Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.6, No.3, 2016

A Novel Technique to Discover De-Authentication DoS Attacks in 802.11 Wi-Fi Networks

Sudeesh Chouhan[1] Prof. Sumit Sharma[2]
1.PG scholar, CSE, VIST, Bhopal, INDIA
2.HOD, CSE department , VIST, Bhopal, INDIA

Abstract
Denial of Service (DoS) Attacks in 802.11 networks is mainly caused because of weaknesses of Media Access Layer (MAC). In this article we study about the de-authentication DoS (De-DoS) attack in 802.11 Wi-Fi networks. In De-DoS attack an intruder transmits huge spoofed de-authentication frames to the client(s) which is caused their disconnection. All existing methods to overcome from this De-DoS attack are depends upon protocol alterations, encryption, 802.11 standard updating, hardware and software upgrades which are costly. In this article we proposed a novel Machine Learning (ML) based Intrusion Detection System (IDS) to recognize the De-DoS attack in Wi-Fi network which doesn't suffer from the above weaknesses. We have utilized number of Machine Learning based classifiers for recognition of De-DoS attack. This facilitates an administrator to decide between wide ranges of classification algorithms. The experiments performed using an in-house test bed shows that the proposed ML based IDS discovers De-DoS attack with precision and recall exceeding 96% mark.
Keywords: De-authentication, DoS, Intrusion Detection System, Machine Learning, Wi-Fi Security, WLAN, 802.11

I. INTRODUCTION

Wireless Local Area Networks (WLANs) [1] have seen a tremendous growth in the last few years. Thousands of wireless Access Points (APs) have been deployed across the world enabling the users to remain connected to the Internet while on the move. However, all of these advantages ignore the cost of security associated with it. An attacker needs to be there in the vicinity of the client to eavesdrop the wireless traffic. Pentest operating system like Kali, BackTrack comes pre-loaded with a large number of readymade tools to launch large number of attacks on Wi-Fi networks. IEEE provided Wired Equivalent Privacy (WEP) as its starting encryption technique for securing communication between Wi-Fi clients. However, many short comings were discovered in WEP's implementation which made WEP vulnerable to various attacks. The works in [2], [3] have demonstrated that WEP can be easily broken. The various shortcomings of WEP to provide robust encryption features led tothe development of the 802.11i standard which offered strong encryption schemes and also provided client authentication absent in WEP. All the encryption schemes of 802.11 standards like WEP, Wi-Fi Protected Access (WPA), and WPA2 encrypt only data frames. The management and control frames are crucial for establishment, maintenance and data exchange are always sent in an un-encrypted (clear-text) fashion. A majority of 802.11 DoS attacks exploit the un-encrypted nature of the control and management and [4].

In this article we focus on the De-DoS attack. A De-DoS attack is launched by bombarding client(s) with a huge number of spoofed de-authentication frames. As de-authentication frame(s) are management frames, they are sent in clear-text. Upon receiving ade-authentication frame(s) a client gets disconnected from the network. A De-DoS attack can be launched simultaneously on multiple Wi-Fi client(s) using minimal resources. Current approaches to handle De-DoS attack include encryption, up-gradation to newer standards, protocol modification etc. Encryption involves key management, key distribution, and certificate management which require additional software and hardware resources and adds to administrative overhead leading to increased costs. Up-gradation to newer standard is usually an expensive task and is not always possible due to the existence of legacy Wi-Fi networks. Protocol alteration often requires both software as well as hardware upgrades which increase deployment and running costs. 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 article, we proposed a machine learning (ML) based IDS for the detection of De-DoS attack in Wi-Fi networks which does not suffer from the limitations listed earlier. ML has found a lot of applications across various domains like 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. We have used various classes of classifier algorithms and evaluated their efficiency for detection of De-DoS attacks in Wi-Fi networks. Most of these classifiers have shown appreciable results. The idea behind the usage of the different algorithms enables an administrator, they choose the best algorithm that suits his/her network characteristics. The experimental results for detection rate and accuracy using the proposed ML based IDS exceed 96% mark which is exemplary.

The organization of our paper is as follows. In Section II we discuss the Wi-Fi basics along with De-DoS attack. We also list out the existing approaches to mitigate 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 results for recall (detection rate) and precision (accuracy) and for the proposed ML based IDSare elaborated in Section IV. Finally we conclude our paper in Section V.

II. BACKGROUND AND MOTIVATION

In this section, at first we look into the basic terminologies associated with Wi-Fi networks. Following that, we discuss the vulnerabilities associated with Control and Management frames in Wi-Fi networks. The De-DoS attack is detailed next. We also discuss the existing solutions to mitigate De-DoS attack and their disadvantages. 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 between Wi-Fi clients happen via the AP. A client needs to first authenticate and then associate with an AP in order to communicate with other Wi-Fi clients. A Wi-Fi client can be in any of the 3 states depicted in Fig. 1.

- 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.

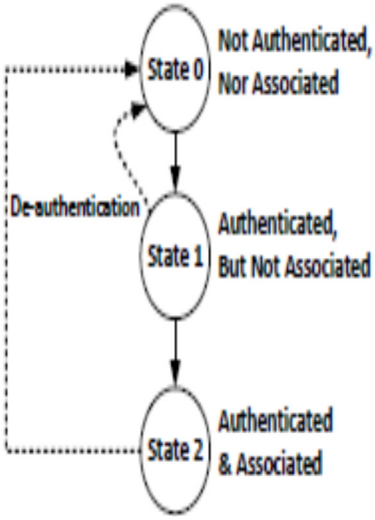

Fig. 1: Possible states of a Wi-Fi client.

It must be noted that on receiving a de-authentication frame, a client directly goes to State 0 irrespective of the state it is currently in (whether State 1 or State 2). So after receiving a de-authentication frame the client needs to re-authenticate and re-associate. Under De-DoS attack an attacker repeatedly sends spoofed de-authentication frame(s) in order to get the client disconnected. This breaks the ongoing client communication leading to Denial of Service for the client. An attacker can launch this attack on multiple clients simultaneously to increase the efficiency of De-DoS attack.

A. De-auth DoS Attack

As seen earlier, the 802.11 encryption schemes do not encrypt the management and control frames making them vulnerable to spoofing. The de-authentication frame is a management frame and is sent in clear-text. Clear-text frames guarantee quicker processing and very little computation for the AP. However, spoofing clear-text frames is trivial. As de-authentication frames are sent in clear-text, AP cannot verify the authenticity of such frames. As a result, the AP has to processes even spoofed de-authentication frame(s) thinking them as genuine de-auth frames. In a De-DoS attack an attacker barrages a client(s) with a large number of spoofed de-authentication frame(s). When the client(s) receive the spoofed deauthentication frame(s) it results in the termination of their existing connection. If the De-DoS attack is launched continuously for longer durations, the client(s) would be unable to maintain the connection with the Wi-Fi network. The 802.11 standard mentions that de-authentication are a notification and not a request.

De-authentication shall not be refused by either party [1]. When a client (AP) sends a de-authentication frame to an associated AP (client), the association ends. The attacker uses multiple approached which can be used to launch De-DoS attack. A few ways in which the attacker can launch De-DoS attack are listed below:

Spoofed AP to client De-authentication Frame: Here an attacker crafts a spoofed frame that appears to be directed from an AP to the client. The attacker sets the SRC MAC address to the AP's MAC address and the DST MAC address as client's MAC address. The client gets disconnected from the Wi-Fi network as soon as it processes the spoofed de-authentication frame assuming the frame coming from the legitimate AP as the attacker had spoofed the SRC MAC address of the AP.

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: The attacker sets the SRC MAC address to AP'sMAC address and the DST MAC address as broadcast MAC address (FF:FF:FF:FF:FF:FF).This is the most severe form of De-DoS attack and leads to disconnection of all the clients associated with the AP.

To launch the De-DoS attack an attacker can use tools like aircrack-ng suite [7] and scapy. The information required by the attacker is: MAC address of AP, client(s) MAC address, network name of the AP (SSID) and the channel number on which the AP is running. Tools like tcp dump, Wireshark, kismet, airodump-ng etc. readily provide this information.

B. Existing Solutions to mitigate De-DoS attack

In this sub-section, we look at the existing solutions proposed in the literature to mitigate De-DoSattacks.

1. Encryption based methods
   - Bellardo [4] suggests that authenticating all of the management frames prevents spoofing of these frames. Nguyen et al. [8] proposes a Letter-envelop protocol that establishes a secret key betweenthe AP and the client which is used for authenticating the de-authentication frame sent by the client. This approach is useful in preventing De-DoS attack but firmware upgrades are needed on both client and the AP which are often costly.

2. Protocol Modification and Up-gradation based methods
   - Bellardo [4] proposed another method to prevent De-DoS attack by delaying the effect of all management frames. If a de-authentication frame is received from some client and subsequently a data frame is also received from the same client, then the previous de-authentication frame(s) is not processed. This idea behind this is that a client sending de-auth frame does not send any other data to the AP before authentication and association again. So, if such a sequence is observed then there are high chances that the previous de-authentication frame(s) received is spoofed. However delaying the effect of all management frames may create association problems for roaming clients and may cause hand-off issues. Also this approach required firmware upgrades.

Upgrading to 802.11w standard - This standard [9] makes authentication of the de-authentication and disassociation frames mandatory. The authentication prevents spoofing thereby preventing the De-DoS attack. However, due to regency in proposed 802.11w standard, it is being used very sparingly. Switching to 802.11w standard also requires firmware upgrades on both client and AP.

3. Non Encryption Based Methods
   - Agrawal et al. [10] detect the De-DoS attack by setting a threshold on the number of de-authentication frame(s) received by a client. If for a client, more than the threshold numbers of de-authentication frame are seen, an alarm is raised indicating the occurrence of De-DoS attack. However, this threshold is static and is set by the administrator making the technique prone to misjudgment. An intelligent attacker can keep the de-auth frames below the statistical count.

4. Sequence Number based methods
   - Guo et al. [11], Xia et al. [12] and Anjum et al. [13] have suggested different schemes for detection of spoofing attacks based on the sequence number analysis. Sequence number is incremented by one in each Wi-Fi frame. If the previous frame number sent by the client is 'x' then the successive frame is sent with the sequence number 'x+1', 'x+2', 'x+3' and so on. If the next frame received from the client has a sequence number other than 'x+1', it is a spoofed frame as the actual sequence number must have been'x+1'. An intelligent attacker can forecast the sequence number in advance in order to escape detection, sending a frame with sequence number 'x+1'. The technique is based on the assumption that sending aframe with correct sequence number at the precise timing is often difficult if the numbers of frames to be sent are high.

To summarize, the disadvantages of the current approaches to detect and prevent the De-DoS attack are as follows:
- Requires modifications in 802.11 protocol stack to support authentication and encryption of frameswhich are currently non-authenticated.
- Patching AP and client software.
- Up-gradation to newer 802.11 standards like 802.11w.

From the above points we can conclude that an effective De-DoS attack detection technique is required to have the following features:
- The 802.11 protocol stack should not be altered.
- It must be easily deployable on new as well as legacy networks.
- Hardware costs if any should be minimum
- Should not depend on the client's underlying operating system, application and must not require any kind of patching of client software or installation of drivers etc.

- Should be a non-cryptographic based scheme as they have an added advantage of being light-weight in terms of processing and key management.

We now discuss our proposed ML based IDS that includes the features listed above and overcomes the disadvantages of the existing approaches.

III. PROPOSED ML BASED IDS

The experimental setup for the proposed ML based IDS and its architecture is depicted in Figs. 2. The IDS is placed near the AP to ensure that the frames to and from the AP are captured correctly. In this section, we look into the vital components of the proposed ML based IDS, process of training and testing data set generation and the motivation behind the feature selection of the ML based IDS. The feature selection is always a critical part of any ML based application. Following that, a briefdescription of the various classifiers used for the proposed ML based IDS has been described.

A. ML Based IDS Components

The ML based IDS primarily consists of two main components: Wi-Fi Frames Sniffer and De-auth DoS Detector module, which are explained next.

1. Wi-Fi Frames Sniffer

The Wi-Fi Frames Sniffer takes as input the raw Wi-Fi frames traveling in the network. It ignores frames belonging to other APs and forwards those frames to the De-auth DoS Detector which contain the MAC address of the monitored AP. Frames to other APs are dropped.

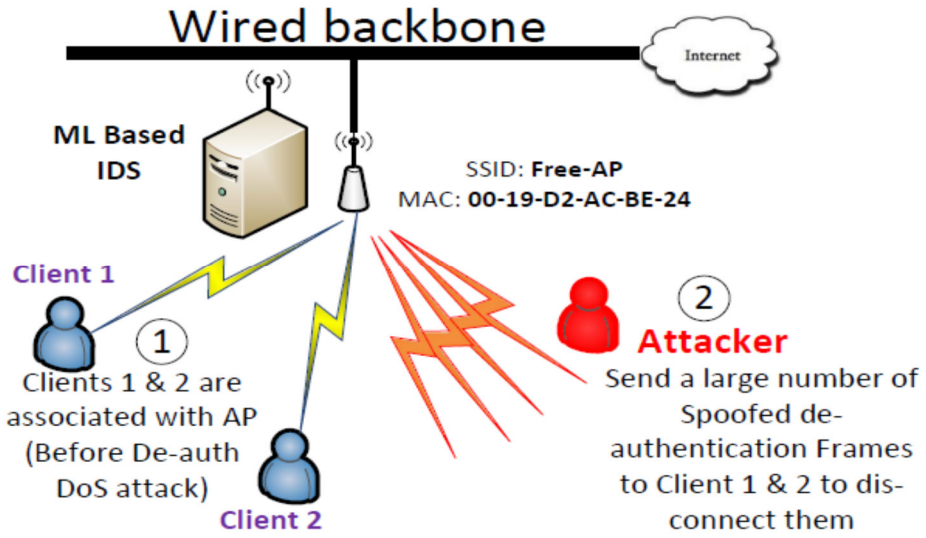

Fig. 2: Experimental Setup

2. De-auth DoS Detector

The De-auth DoS Detector module is initially trained using the Training Data which is generated offline. 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 in order to identify the occurrence of the De-DoS attack and deployed on a live network. The De-auth DoS Detector analyzes the frames traveling in a live network obtained from the Wi-Fi Frame Sniffer. 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 De-DoS attack has indeed occurred, the IDS generate an alarm indicating De-DoS attack.

B. Testing and Training Dataset Generation

The De-auth DoS Detector module is trained using Training Data which is generated in-house. Since there is no public data set is available for De-DoS attack in Wi-Fi networks, we have created an in-house data set in the lab for the De-DoS attack. We designated 5 Wi-Fi nodes (2 laptops, 2 smart-phones and 1 tablet equipped with Wi-Fi connectivity) as clients. For the attacker machine, we chose a laptop with x64 bit operating system installed UBUNTU Linux operating system contains the aircrack-ng suite which is used to launch De-DoS attack. Aircrack-ng suite is a comprehensive suite for testing and penetrating Wi-Fi networks.

All the designated clients and the attacker are associated with the same AP for simplicity. A dedicated machine is used for sniffing the frame exchange using Wireshark. This ensures that maximum frames are captured by the dedicated device. The traces collected by Wireshark helps to analyze the behavior of clients under normal and de-auth attack conditions. The clients are asked to perform routine Internet activities like downloading, surfing, watch live streams etc. while the attacker selects a random time interval and chooses a set of client(s) and launches De-DoS attack on them by injecting spoofed de-auth frames. We have assumed that the attacker launches all three

form of De-DoS attack as explained in the earlier section. The data set is collected over a period of 5 hours. For training purposes we use 75% ofthe data set generated while the remaining 25% is used for testing purposes.

C. Feature Selection for the ML based IDS

For feature selection of the proposed ML based IDS, we analyze the frame exchange characteristics captured by Wireshark during normal and De-DoS attack situations. Using this information we have listed down 7 features in decreasing order of their significance as depicted in Table I. The significance is determined by information gain test which evaluates the importance of an attribute. WEKA was used for getting the results of test. The attribute having lower (higher) weights have lesser (higher) significance role in De-DoS attack detection.

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.

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: It has been experimentally observed that under De-DoS attack, as the clientis abruptly disconnected, it tries to immediately re-authenticate itself with the same AP so that its communication can begin again. On the other hand, under normal circumstances it has been observed that when a client genuinely disconnects from an AP, it rarely re-connects to it as immediately as it does under de-auth dos attack. The Time_Difference feature here is the difference in time-stamp when the client gets disconnected to the time it gets re-authenticated with the same AP. For example, if the client gets disconnected at time T1 and gets re-authenticated at time T2 the value of Time_Difference is T2 - T1. Under De-DoS attack this value is quite small. If the client never re-authenticates again, the value of Time_Difference is taken as infinity.

2. #Deauthentication Frames: The attacker launches De-DoS attack by sending a large number of de-authentication frame(s) towards a set of targeted client(s). In order to increase the efficiency of the De-DoS attack the attacker often sends multiple number of de-authentication frame(s) to a single client making it almost certain that the client shall disconnect. So the number of De-authentication Frames feature is taken into account. Larger the number of de-authentication frame(s) for a client, more are the chances of De-DoS attack in the network.

3. # Frame_Exchange: This feature keeps the count of the number of frame exchanges made by the individual client(s) per session (from the time it authenticates till it disconnects). If the same client re-associates with the AP, its initial Frame_Exchange value is set to 0. If the attacker repeatedly launches De-DoS attack on a set of clients, Frame_Exchange value for those client(s) tends to be quite low. Due to frequent disconnection as a result of De-DoS attack, the length of per session is small so, the amountof frame exchange in a De-DoS attack scenario differs significantly as compared to normal scenarios (where usually appreciable numbers of frames are exchanged per session). Hence this feature is included.

4. # Authentication Frames: As explained earlier a client if disconnected via the De-DoS attack usually tries to re-authenticate itself with the same AP quickly. This features counts the number of authentication frames exchanged after the client gets disconnected and tries to re-authenticate. Under normal circumstances, the client if disconnects and does not connect back resulting in the value to be 1set to 0. However under De-DoS attack the client tries to re-connect to the same AP increasing the count of this feature making its inclusion necessary.

5. # TCP Frames: This feature keeps the count of the number of TCP frames exchanged by individual clients. The number of TCP frames exchanged under normal circumstances is quite large as majority ofthe traffic exchange is using TCP. However under De-DoS attack this number reduces substantially as the clients are automatically disconnected from the AP indicating possible attack activity.

6. # Association Frames: Similar to Authentication Frames

7. # UDP Frames: Similar to TCP frames.

D. Classifier Design and Selection

The success of ML based IDS depends largely on the classifier chosen. The task of a classifier is to meticulously differentiate between normal and attack frames. As classifiers have varying features, their performance also changes. In this section, we first describe few classification algorithms that are used in our proposed scheme. Each classifier has its own advantages and disadvantages with respect to parameters like accuracy, speed, and detection rate. From the perspective of IDS precision and recall should be as high as possible. An administrator can choose

amongst various techniques discussed below based on his requirements and network characteristics. Data classification involves a two step procedure.

- Step 1: Here the classification algorithm builds a classifier using the training data.
- Step 2: In the second step, the model built in Step 1 is used for classification and its performance is analyzed using test data. We outline a few classification techniques that we have used for our ML based IDS [6].

1) Bayesian Networks: Bayesian networks (BNs) or Bayes Nets are probabilistic graphical models ABN consists of an notated directed acyclic graph where each node serves as a random variable, whereas the edges between nodes depicts the probabilistic dependencies among the corresponding random variables. These conditional dependencies are estimated using known statistical and computational methods. The links between the nodes in BNs can be explained as association or correlation between random variables.

2) SVM: Support Vector Machines or SVMs are kernel based classifiers. SVMs are very much suitable in cases where the data has exactly two classes (our data too has two classes: attack and normal). A SVM classifies data by searching the best hyperplane that splits all data points of one class from the other. The best hyperplane for an SVM is the one which has the largest margin between the two classes under consideration.

3) RIDOR: Ripple-Down Rule Learner or RIDOR is a rule based classifier. Based on the training data, RIDOR forms a set of rules from the data. First, it generates a default rule and then the exceptions for the default rule with the least (weighted) error rate. The process is repeated till the final leaf is reached which has only one default class and no exceptions.

4) C4.5/J48: C4.5 classifier builds decision trees from a set of training data in the same way as ID3 classification algorithm, using the concept of information entropy. The training data consists of a set of already classified samples. Each sample is identified using a k-dimensional vector that represents the attributes or features of the sample as well as the class to which the sample belongs. At each node of the tree, C4.5 chooses the attribute of the data that most effectively splits its set of samples into subsets enriched in one class or the other. The splitting criterion is based on the normalized information gain. The attribute having the highest normalized information gain is chosen to make the decision. The C4.5 algorithm is then repeated on the smaller sub lists. In the next section, we will look into the experimental setup and the results obtained using the proposed ML based IDS.

IV. EXPERIMENTAL SETUP AND RESULTS

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. 2. Attacker machine is loaded with aircrack-ng suite which 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) getdisconnected resulting in DoS.

A. Precision and Recall of proposed method

The metrics used for measuring the performance of IDS are accuracy and detection rate. Accuracy is the proportion of the total number of predictions that are correct. It is determined using the equation:

$$\textbf{Precision} = TP/(TP+FP)$$

Detection Rate is defined as the number of attacks detected by the IDS to the total number of attacks actually present.

$$\textbf{Recall} = TP/(TP+FN)$$

Here, TP is True Positive, FP is False Positive, and FN is False Negative. A TP arises when a real attack and is declared as attack by the IDS. A FP arises when IDS marks a normal activity as attack activity. A 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 probability based (NaiveBayesand BayesNet), decision tree based (C4.5/J48), rule based (RIDOR) and kernel based classifiers (SVM).

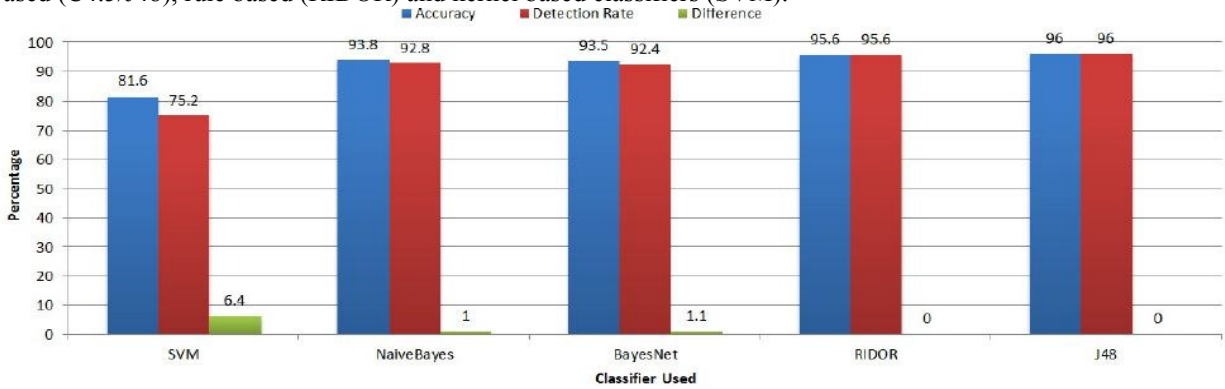

Fig. 3: Accuracy & Detection Rate of the Classifiers Used

We have used the WEKA tool for analysis purposes as all these classifiers are already built into WEKA.Fig. 3 shows the accuracy and detection rate of the various ML classifiers used for the proposed IDS todetect the de-auth DoS attack. It can be observed that quite promising results have been delivered by the various classifiers used.

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

Classifier	Accuracy (Precision)	Detection Rate (Recall)	F-Measure	ROC Area
NaiveBayes	0.854	0.704	0.715	0.901
BayesNet	0.938	0.928	0.93	0.984
SVM	0.816	0.752	0.677	0.569
Ridor	0.956	0.956	0.956	0.944
J48	0.96	0.96	0.96	0.966

The objective of choosing the different classifiers amongst different classes is to enable the network administrator the freedom to choose the most preferred classification algorithm, basedon the network characteristics like the number of clients, encryption used, data usage etc. Naive Bayes classifier which is a probabilistic based classifier has a precision (93.8%) and recall (92.8%) as compared to other classifiers. Bayes Net which is another probabilistic classifier performs significantly better as compared to Naive Bayes. The precision and recall for BayesNet is 93.5% and 92.4%, respectively.

BayesNet performs better than NaiveBayes as it does not assume every feature to be independent of others as assumed by NaiveBayes. For example, the quick re-authentication of a client after the De-DoS attack cannot be considered as an independent event. The quick re-authentication usually occurs due to the De-DoS attack (showcasing that quick re-authentication depends on De-DoS attack). NaiveBayes on the other hand considers all the events as independent of one another and does not assume any sort of dependence between various events. Support Vector Machines (SVM) has the lowest precision rate of 81.6% and its recall is just 75.2%. A precision of 81.6% implies that SVM does not report 18 attacks out of every 100 De-DoS attacks launched.

This is unacceptable from an IDS perspective. RIDOR is a rule based classifier having precision and recall rate of 95.6% which is better than SVM and both the probabilistic based classifiers used. However the issues with rule based classifier is that it often depends on the expert opinion. Different experts may have contrasting opinion regarding the same set of rules which affects the precision and recall values. J48 is a decision tree based classifier improves both in terms of precision and recall as compared to RIDOR. J48 is an open source Java implementation of the C4.5 implemented in WEKA. The precision and recall for J48 stands at 96%. With both detection rate and accuracy and detection rate more than 96%, J48 certainly is the best choice for the IDS among various classifications algorithms tested.

V. CONCLUSION AND FUTURE WORK

In this article we have proposed a novel ML based Intrusion Detection System for De-DoS attack recognition in 802.11 Wi-Fi networks. The proposed ML based IDS method discovers the De-DoS attack with high detection rate and low false positive rate. Many WEKA classifiers like BayesNet, NaiveBayes, SVM, RIDOR and J48 give promising results. The proposed IDS utilize the J48 classifier as both the precision and recall exceeds 96% which is quite good. Another major advantage of the machine learning based IDS is that it doesn't require use of any encryption algorithms, protocol modifications, or firmware upgrades. Besides this, the proposed work can be applied on legacy as well as present-day systems.

REFERENCES

[1] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2007 (Revision of IEEEStd 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 NetworkSecurity, 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 Securityand 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 12thConference 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 IEEEInternational 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 802.11networks 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/disassociationattacks on 802.11 networks," in Computer Communications and Networks, 2008. ICCCN'08. Proceedings of 17th InternationalConference on. IEEE, 2008, pp. 1–6.

[9] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Protected ManagementFrames. IEEE Std. 802.11w-2009, September 2009."

[10] M. Agarwal, S. Biswas, and S. Nandi, "Detection of De-authentication Denial of Service attack in 802.11 networks," in Annual IEEEIndia Conference (INDICON) , Dec 2013, pp. 1–6.

[11] F. Guo and T.-c. Chiueh, "Sequence number-based MAC address spoof detection," in Proceedings of the 8th International Conferenceon Recent Advances in Intrusion Detection, ser. RAID'05, 2006, pp. 309–329.

[12] 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.

[13] F. Anjum, S. Das, P. Gopalakrishnan, L. Kant, and B. Kim, "Security in an insecure WLAN network," in 2005 International Conferenceon Wireless Networks, Communications and Mobile Computing, 2005, pp. 292–297.