ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

A Robust Method for Recognition of De-Authentication Dos Attacks

Manish Tyagi[*1], Seema Narvare[2], Chetan Agrawal[3]

PG Scholar, CSE Dept. RITS, Bhopal, India[1]

Asst. Prof., CSE Dept. RITS, Bhopal, India[2,3]

Abstract: In this paper we look into the deauthentication Denial of Service (De-DoS henceforth) attack in 802.11 Wi-Fi networks. The attack is very serious in nature, as the usage of few system resources can actually disconnect the Wi-Fi clients connected to the network facing immediate disconnection. The primary reason for this attack is the MAC layer vulnerabilities that exist in 802.11 Wi-Fi networks. Many current solutions to deal with De-DoS attack propose usage of digital certificates, using encryption, up-gradation of standards, and other cumbersome solutions which are difficult to deploy and increase the maintenance costs. In De-DoS attack and attacker sends a large number of deauth frames targeting a set of clients. All the client receiving this deauth frames are immediately disconnected from the network. In this paper we propose a Machine Learning (ML) based Intrusion Detection System (IDS) to identify the De-DoS attack in Wi-Fi network. The proposed solution is effective and has high detection rate and accuracy and does not have the problems associated with the existing solutions.

Keywords: Deauthentication DoS, Wi-Fi Security, Intrusion Detection System.

I. INTRODUCTION

Wireless Local Area Networks (WLANs) [1] has been adopted at a variety of places worldwide due to its ease of installation, hassle free expansion and absence of wires. Many Wi-Fi AP are deployed worldwide and in-fact many offer frees Internet access to the users. Many cities, airports, libraries, coffee shops now have Wi-Fi Internet providing Internet connectivity to its users enabling the users to stay online on to go. However, Wi-Fi internet possesses serious security risks also. The sending of frames over the air enables an attacker to spoof and sniff the Wi-Fi frames easily. A user using unsecured Wi-Fi can be easily tricked into clicking on luring ads thereby collecting his/her personal information easily. Many penetrating OS like Kali come with built in tools to launch a myriad of attack on Wi-Fi networks.

Wired Equivalent Privacy (WEP) provided by IEEE is long broken. Researchers have even proposed methods to crack the WEP password in less than 60 seconds [2], [3]. WEP almost became a synonym for unsecured Wi-Fi internet. Later IEEE proposed the WPA, WPA2 encryption standards that provided robust security features and are still used across various places. All the encryption schemes of 802.11 standards like WEP, Wi-Fi Protected Access (WPA), and WPA2 encrypt only the data frames. The management and control frames are left unencrypted. These management and control frames are vulnerable to various attacks [4]. In this paper we focus on the De-DoS attack.

An attacker launches a De-DoS attack by injecting a large number of spoofed deauth frames targeting a set of client(s). De-authentication frame(s) are not encrypted since they are management frames. So it's easier to spoof these frames also. As we shall see, De-DoS attack can be launched using minimal resources. Existing methods handle the De-DoS attack using the following mechanism:

- Encryption
- Digital Certificate
- Protocol Up-gradation
- Standard Up-gradation
- H/w & S/W changes

All of the above methods are either too expensive or require too high management and maintenance costs. So, the existing methodologies are expensive. So we see that, adoption of the existing schemes to handle De-DoS attack leads to increased running as well as maintenance costs.

In this work, we propose a machine learning (ML) based IDS for detecting the De-DoS attack in 802.11 networks. The advantage of our approach is that it works both on legacy as well as modern day networks. It does not require any sort of protocol modifications, encryption etc and works across various networks. The only requirement of it is a hardware

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

wireless sniffer that can sniff the radio frames that travel in the air. ML has found a lot of applications across various domains like fault detection, pattern recognition, Spam filtering, image processing, atmospheric study, security, traffic control and many more [5], [6]. To the best of our knowledge, none of the approaches in the literature use ML based methods to detect De-DoS attacks in 802.11 Wi-Fi networks.

The summary of the contributions are:

1) A ML based IDS for detecting De-DoS attack is proposed. It overcomes the drawbacks of existing approaches and provides high detection rate and accuracy.

2) It does not require encryption, any sort of protocol up gradation, standard up gradation etc

3) The proposed technique is applicable to legacy, encrypted as well as non-encrypted Wi-Fi networks.

4) It does not require any changes on the client s/w or h/w.

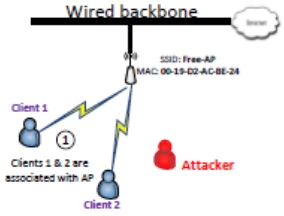

Fig. 1: Before De-authentication DoS attack scenario.

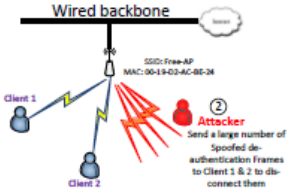

Fig. 2: During De-authentication DoS attack scenario.

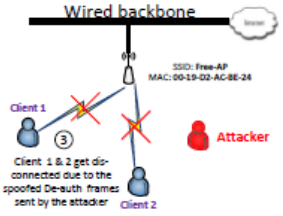

Fig. 3: After De-authentication DoS attack scenario.

The organization of our paper is as follows. In Section II contains the Wi-Fi basics along with De-DoS attack. We detail our current approaches to handle the De-DoS attack in the same section. Our proposed architecture for ML based IDS and the various ML techniques used are explained in Section III. The experimental results for recall (detection rate) and precision (accuracy) and for the proposed ML based IDS are elaborated in Section IV. Finally we conclude our paper in Section V.

II. BACKGROUND AND MOTIVATION

This section begins by describing the basic stuff about the Wi-Fi networks, their working. It is followed by the discussion of vulnerabilities associated with the management and control frames and how De-DoS attack is easily achievable via minimum resource usage. We also discuss the De-DoS attack in detail in this section. Finally we describe the motivation behind this work.

A Wi-Fi network consists of a Wi-Fi client and an Access Point (AP). The AP acts as a central authority between Wi-Fi clients. All the communication that happen in a Wi-Fi network happens via the AP. In order to access the services offered by the AP the station needs to first authenticate itself to AP and then associate it with the same AP. A Wi-Fi client can be in any of the 3 states depicted in Fig. 4.

- State 0: Client is neither authenticated nor associated.
- State 1: Client is authenticated but not associated.
- State 2: Client is both authenticated as well as associated. The client can now perform data exchange with the AP after it is in State 2.

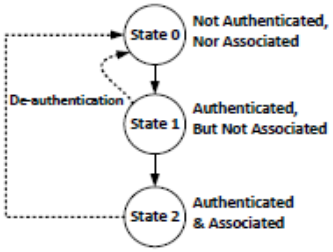

Fig. 4: Possible states of a Wi-Fi client.

When a client receives a deauth frame (irrespective whether it's spoofed or real) it directly comes to state 0 irrespective of the state it is presently in. So, in a De-DoS attack when the attacker sends a large number of deauth frames all the affected clients reach state 0 and hence needs to re-authenticate and re-associate which is a costly process. Hence De-

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

DoS attack is a catastrophic attack. Also, it breaks ongoing downloading and transaction being performed by the client. An attacker usually does De-DoS attack on multiple users simultaneously

A. De-auth DoS Attack

The de-authentication frame is a management frame and hence is not encrypted (sent in clear text). Clear text is always easier and faster to process as compared to their encrypted counterparts. On the other hand, it is very easy to spoof clear text frames as all the info in them is easily available making it easier for the attacker. In De-DoS attack the attacker checks the deauth frame format sent by a client / AP and then crafts similar frames targeting other users in the network. If a set of users are being targeted again and again, they may completely get off the Wi-Fi network due to frequent disconnection.

De-authentication frame shall not be refused by either party as per the 802.11 standard. [1]. When a client (AP) sends a de-authentication frame to an associated AP (client), the association ends. An example of De-DoS attack is depicted in Figs. 1, 2 and 3. Fig. 1 represents the pre-attack scenario (normal network conditions assumed), Fig. 2 shows the network under De-DoS attack conditions and Fig. 3 depicts the network scenario after De-DoS attack is launched. Here we assume that the targeted users were initially browsing the Internet and attacker promiscuously watched their communication pattern to obtain their IP address and other information. After getting the set of client to target the attacker launches the De-DoS attack and gets the users disconnected from the network. In pre-attack scenario as depicted in Fig. 1, it can be seen that the clients 1 & 2 are associated with the AP. The attacker then launches De-DoS attack on both clients 1 & 2 by injecting spoofed de-authentication frame(s) in the network. Attacker can spoof the frames using scapy or mdk2 tool available in UNIX. In post-attack scenario depicted in Fig. 3, client 1 and client 2 are disconnected from the AP caused by De-DoS attack launched by the attacker. There are a number of ways an attacker can launch the De-DoS attack which are listed as below:

- Spoofed AP to client De-authentication Frame: In this mode of attack, the attacker takes the AP MAC address and client MAC address following which it crafts a spoofed deauth frame which appears to be coming from the AP to the client. When the client receives and processes this frame it assumes that the genuine AP had sent this frame and gets disconnected from the network.
- Spoofed client to AP De-authentication Frame: It is similar to above approach but the SRC MAC address and DST MAC address are reversed.
- Broadcast Spoofed De-authentication Frame: This is a severe form of attack done by the attacker where the SRC MAC address is set as AP MAC address and DST MAC address is set to broadcast address thereby disconnecting all clients associated with the same AP.

To launch the De-DoS attack an attacker can use built in utilities like aircrack-ng suite [7] and scapy which are freely available in BackTrack, Kali and other penetrating operating system. The information required by the attacker is: channel number on which the AP is running, MAC address of AP, network name of the AP (SSID), and client(s) MAC address. Tools like tcpdump, Wireshark, kismet, airodump-ng etc. readily provide this information required by the attacker are: channel number on which the AP is running, MAC address of AP, network name of the AP (SSID), and client(s) MAC address. Tools like tcpdump, Wireshark, kismet, airodump-ng etc. readily provide these information.

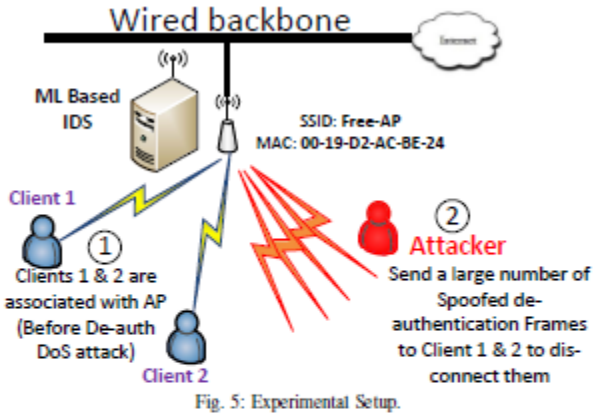

Fig. 5: Experimental Setup.

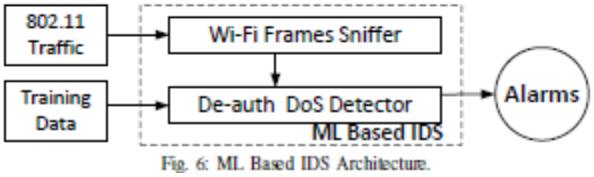

Fig. 6: ML Based IDS Architecture.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

B. Existing Solutions to mitigate De-DoS attack

In this sub-section, we look at the various approaches proposed in the literature that help to mitigate the De-DoS attacks. The obvious approach is to use encrypt all the deauthentication frames that travel in the network. By default deauthentication frame is non-authenticated, so by encrypting the deauthentication frame it will be impossible to spoof them by the attacker. Bellardo [4] suggests that authenticating the deauthentication frame can help prevent the De-DoS attack. Next, Nguyen et al. [8] proposes a Letter-envelop protocol that proposed to establish a secret key between the AP and the client. This is used to authenticating the de-authentication frame sent by the client in order to prevent spoofing. This approach is useful in preventing De-DoS attack but the issue is that it requires firmware upgrades on both the client as well as AP which increases the cost.

Next, the major approach is - Protocol Modification and Upgradation based methods. The idea here is that 802.11 protocol needs to tweaked or completely upgraded to a more secure version in order to prevent De-DoS attack. Bellardo [4] suggests a method that says to delay the effect of all management frames. If a normal data frame comes after a deauth frame sent by the client it is definitely a De-DoS attack since a normal client shall never send frames in this order. It will deauth, re-auth and then sends data frames. However, this approach may delay the authentication of roaming clients and also requires firmware upgrades. 802.11w standard is a promising upgrade that provides inbuilt protection to the De- DoS attack. However it is a quite recent standard and again requires both hardware as well as software upgrades and hence less popular. However it provides inbuilt mechanism for the prevention of De-DoS attack. Few other related methods can be referred in [9], [10], [11]

Under non-encryption based methods is one proposed by Agarwal et al. [12] detect the De-DoS attack by setting a threshold on the number of de-authentication frame(s) received by a client. If for a user, the number of deauth frames received is less than a threshold network is reported to be under normal conditions, while if more frames are seen, then network is reported to be under De-DoS attack. The threshold is set by the administrators which can be tweaked. However, setting the threshold can be a cumbersome task, as experts may have different opinion for the number of frames to be set as threshold. Sequence number based methods are also an approach proposed in the literature where the sequence numbers of adjacent frames are compared. Normally, the Sequence Number incremented by 1, every frame. However, if a different increment sequence number is found in a deauth frame, it indicates towards a possible De-DoS attack in the network. Other relevant studies can be found in [13], [14], [15].

In brief, we can list down the following drawbacks of the proposed approach to detect and prevent the De-DoS attacks are as follows:

1) Does require major modifications in 802.11 protocol.
2) Required hardware and software upgrades to support authentication and encryption of frames which are currently non-authenticated.
3) Patching AP and client software.
4) Upgradation to newer 802.11 standards like 802.11w which requires firmware upgrades and is costly.

We now discuss our proposed ML based IDS that overcomes the disadvantages of the existing approaches.

III. PROPOSED ML BASED IDS

The proposed IDS have the following experimental setup shown in Figs. 5 and 6 respectively. The IDS is purposefully placed closed to the real AP so that it never misses a frame traveling from the real AP and reaching the real AP. In this section, we look into the vital components of the proposed ML based IDS and describe them in detail. The feature selection is always a critical part of any ML based application. Following that, a short description of the various classifiers used in the IDS proposed are also discussed. The flow Diagram of the proposed ML based IDS is shown in Fig. 7.

Major IDS Components the ML based IDS primarily consists of two main components: Wi-Fi Frames Sniffer and De-auth DoS Detector module. We detail them out below:

- Wi-Fi Frames Sniffer: Sniffer's job is to sniff raw frames traveling in the network. It ignores the frames being sent to other Wi-Fi AP as the sniffer is configured to monitor only the AP under consideration. It also forwards frames to the De-auth DoS Detector.
- De-auth DoS Detector: This module is trained using offline generated dataset. The method of generation of the training and testing dataset is described in the following sub-section. Based on the Training Data, the De-auth DoS Detector is appropriately trained which helps it to identify the patterns and statistical features required for identifying the occurrence of the De-DoS attack and deployed on a live network. While capturing the network statistics for various clients connected to the monitored AP this module determines whether De-DoS attack has occurred or not. If the module detects that a De-DoS attack has been occurred it raises an alarm to the administrator indicating the occurrence of the De-DoS attack.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

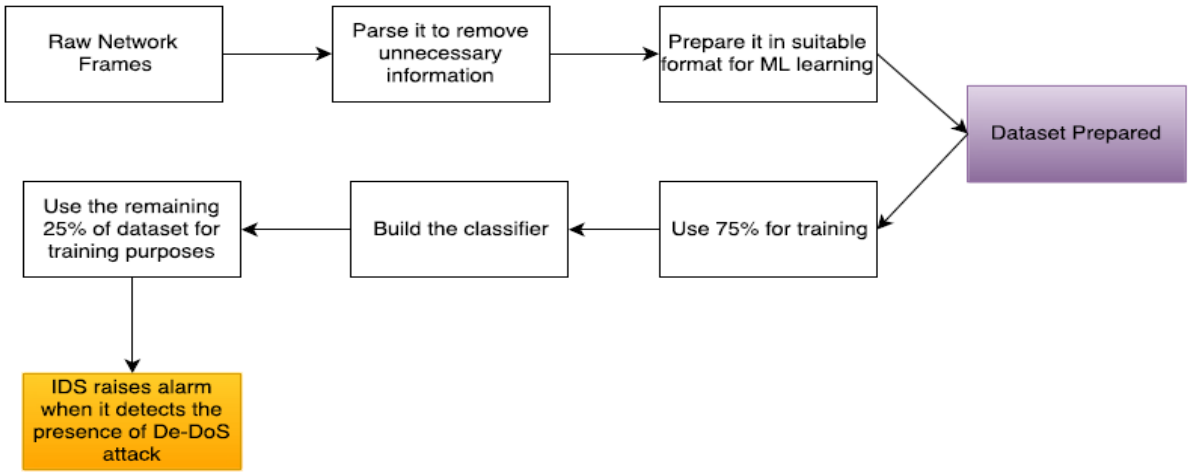

Fig. 7: Flow Diagram of the proposed ML based IDS.

A. Testing and Training Dataset Generation

As no public dataset was available we made use of tools available in backtrack and Kali Linux in order to generate the dataset. The dataset contained information about the various clients that connected to the network, and amongst those we had selected a few clients that were disconnected using the De- DoS attack. We designated 7 Wi-Fi nodes (2 laptops, 4 smart-phones and 1 tablet equipped with Wi-Fi connectivity) as clients. The attacker machine is configured with BackTrack 5R3 x64 bit operating system installed. BackTrack operating system has an exclusive suite of commands that can be used to launch various attacks on Wi-Fi networks. For this case we have taken the aircrack-ng suite which is used to launch De-DoS attack.

All the clients under testing are connected to the same AP for convenience. For sniffing purposes we dedicate a Linux machine with Ubuntu 14.04 x64 operating system installed. For frame capturing we have used the pcap library. Alternatively, Wireshark could also be used. The traces collected by Wireshark are then subjected to filtering, data sorting, extraction of useful features, and creation of dataset that can be fed to WEKA. The clients are asked to perform routing network activities like surfing, downloading, heavy data transfer, client doing transactions, client with little data transfer. This helps to create a broader view of the data that can be used in order to separate data more effectively and make the machine learning algorithm distinctly classify the attacker and non-attacker cases. Also the De-DoS attack is launched on majority of clients and few clients are skipped. The dataset is collected over a period of 5 hours. For training purposes we use 75% of the dataset generated while the remaining 25% is used for testing purposes.

TABLE I: Ranking of features using Information Gain

Weightage	Feature
0.5092	Time_Difference.
0.4080	Deauthentication Frames.
0.0823	Frame_Exchange.
0.0613	Authentication Frames.
0.0417	TCP Frames.
0.0412	Authentication Frames.
0.0366	UDP Frames.

B. Feature Selection for the ML based IDS.

A success of any machine learning algorithm depends on the importance of the features selected. As we capture the frame traces using Wireshark, after pre-processing we analyze the frame exchange characteristics captured by Wireshark during normal and De-DoS attack situations. Using this pre-processed information we have listed down 7 features in decreasing order of their significance as depicted in Table I. We have used the information gain attribute built in WEKA in order to determine the significance of the features selected. The attribute having lower (higher) weights have lesser (higher) significance role in De-DoS attack detection.

The list of features along with their motivation behind selection for training and testing purposes the system for De-DoS attack detection is described next.

1. Time_Difference: In a De-DoS attack, when a client gets disconnected due a De-DoS attack, it is observed that the client tries to connect to the same AP as it was in a midst of a transaction (browsing, downloading etc). Since the client was abruptly disconnected, it tries to connect immediately as against this under normal situation, a client if disconnects

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

does not connect immediately. Time_Difference feature here is the subtraction in time-stamp when the client gets disconnected to the time it gets re-authenticated with the same AP. For e.g., if user get disconnected at time Ty and subsequently re-connects at time Tz then Time_Difference is difference Tz - Ty.
2. Deauthentication Frames: For successful launching of De-DoS attack, an attacker sends a large number of (#) of deauth frames to get the client disconnected. Hence the inclusion of this feature is important. More the frames sent, more surety that client is disconnected.
3. Frame_Exchange: This feature keeps tracks f frames exchanges per session. Per session implies the frames from once the client is authenticated to the time the client is disconnected. If a client is getting frequently disconnected due to De-DoS attack, this number is low else under normal conditions this is high.
4. Authentication Frames. Under De-DoS attack, due to frequent disconnections a client makes large number of re-authentications. Hence this feature is included as more re-authentication of a client is an indicator of the De-DoS attack.
5. TCP Frames. A client under normal circumstances makes a large number of TCP exchanges. However, due to the De-DoS attack, it gets frequently disconnected. Hence in a disconnected session the number of TCP exchange is low. Hence the inclusion of feature is necessary.
6. Association Frames. Similar to Authentication Frames.
7. UDP Frames. Similar to TCP frames.

C. Classifier Design and Selection

The better the Classifier Design and Selection the better is the performance of the ML algorithm. In this we look at a few classifiers that we have used. We have used various classifiers since an administrator can choose amongst them as it gives flexibility to the network administrator to use a particular classifier as per his network packet characteristics. Data classification involves 2 steps: 1) Build Classifier using training data. 2) Use the above classifier to test the data. We now look at few classifiers [6].
1) ADTree: Alternating decision trees (ADTree) algorithm is a generalization of voted decision trees, decision trees, and voted decision stumps. The ADTree algorithm makes use of boosting methods to decision tree algorithms to produce authentic classifiers. The classifiers consist of a majority vote over a large number of decision trees but having an easier and smaller to understand classification rules.
2) DecisionStump: The DecisionStump classifier constructs a binary decision 'stumps' (one level decision trees) for both nominal and numeric classification problems. It adjusts with mission values by extending a 3rd branch from treating 'missing' or stump as a separate attribute value. DecisionStump algorithm is usually used in conjunction with a boosting algorithm such as ADABoost. It does classification (based on entropy) or regression (based on mean-squared error).
3) REPTree: REPTree algorithm is a quick decision tree-learner. It constructs a regression/decision tree using the variance/ information gain attribute and prunes it using reduced-error pruning. REPTree sorts values for numeric attributes only once. If there are missing values, they are dealt with by splitting the corresponding instances into chunks (i.e. as in C4.5).
4) DecisionTable: This algorithm builds using a simple decision table majority classifier. This algorithm summarizes the dataset under consideration with a 'decision table' which usually contains the same number of attributes as that of the original dataset. Following that, a new data item is assigned a category by finding the row in the decision table that exactly matches the non-class value(s) of the data item. DecisionTable make use of the wrapper method to locate a good subset of the attributes for inclusion in the main table. By carrying off attributes that contribute nothing or little to a model of the dataset, the algorithm reduces the probability of over-fitting and creates a smaller and condensed decision table.
5) JRip: JRip applies a propositional rule learner, Repeated Incremental Pruning to Produce Error Reduction. JRip constructs a rule-set by repeatedly adding together rules to a null rule-set till all the positive samples are covered. Rules are greedily formed by adding conditions to the ancestor of a rule (starting with null ancestor) until no negative examples are covered. After a rule-set is built, an optimal post pass processes the rule-set so as to reduce its size and at the same time improve its fit to the training data. A combination of minimum-description length and cross-validation techniques is used to prevent over fitting
6) ConjuctiveRule: In this algorithm a single conjunctive rule learner is used that predicts for numeric and nominal class labels. A rule consists of ancestors "AND"ed together and the consequent for the regression/classification. In this case, the consequent consists of the distribution of the available classes of the dataset under consideration. If the test instance has not been covered by this rule, then it is predicted using the default class distributions/value of the data not covered by the rule specified in the training data. This learner selects an ancestor by computing the Information Gain attribute of each antecedent and prunes the rule generated using simple pre-pruning based or Reduced Error Pruning (REP) on the number of ancestors. For classification, the Information Gain attribute of one antecedent is the weighted average of the entropies of both the data covered and not covered by the rule. Sub lists.
In the next section, we will look into the experimental setup and the results obtained using the proposed ML based IDS.

III. EXPERIMENTAL SETUP AND RESULTS

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

The test-bed setup for the proposed ML based IDS consists of a NETGEAR AP with network name "Free-AP" along with an IDS infrastructure placed as depicted in Fig. 5. Attacker machine is loaded with BackTrack 5R3 and aircrack-ng suite is used to launch De-DoS attack. The attacker's main target is to overwhelm the victim client(s) with large number of de-authentication frame(s) so that the client(s) get disconnected resulting in DoS.

A. Precision (Accuracy) and Recall (Detection Rate) of proposed IDS For an IDS, Accuracy and Detection rate are the most important criteria for its evaluation. Accuracy is the ratio of the total number of predictions that are correct. It is determined using the equation:
Accuracy = Precision = TP/TP+FP
B. Detection Rate is defined as the number of attacks detected by the IDS to the total number of attacks actually present.
DetectionRate = Recall = TP / TP+FN

Here, the abbreviation used is:

- TP is True Positive: A TP arises when a real attack and is declared as attack by the IDS.
- FP is False Positive: A FP arises when IDS marks a normal activity as attack activity.
- FN is False Negative: FN occurs when the IDS marks an attack activity as normal.

We have tested the accuracy and detection rate of the generated dataset with various classifiers. The classifiers chosen are

- ADTree
- DecisionStump
- REPTree
- DecisionTable
- ConjuctiveRule
- JRip

We have used the WEKA tool since these classifiers are built into WEKA.
Fig. 8 shows the accuracy and detection rate of the various ML classifiers used for the proposed IDS to detect the De-DoS attack. It can be observed that quite promising results have been delivered by the various classifiers used. This helps the admin to choose a suitable classifier based on the network characteristics like the count of clients, data usage, encryption used, number of simultaneous connections etc. ADTree classifier which is a boosting based classifier has a precision (95.6%) and recall (95.6%) as compared to other classifiers. The precision and recall for DecisionStump is 86.6% and 82.4%, respectively. DecisionStump performs badly than ADTree as it does not employ boosting features. REPTree has the accuracy of 95.2% and its detection rate is 95.2%. The REPTree offers a good accuracy and detection rate, also being a tree based classifier it is fast. DecisionTable is another tree based classifier that having precision and recall rate of 95.6% which is better than other classifiers except JRip. JRip is rules based classifier and has precision and recall both at 96%. Though it's good, choosing of rules is a tedious task. With both detection rate and accuracy and detection rate more than 95%, ADTree, DecisionTable, JRip can be effectively chosen to be the classifier.

TABLE II: Comparison of Various Classification Techniques Used for Detection of De-DoS attack .

Classifier	Accuracy (Precision)	Detection Rate (Recall)	F-Measure	ROC Area
ADTree	0.956	0.956	0.956	0.985
DecisionStump	0.866	0.824	0.831	0.852
REPTree	0.952	0.952	0.952	0.971
DecisionTable	0.956	0.956	0.956	0.976
ConjuctiveRule	0.866	0.748	0.759	0.823
JRip	0.96	0.96	0.96	0.955

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

TABLE III: Comparison of existing mitigation solutions to De-DoS attack

Method	Detects/Prevents Deauth DoS attack	Requires Threshold	Requires authen-tication	Requires Protocol Modification	Requires Standard Upgradation	Overhead	Remarks
Bellardo [4]	**Overview:** Authenticate all the deauthentication frames						
	Y	N	Y	Y	N	Y	Difficult. Requires client and AP firmware upgrades.
Bellardo [4]	**Overview:** Delay the effect of frames captured.						
	Y	N	Y	Y	N	Y	Difficult. Makes roaming non-transparent.
Nguyen et al. [8]	**Overview:** Proprietary protocol to authenticate the deauth frame.						
	Y	N	Y	Y	N	Y	Difficult. Makes roaming non-transparent.
Agarwal et al. [12]	**Overview:** Threshold based deauth frame count detection.						
	Y	Y	N	N	N	N	Moderately Difficult. Setting threshold is trade off. Deauth frames below threshold always marked as normal network activity.
Standard Upgradation 802.11w	**Overview:** 802.11w has inbuilt protection for De-DoS attack						
	Y	N	Y	Y	Y	N	Difficult. Requires both hardware and firmware upgrades. Being a new standard the adoption is very low.
Guo et al. [16], Xia et al. [17] Anjum et al. [18]	**Overview:** Detect illegal jump in sequence number of the deauthentication frames.						
	Y	Y	N	N	N	N	Effectiveness is low as an intelligent attacker can tweak the sequence number count accordingly.
Proposed Scheme	**Overview:** Make use of ML based IDS						
	Y	N	N	N	N	Low	Easy to deploy on legacy as well as modern Wi-Fi networks. No protocol changes required, no encryption. High detection rate and accuracy.

IV. CONCLUSION AND FUTURE WORK

In this paper we have proposed machine learning based Intrusion Detection System for De-DoS attack detection in 802.11 Wi-Fi networks. We have shown that various classifiers used have shown pretty good accuracy and detection rate. Also the usage of various algorithms enables the administrator to choose amongst various classifiers that can be chosen based on network characteristics. Many other classifiers like ADTree, DecisionStump, REPTree, DecisionTable, JRip, and ConjuctiveRule give promising results. The proposed IDS uses the JRip classifier as both the precision and recall exceeds 96% which is quite good. Other advantages of the ML based IDS is that it does not require use of any protocol modifications, encryption algorithms or firmware upgrades. Besides this, the proposed work can be applied on legacy as well as state of art networks.

REFERENCES

[1] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), pp. C1–1184, 12 2007.
[2] E. Tews and M. Beck, "Practical Attacks Against WEP and WPA," in Proceedings of the Second ACM Conference on Wireless Network Security, ser. WiSec '09, 2009, pp. 79–86.
[3] A. Bittau, M. Handley, and J. Lackey, "The Final Nail in WEP's Coffin," in Proceedings of the 2006 IEEE Symposium on Security and Privacy, ser. SP '06, 2006, pp. 386–400.
[4] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions ," in Proceedings of the 12th Conference on USENIX Security Symposium - Volume 12, 2003, pp. 15–28.
[5] M.-K. Lee, S.-H. Moon, Y.-H. Kim, and B.-R. Moon, "Correcting abnormalities in meteorological data by machine learning," in IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2014, Oct 2014, pp. 888–893.
[6] M. Agarwal, D. Pasumarthi, S. Biswas, and S. Nandi, "Machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization," International Journal of Machine Learning and Cybernetics, pp. 1–17, 2014.
[7] "Aircrack-ng Suite." [Online]. Available: http://www.aircrack-ng.org/
[8] T. D. Nguyen, D. Nguyen, B. N. Tran, H. Vu, and N. Mittal, "A lightweight solution for defending against deauthentication/disassociation attacks on 802.11 networks," in Computer Communications and Networks, 2008. ICCCN'08. Proceedings of 17th International Conference on. IEEE, 2008, pp. 1–6.
[9] M. Bernaschi, F. Ferreri, and L. Valcamonici, "Access points vulnerabilities to dos attacks in 802.11 networks," Wireless Networks, vol. 14, no. 2, pp. 159–169, 2008.
[10] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in ieee 802.11 wireless networks," Computer Standards & Interfaces, vol. 31, no. 5, pp. 931–941, 2009.
[11] Y.-S. Lee, H.-T. Chien, W.-N. Tsai et al., "Using random bit authentication to defend ieee 802.11 dos attacks," Journal of Information Science and Engineering, vol. 25, no. 5, pp. 1485–1500, 2009.
[12] M. Agarwal, S. Biswas, and S. Nandi, "Detection of De-authentication Denial of Service attack in 802.11 networks," in Annual IEEE India Conference (INDICON) , Dec 2013, pp. 1–6.
[13] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proceedings of the 5th ACM workshop on Wireless security. ACM, 2006, pp. 43–52.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

[14] C. Liu and T. Y. James, "An analysis of dos attacks on wireless lan." in Wireless and Optical Communications, 2006.
[15] M. Raya, J.-P. Hubaux, and I. Aad, "Domino: a system to detect greedy behavior in ieee 802.11 hotspots," in Proceedings of the 2nd international conference on Mobile systems, applications, and services. ACM, 2004, pp. 84–97.
[16] F. Guo and T.-c. Chiueh, "Sequence number-based MAC address spoof detection," in Proceedings of the 8th International Conference on Recent Advances in Intrusion Detection, ser. RAID'05, 2006, pp. 309–329.
[17] H. Xia and J. Brustoloni, "Detecting and Blocking Unauthorized Access in Wi-Fi Networks," in Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications, 2004, vol. 3042, pp. 795–806.
[18] F. Anjum, S. Das, P. Gopalakrishnan, L. Kant, and B. Kim, "Security in an insecure WLAN network," in 2005 International Conference on Wireless Networks, Communications and Mobile Computing, 2005, pp. 292–297.