A LIGHTWEIGHT WIRELESS INTRUSION DETECTION SYSTEM FOR IEEE 802.11 BASED WIRELESS SENSOR NETWORK

Siva Balaji Yadav C[1]

Research Scholar, SVU College of Engineering, SV University,
Tirupati-India
E-mail: sivabalaji2233@gmail.com

R Seshadri, PhD[2]

Director, SVU Computer center, SV University,
Tirupati-India
E-mail: ravalaseshadri@gmail.com

Abstract

Heterogeneous Wireless Sensor Network with IEEE 802.11 as communication medium possess various risks and threats in the cyber space. Increased level of pervasive devices and open access to the sensor leads the threat to pitfall the performance of the system and network as well. Existing security solutions such as authentication keys, built-in MAC filtering can help the network to prevent against layer 2 attacks. However, the non logical payload based attack such as Distributed Denial of Service (DDoS) is still possible to perform against the existing security solutions. Hence in this paper a novel light weight Intrusion Detection System (LWIDS) is proposed. The key idea of the proposed LWIDS is to use the fuzzy rules based decision tree classifier to train, test and classify the wireless traffic. In contrast to previous research in this area that generally has investigated known wireless attacks, this paper actively considers the outfitted features of the IEEE 802.11 and presents a complete solution to deal with not only known attacks but also unknown attacks.

keywords: DDoS; IEEE 802.11 WSN; IoT; IDS; LWIDS; NFC; Wireless networks; Wireless Security; Fuzzy logic; Fuzzy controller; Fuzzy rules.

1. Introduction

In past few decades the rise of Internet of Things Technology has brought the tremendous growth for wireless sensor network. The sensor technology has a wide range of application which are powerful and flexible enough with affordable cost. Most of these sensor technologies are widely used for short range and long range of wireless communication. In general, the sensor network consists of wireless sensor nodes in larger number and deployed in target area for the target specific application. Most of the lower end sensor nodes uses Bluetooth, zigbee, NFC as communication protocol and high configuration sensor nodes such as nodemcu, Wisense etc uses IEEE 802.11 as communication protocol. Heterogeneous deployment of WSN has both higher end and lower end sensor nodes. Recent advancement of Internet of Things based WSN has self organizing structure to frame a network by itself and complete its deployment task. However the self organizing structure in WSN possesses various host based and network based attacks. WSN deployment in open, un-monitored, hostile environment [1], or operated on an unattended mode, sensor nodes will be exposed to the risk of being captured by an active adversary [2].

Larger deployment of high configuration sensor nodes are exposed and vulnerable to Distributed denial of service (DDoS) which is a most common attack in the WSN. The aim of DDoS is to disrupt the services between the nodes and base station rather than to perform logical service subverting. There are many types of DDoS attacks can be possible to launch over the sensor networks. Such attacks include Jamming, deauthentication, fragmentation, chip chop, flooding fragmented redirectional packets etc. Figure 1 shows the scenario of DDoS attack launched over the sensor network.

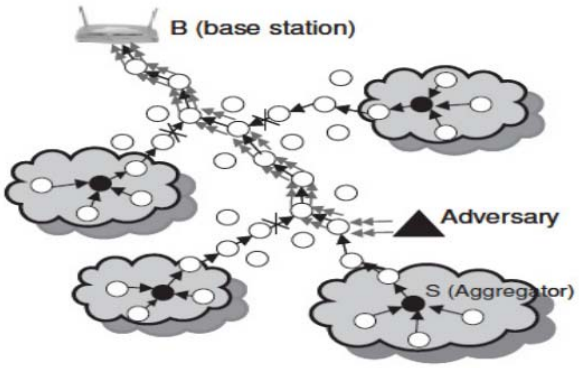

Figure.1. DDoS attack against the wireless sensor network and Wi-Fi based sensor nodes.

Hence many sensor network deployments have critical tasks hence the need for security consideration is to be taken into the account. In this paper, sensor node and sensor network using IEEE 802.11 is taken into consideration. This paper summarizes the detail view about the threats and vulnerabilities possessed over IEEE 802.11 based wireless sensor network. A few literature on mitigation techniques for threats such as DDoS can be found on [3][4]. However, these paper do not consider the relevant security issues such as data assurance, node survivability etc. The form factors mentioned here is also an important criteria to secure WSNs.

Various Network security tools such as IDS [1-5][7-11], IPS helps in identifying and preventing the attacks. Still attackers breaching the primary security is happening in all possible ways. Most of the traditional security solutions are signature based systems, since these system are to be updated periodically/intervally to endure for the real time attacks [9][11-13]. If the system with the existing security measures is compromised to any form of attacks other than in the set of lists, then the system is not able to handle those attacks. This was stated as the serious challenge, hence in order to detect an anomaly, an optimal IDS is to be developed to identify the real time intrusions[10]. Hence an external software mechanism is required in order to detect such intrusions.

The remainder of 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 LWIDS. Section IV dealt with the experimental results and The performance analysis of the proposed LWIDS with the state of the art methods is given in the penultimate section. Finally the paper is concluded in section VI.

2. Related Works

Initial level of Intrusion detection system for detecting anomalies was led by the author Salem et. Al who provides a vast range of research in designing anomaly model [6]. Next attempt for modelling anomaly based behaviour model was achieved by Bivens etal. Al at 2002, using neural network. This IDS model plays an important role in detecting network anomalies. In 2005, Salvatore et. Al designed a hardware based IDS which was proficient in nature and deployed in FPGA based embedded circuits. The main anomaly detector was designed by Laheeb at 2007, this was the first attempt made to detect the anomalies which are running as an internal threat. A new strategy of profiling scheme was proposed by the author Akaninyene who developed an IDS[4-12] to detect the network abnormality using K-means unsupervised clustering scheme. Various authors demonstrated the taxonomy of Various IDS proposed for Wired and Wireless environment; out of them some are benchmarked with its reliable efficacy and deployed in real time designated security tools.

According to Kamalnaban et al (2013) present day network security tools such as IDS[1-5][7-11], IPS helps in identifying and preventing the attacks. Most of the traditional security solutions are signature based systems, since these system are to be updated periodically/intervally to endure for the real time attacks [9][11-13]. If the system with the existing security measures is compromised to any form of attacks other than in the set of lists, then the system is not able to handle those attacks.

In general, the wireless nodes in WSN are managed by the local cluster heads where the malicious adversaries can easily compromise any child node or cluster heads to launch a successful DDoS attacks. Due to constraint factors of low end sensor nodes such as energy consumption, the malicious adversaries require enough energy to launch a successful DDoS attack in the WSN. Most of such attacks can be easily monitored using node power level and rate of packet generation from the compromised node whereas the situation for Wi-Fi enabled sensor nodes are different in our case. In higher end sensor nodes the energy criteria is not a hardening factor hence the

malicious adversaries can launch the attack from any nodes at any interval t. Hence to overcome the above addressed issues a novel IDS is desirable. In this paper, a novel intrusion detection system is designed to detect DDoS attacks in IEEE 802.11 wireless network.

3. Proposed - light weight Intrusion Detection System (LWIDS)

Figure 2 shows the system architecture of the proposed LWIDS. LWIDS is classified into two main categories i) Self-Training and ii) live-testing. In self-training category, the primary task of LWIDS is to train the entire system to categorize the target network based on feature sets and auto-generated fuzzy rules. The feature sets are taken into training consideration based on the parameters and their values in normal and intrusive conditions. The features consist of commonly seen protocols in the network traffic, the traffic data rate and the flow direction. Live-Testing is the part where the IDS system is switched to promiscuous mode to tap all the traffic in IEEE 802.11 based WSN.

3.1. LWIDS components

LWIDS consists of various tools to perform basic pre-processing steps. The pre-processing step is explained as follows:

3.2. Pre-processing

Pre-processing is the first key step where the general raw traffic is structured into valuable attributes of data.

3.3. Normalizing the attribute data

Data normalization is achieved using Min-max normalization technique. Normalization is performed to distribute equal weights among the attributes. Here the data is scaled to fit the minimum and maximum range of the values. The min-max value fitting is achieved using the formulae for the value tends from A to B which fits the limit of C,D

$$B = [(A - \text{min\_value}(A)/(\text{max\_value}(A)-\text{min\_value}(A))]*(D-C)+C \quad ...1$$

3.4. Feature transformation

Feature transformation is the process to convert the continuous feature to discrete feature nominal feature with a finite set of feature values. This transformation is to be performed in order to enhance the performance of the feature classifier. For larger datasets, most of the classifiers are capable to classify the discrete domain features only and fails to handle the continuous feature sets. Hence it is mandatory to perform feature transformation.

Hence in order to perform feature transformation, Equal Width Discretization technique is used. The method uses the split of equal number of bins where the large continuous feature sets are divided into equal bins of K. Here the min -max values of the divided feature sets are considered at time t and calculated width for each bin is as follows

$$\text{Width of each bin} = (\text{Max} - \text{Min})/T$$

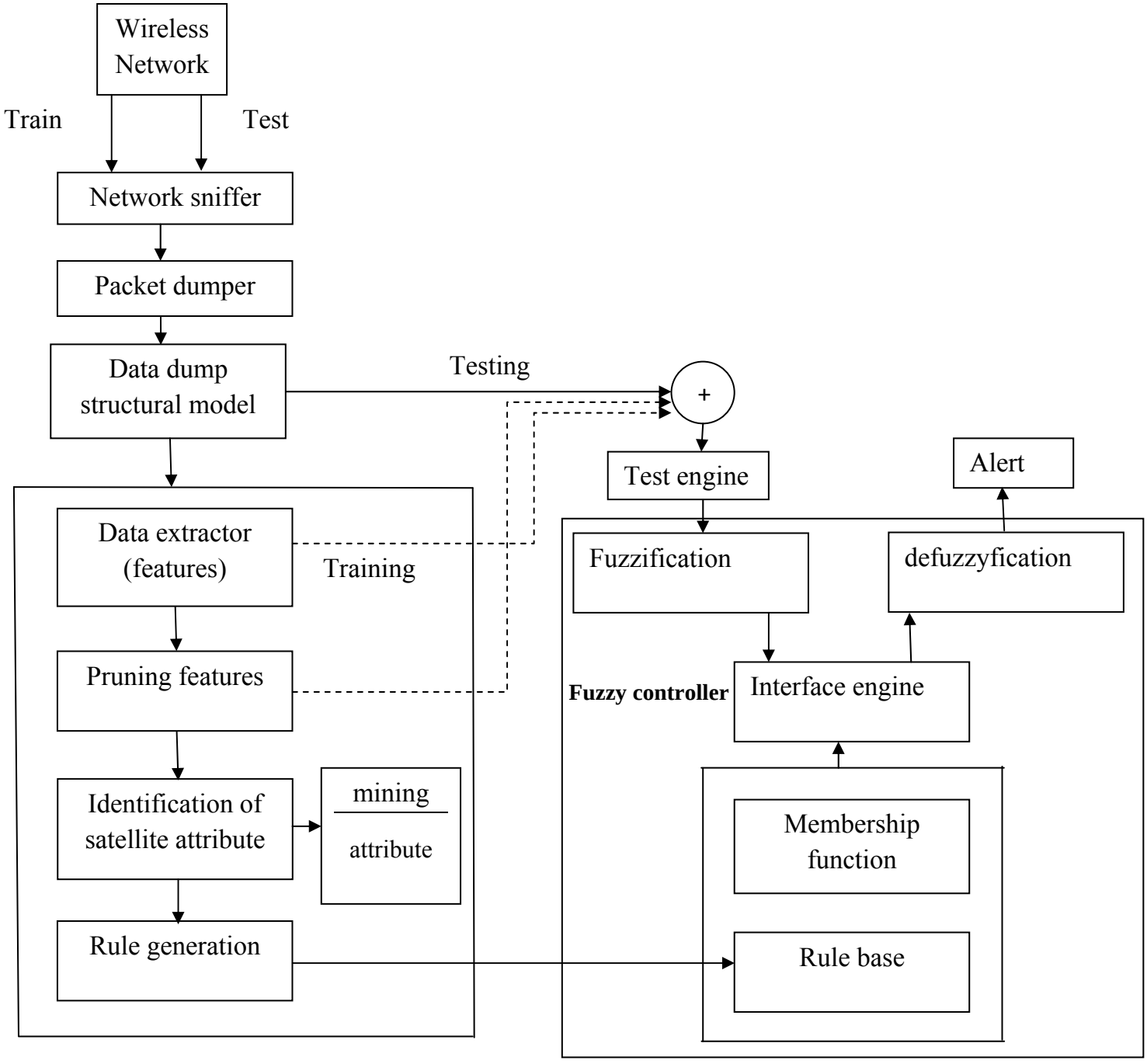

Figure 2. System architecture of the proposed LWIDS

3.5. Feature extraction

Once the feature bins are calculated and grouped. Each bins are allowed to form a structural data model. Here, KDD dataset is modified for IEEE 802.11 based WSN and used. The features in the bins are stored in KDD format. The modified KDD format for IEEE 802.11 based WSN is defined in Figure 3.

back dos
buffer_overflow u2r
ftp_write r2l
ipsweep probe
land dos
loadmodule u2r
multihop r2l
neptune dos
nmap probe
perl u2r
phf r2l
pod dos
portsweep probe
satan probe
smurf dos
teardrop dos
MAC_spoofing probe
deauth dos
deauth arp
packet_frag arp
fakeauth dos
jamming dos
proc_ipv4 u2r
dummy_mac arp

Figure 3. Modified KDD feature format

3.6. Feature selection

Feature selection is one of the important step to be carried out on selecting the features based on some functional criteria. Here, Correlation based feature selection method is used to select the feature subsets. CBFS uses correlation rank between the features and calculates the amount of correlativity among feature sets.

3.7. Fuzzy rules based decision tree classifier

Fuzzy rule generation is based on rule matrix which depends on fuzzy operation. A simple fuzzy rule can be a combination of two or more fuzzy operations. Fuzzy operations are combined to form rules based on two or more inputs. Fuzzy operators include OR, AND, NOT. Rule matrix is a simple form to map fuzzy rules. Fuzzy inference system is used to correlate the given input to the prediction based on logic and FCM. In this paper, Mamdani method is used as fuzzy inference system.

$$\mu : X \rightarrow [0,1] \quad (1)$$

where μ is the function and X is the feature set
Let us consider the simple fuzzy rule for detecting deauthentication frames in the single host and single network. Let host1 and network1 be in the same environment

Frame1 = IF wlan.fc.type_subtype == 0x0C AND BSSID = AP_mac THEN ALERT = DDoS
Frame2 = IF wlan.fc.type_subtype == 0x0A AND BSSID = AP_mac THEN ALERT = DDoS
Frame3= IF wlan.fc.type_subtype == 0x02 AND BSSID = Client_mac THEN ALERT = DDoS
Frame4= IF wlan.fc.type_subtype == 0x00 AND BSSID = Client_mac THEN ALERT = DDoS
Frame5= IF wlan.fc.type_subtype == 0x04 AND BSSID = Client_mac THEN ALERT = Probing

where alert module is c, where wlan.fc.type_subtype is x_0 and BSSID is y_0 (host/network identity)
The firing values are represented as α_i, where i = 1,2 follows

$$\alpha_1 = 0x0C(x_0) \wedge 00{:}FE{:}DE{:}A3{:}44{:}52(y_0)$$
$$\alpha_2 = 0x0A(x_0) \wedge 00{:}FE{:}DE{:}A3{:}44{:}52(y_0)$$
$$\alpha_3 = 0x02(x_0) \wedge 00{:}AA{:}44{:}55{:}AD{:}42(y_0)$$
$$\alpha_4 = 0x00(x_0) \wedge 00{:}AA{:}44{:}55{:}AD{:}42(y_0)$$

$$\alpha_5 = 0x04(x_0) \wedge 00{:}AA{:}44{:}55{:}AD{:}42(y_0)$$

The derived rule prediction and its associated output is denoted as follows

$$C_1^{'}(\omega) = (\alpha_1 \wedge C_1(\omega))$$
$$C_2^{'}(\omega) = (\alpha_2 \wedge C_2(\omega))$$
$$C_3^{'}(\omega) = (\alpha_3 \wedge C_3(\omega))$$
$$C_4^{'}(\omega) = (\alpha_4 \wedge C_4(\omega))$$
$$C_5^{'}(\omega) = (\alpha_5 \wedge C_5(\omega))$$

The overall rule framed from the derived prediction is as follows

$$C(\omega) = C_1^{'}(\omega) \vee C_2^{'}(\omega) \vee C_3^{'}(\omega) \vee C_4^{'}(\omega) \vee C_5^{'}(\omega)$$
$$= (\alpha_1 \wedge C_1(\omega)) \vee (\alpha_2 \wedge C_2(\omega)) \vee (\alpha_3 \wedge C_3(\omega)) \vee (\alpha_4 \wedge C_4(\omega)) \vee (\alpha_5 \wedge C_5(\omega))$$

3.8. Fuzzy Cognitive Mapper and Fuzzy Controller

FCM is used to map two or more fuzzy rules based on periodic time interval t i.e., the malicious activities defined by two or more rules can be mapped using FCM to infer better knowledge information. Alert generation module is designed based on the fuzzy controller which works on the basis of Fuzzy associative Map (FAM) to calculate and generate alert as the classified form. The alert level raised by the controller lies on high to low rate. The severity of the attack is measured based on the correlativity of the feature set using CBFS method.

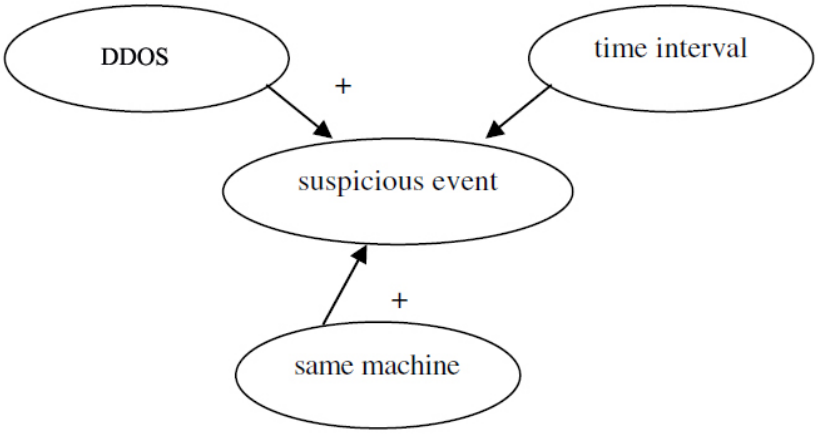

Figure 4. Fuzzy cognitive mapper for Deauthentication (DDoS)

4. Experimental setup

The experimental setup is carried out using three Raspberry Pi 3 with built-in Wi-Fi modules, One server, three laptops. Here the Raspberry Pi 3 module runs in Raspbian OS whereas rest of all runs in Parrot operating system. The proposed LWIDS is deployed in the server and act as the base station to all the Raspberry Pi nodes. Here Raspberry Pi nodes are assumed to form an IEEE 802.11 based WSN with Wi-Fi as communication protocol. All the sensor nodes are directly connected to the server by dynamic addressing achieved using separate server specific DHCP. The server is the gateway node used to store and compute client nodes data. All the laptops are preinstalled with aircrack-ng a built-in wireless pentesting utility. Laptops are networked and controlled by Job manager to perform intrusions randomly. Job manager is assigned with job scripts to execute the payload. Various experimental test cases are carried out to perform attacks such as Deauth, Fakeauth, MITM etc. The experimental procedure for IDS deployment is mentioned as follows:

4.1. Experimental procedure for learning (training)

Step 1: airmon-ng is used to enable the interface in mon_0..mon_n or $wlanmon_0$ .....$wlanmon_n$

Step 2: Pre-processing the raw traffic is initially achieved using t-shark on the interface wlanmon0. Here the t-shark utility enables the tapping interface to wlanmon0.

Step 3: Once the pre-processing is done, then the feature value is extracted by passing the data in a KDD 99 IDS data format in the form of JSON.

Step 4: The extracted features are stored in the CSV format and class is labeled for both normal and abnormal traffic. For abnormal traffic the pattern of abnormality is also mentioned in the format.

Step 5: The rule matrix is initiated based on fuzzy logic to generate the rules

Step 6: After the rule generation, the rule is stored in knowledge base

4.2. Experimental procedure for detection (testing)

Step 1: airmon-ng is used to enable the interface in mon_0..mon_n or $wlanmon_0$ .....$wlanmon_n$

Step 2: Pre-processing the raw traffic is initially achieved using t-shark on the interface wlanmon0. Here the t-shark utility enables the tapping interface to wlanmon0.

Step 3: Once the pre-processing is done, then the feature value is extracted by passing the data in a KDD 99 IDS data format in the form of JSON.

Step 4: The extracted features are passed to the fuzzy controller where fuzzification takes place.

Step 5: Then the fuzzified data is processed in the fuzzy inference engine

Step 6: Fuzzy inference engine generates the output data based on the rules trained and stored in knowledge base

Step7: The output is then given to defuzzification engine to convert fuzzy data into normal data

Step 8: If the data predicted is subjected to any abnormality then the alert module is triggered.

Figure 5 shows the results of LWIDS captured data for normal traffic and abnormal traffic pattern for the time interval of 4 hours. Green spikes represents the normal traffic where as yellow spikes represents the abnormal traffic. The traffic is live and network generated.

5. Experimental Test cases:

All the laptops have configuration of Intel i7 processor with ASUS USB-N13 N300 and set to mon0 mode to perform and tap the packets in the air.

5.1. Attack Scenario

Deauth: Laptop1 is equipped to capture al the packets using airodump-ng utility. Laptop 2 is equipped with aireplay-ng with the payload Deauth. The BSSID is captured and tapped easily when running airodump utility. The payload is configured in such a way that to send deauthentication request frame to both client and server in equal interval of 5 millisecond.

Fakeauth: Laptop 3 is equipped with aireplay-ng with the payload fakeauth. The BSSID is captured and tapped easily when running airodump utility. The payload is configured in such a way that to send deauthentication request frame to both client and server in equal interval of 15 millisecond.

Figure 5. Normal traffic vs abnormal traffic

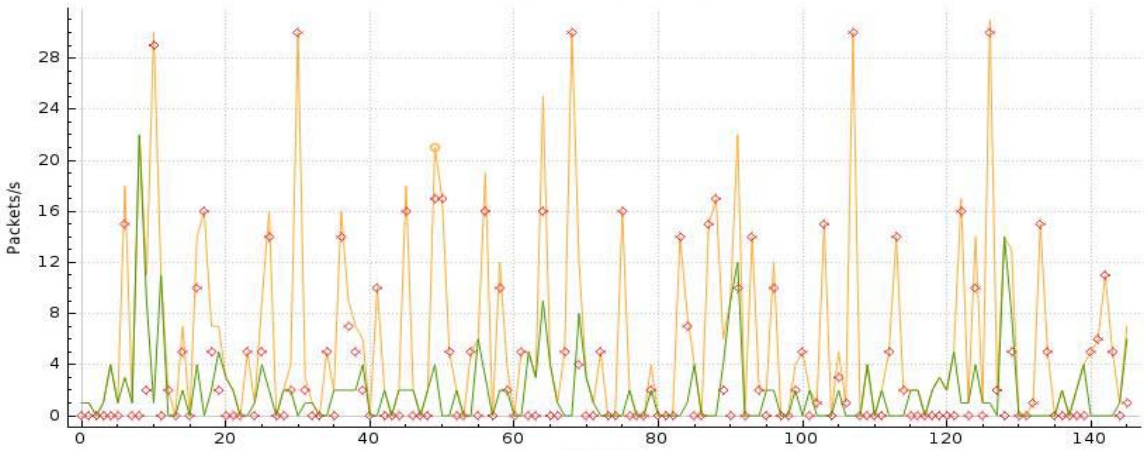

Figure 6. Normal traffic vs abnormal traffic with correlated entropy

Figure 6 represents the entropy calculated for abnormal traffic and point of variation in traffic is also denoted as red spots. Figure 7 clearly shows the results of abnormal packet generated at the periodic time interval. Red impulse line shows the abnormality in traffic and excessive packet generated in the network.

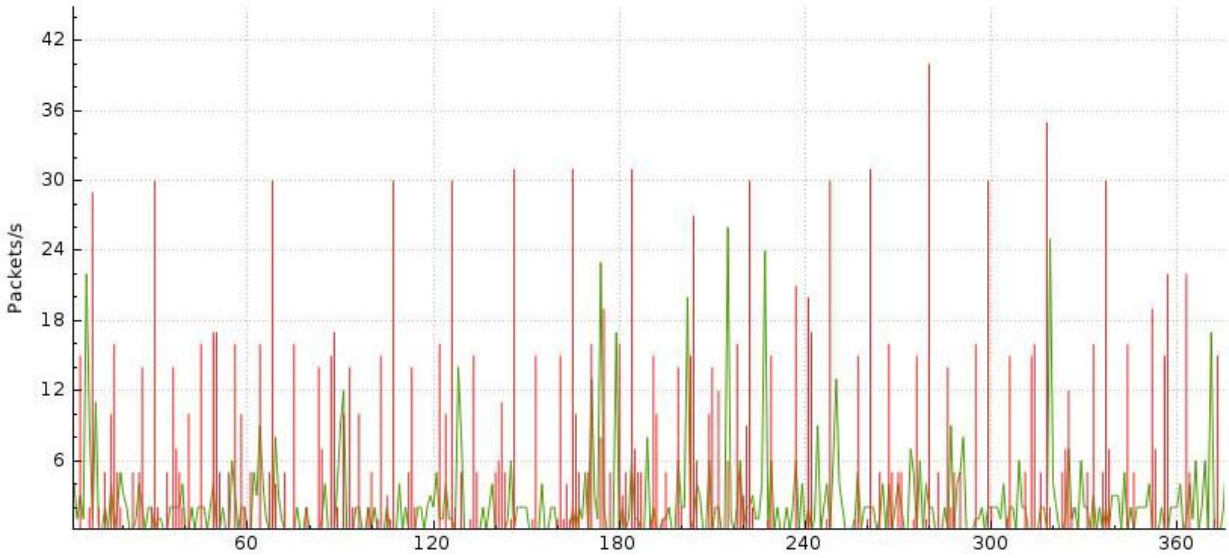

Figure 7. Normal traffic vs DDoS traffic

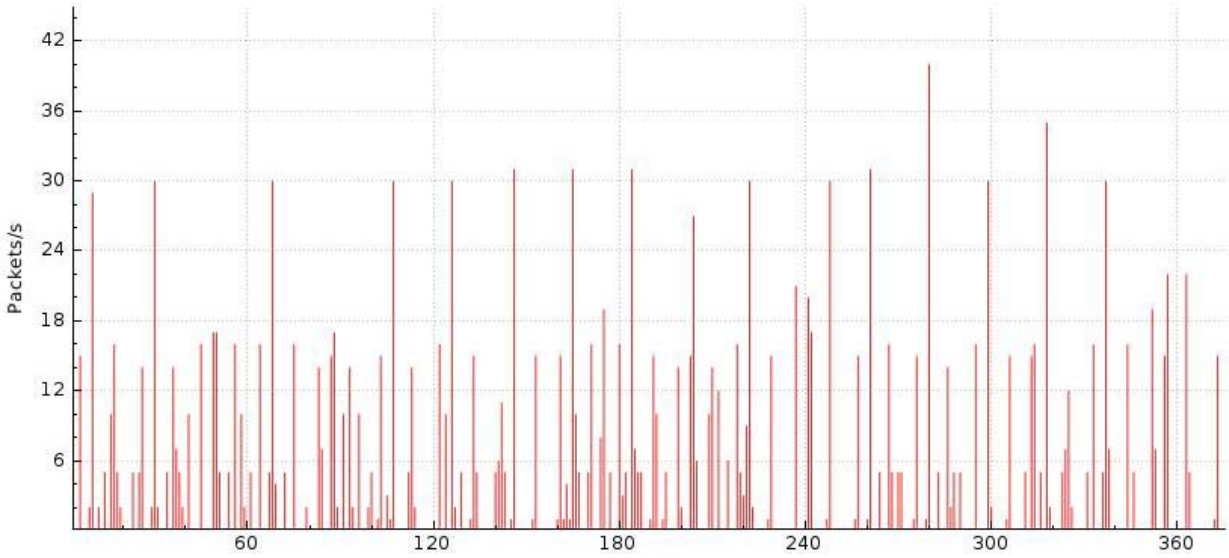

Figure 8. Detected DDoS traffic

Figure 8 shows the DDoS traffic detected at each point of interval at time t. The overall detection rate for malicious packets is also denoted. The malicious packet rate is shown in Figure 9. Most of the payloads used here are deauth and jamming attacks. From the figure it is observed that the malformed packets detected is nearly found in all the interval of time t.

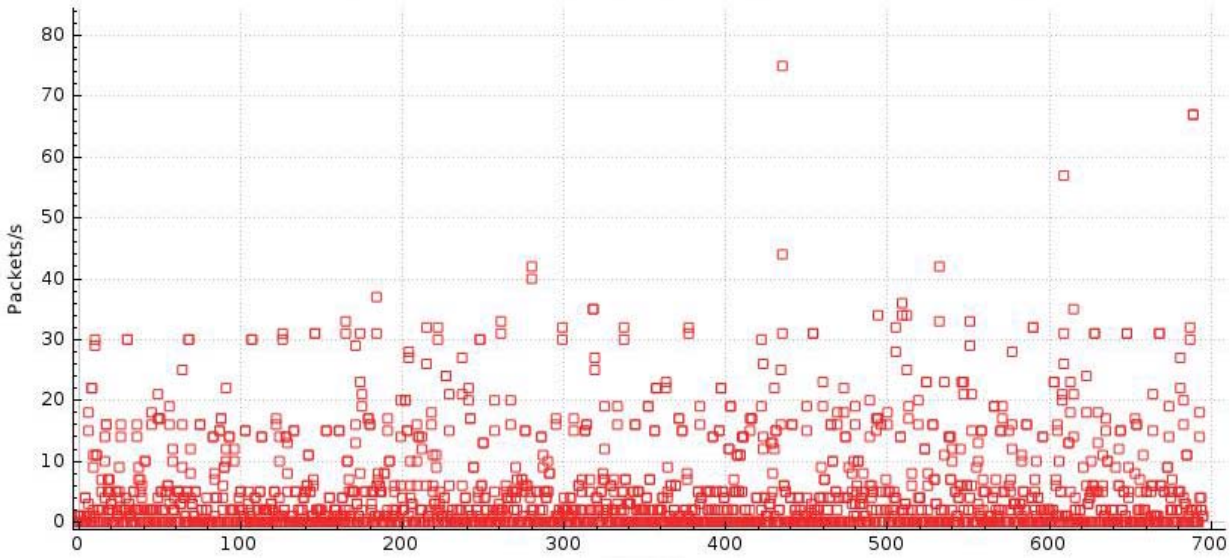

Figure 9. DDoS detection rate

6. Performance analysis

The performance of the proposed LWIDS is calculated based on comparing various evaluation parameters such as Accuracy, precision, recall, F measure, kappa statistics, ROC, False positive rate and True negative rate etc. Here the kappa statistic is used not only to evaluate a single classifier, but also to evaluate classifiers amongst themselves. The fuzzy inference rule engine classification is compared with traditional classifiers such as Random forest, K-means etc. Figure 10 shows the throughput of the network at interface wlan0, wlanmon0. Figure 11 and Figure 12 shows the results of two fold ROC validation for the proposed LWIDS. From the observation it is clearly shown that the proposed LWIDS is better in performance to the large scale networks.

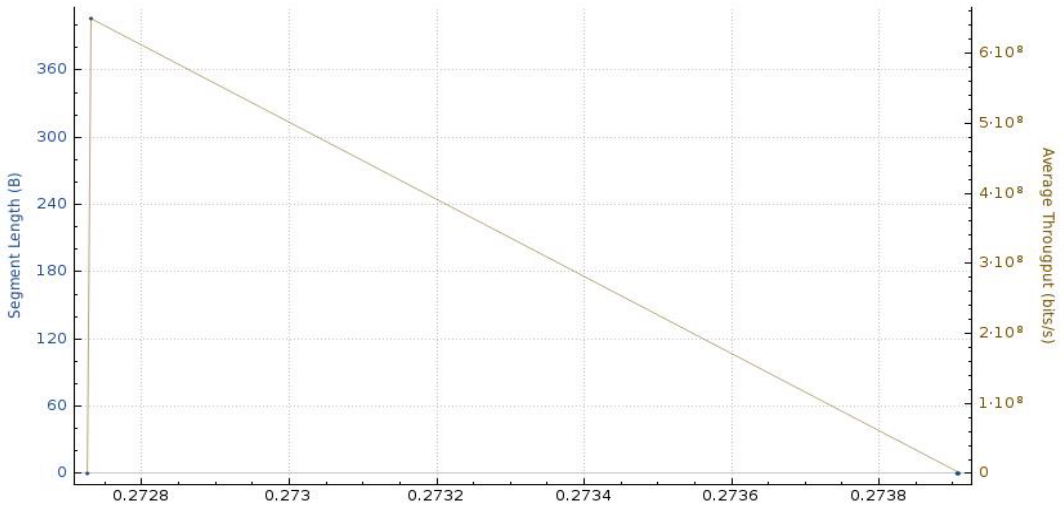

Figure.10 Throughput of interface wlan0

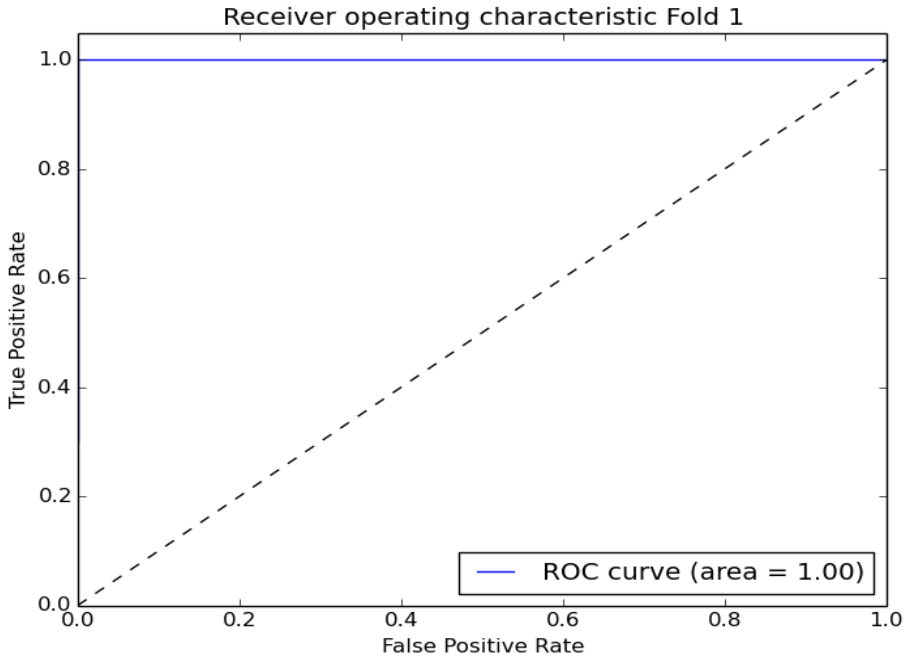

Figure 11. ROC curve for operational fold 1

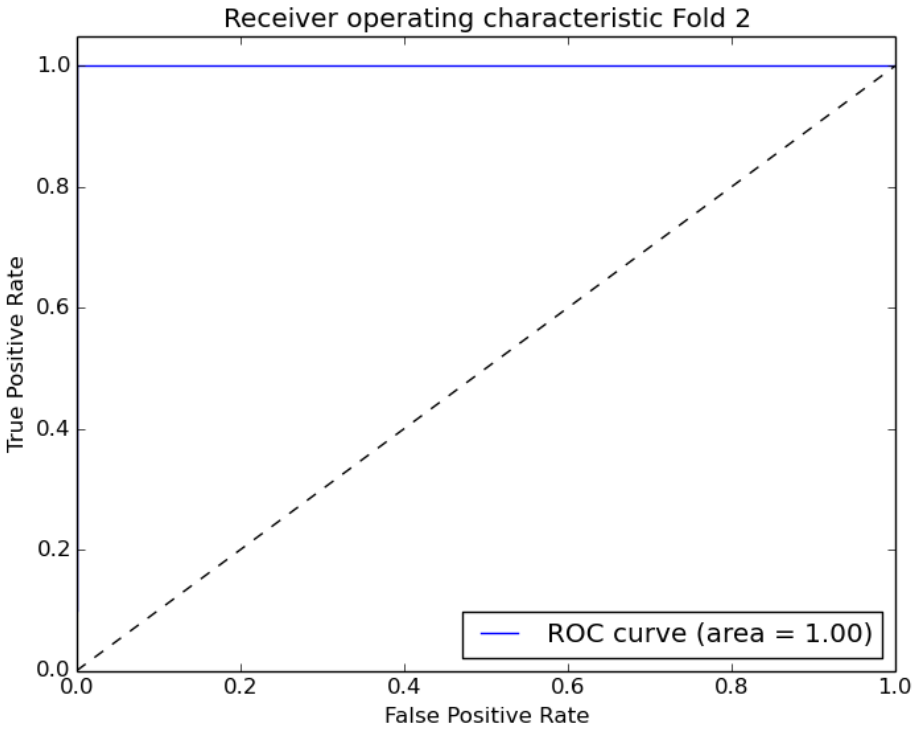

Figure 12. ROC curve for operational fold 2

7. Conclusion

Hence this paper is concluded by proposing a robust light weight wireless Intrusion Detection System (LWIDS). From the experimental results it is shown that the proposed IDS is robust enough to detect DoS attacks in the wireless network with the base of IEEE 802.11. The methodology used in the LWIDS is robust enough with additional components to reduce overheads and performance related issues. Selection of features is a major criteria in designing an optimal IDS. In this paper such issues have sort out and selection parameters for specific attacks such as Deauth, fakeauth etc has been fetched as predefined rules in knowledge base. This helps IDS to identify the malformed traffic by computing very few correlations rather than to perform general traffic correlation. The approach used here is self trained model therefore it can be adoptable to any networks and rules are also auto generated which makes the system to accurately predict the defined attacks in the rule set. In future, the LWIDS can be enhanced by incorporating machine learning techniques in order to automate specific rule base or rule engine. So that the automated procedure can lead the IDS to develop self learned rules.

References

[1] F. Akyildiz W. Su Y. Sankasubramaniam E. Cayirci, "Wireless Sensor Networks: A Survey", Computer Networks, vol. 38 pp. 393-422 2002.

[2] Y. X. Li, L. Qin and Q. Liang, "Research on Wireless Sensor Network Security", *International Conference on Computational Intelligence and Security*, Nanning, 2010, pp. 493-496.

[3] 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.

[4] *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

[5] 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.

[6] 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.

[7] 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.

[8] L. Frikha, Z. Trabelsi and S. Tabbane, "Simulation, optimisation and integration of Covert Channels, Intrusion Detection and packet filtering systems," *2009 Global Information Infrastructure Symposium*, Hammemet, 2009, pp. 1-4. doi: 10.1109/GIIS.2009.5307102.

[9] E. Tumoian and M. Anikeev, "Network Based Detection of Passive Covert Channels in TCP/IP," *The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05)l*, Sydney, NSW, 2005, pp. 802-809.

[10] G. Schwenk and K. Rieck, "Adaptive Detection of Covert Communication in HTTP Requests," *Computer Network Defense (EC2ND), 2011 Seventh European Conference on*, Gothenburg, 2011, pp. 25-32.
[11] Yali Liu, C. Corbett, Ken Chiang, R. Archibald, B. Mukherjee and D. Ghosal, "SIDD: A Framework for Detecting Sensitive Data Exfiltration by an Insider Attack," *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, Big Island, HI, 2009, pp. 1-10.
[12] 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.