attack vector found in 3-5-warezmaster at 18.1818181818 %
Attack vector found in 4-1-warezclient at 10.0 %
Attack vector found in 4-2-spy at 25.8064516129 %
```

Figure.10 Screenshot - Result for detection and prevention statistics

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.

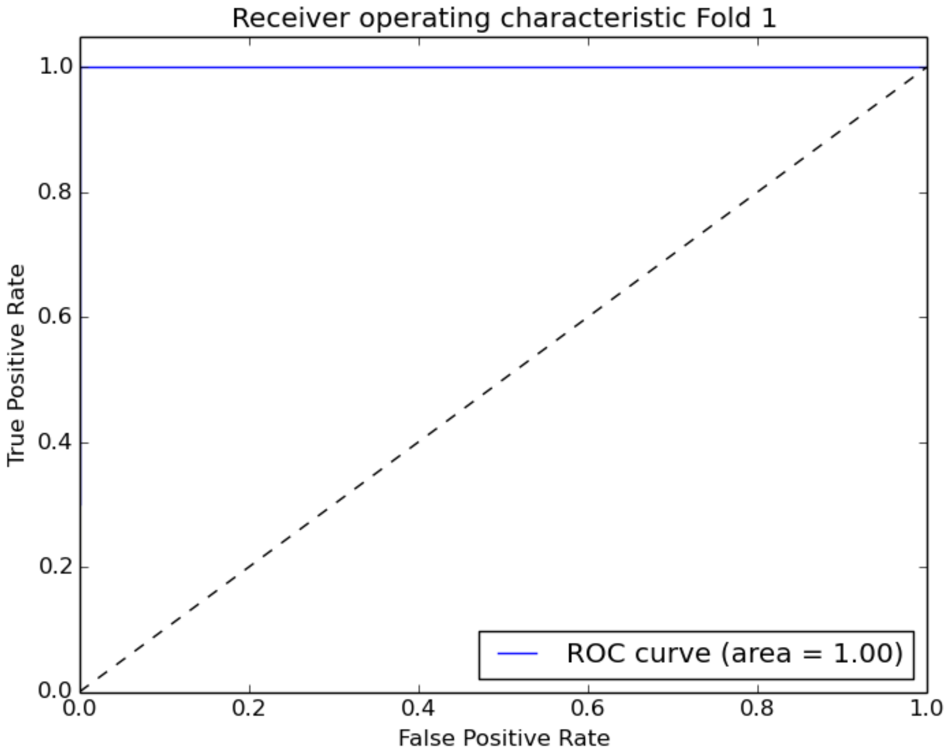


Figure.11 ROC curve for functional mean area level at 1

II. Conclusion

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 disassocation based DDoS attacks.

Reference

[1]. R. Mohan, V. Vaidehi, Ajay Krishna A, Mahalakshmi M and S. S. Chakkaravarthy, "Complex Event Processing based Hybrid Intrusion Detection System," 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, 2015, pp. 1-6.

[2]. Ethala, K., Sheshadri, R., & Chakkaravarthy, S. S. (2014). WIDS Real-Time Intrusion Detection System Using Entrophical Approach. Advances in Intelligent Systems and Computing Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, 73-79. doi:10.1007/978-81-322-2126-5_9

[3]. S.Sibi Chakkaravarthy, V.Vaidehi; "Behavior based anomaly detection model for. detecting wireless covert attacks in Wi-Fi", Security and Privacy Symposium, 2015, IIITD, February 13-14,2015.

[4]. J. Milliken, V. Selis, K. M. Yap and A. Marshall, "Impact of Metric Selection on Wireless DeAuthentication DoS Attack Performance," in IEEE Wireless Communications Letters, vol. 2, no. 5, pp. 571-574, October 2013.

[5]. K. El-Khatib, "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems," in IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 8, pp. 1143-1149, Aug. 2010.

[6]. P. L. Shrestha, M. Hempel, F. Rezaei and H. Sharif, "Leveraging Statistical Feature Points for Generalized Detection of Covert Timing Channels,"2014 IEEE Military Communications Conference, Baltimore, MD, 2014, pp. 7-11.

[7]. R. Singh and T. Parval Sharma, "Detecting and reducing the denial of Service attacks in WLANs," 2011 World Congress on Information and Communication Technologies, Mumbai, 2011, pp. 968-973.

[8]. B. Könings, F. Schaub, F. Kargl and S. Dietzel, "Channel switch and quiet attack: New DoS attacks exploiting the 802.11 standard," 2009 IEEE 34th Conference on Local Computer Networks, Zurich, 2009, pp. 14-21.

[9]. T. D. Nguyen, D. H. M. Nguyen, B. N. Tran, H. Vu and N. Mittal, "A Lightweight Solution for Defending Against Deauthentication/Disassociation Attacks on 802.11 Networks," 2008 Proceedings of 17th International Conference on Computer Communications and Networks, St. Thomas, US Virgin Islands, 2008, pp. 1-6.

[10]. C. Liu and J. Yu, "Rogue Access Point Based DoS Attacks against 802.11 WLANs," 2008 Fourth Advanced International Conference on Telecommunications, Athens, 2008, pp. 271-276.

[11]. Wenzhe Zhou, A. Marshall and Qiang Gu, "A novel classification scheme for 802.11 WLAN active attacking traffic patterns," IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006., Las Vegas, NV, 2006, pp. 623-628.

[12]. K. El-Khatib, "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems," in IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 8, pp. 1143-1149, Aug. 2010.

[13]. J. Bellardo, S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", Proceedings of the 12th Conference on USENIX Security Symposium, vol. 12, pp. 15-28, 2003.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Siva Balaji. "Wireless Intrusion Detection And Prevention System For IEEE 802.11 Based Wireless Sensor Network." IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): 30-36.