Detection of The De-Authentication Denial of Service Attack in 802.11 Wireless networks

Vipin Poddar
Suresh Gyan Vihar School of
Engineering and Technolgy
Jaipur, Rajasthan

Mrs. Anita Chopra
Assistant Professor
Suresh Gyan Vihar School of
Engineering and technology
Jaipur, Rajasthan

Abstract—Wi-Fi wireless networks are prone to a very large number of Denial of Service (DoS) attacks due to the vulnerabilities at the MAC layer of 802.11 wireless protocol systems. In this paper we are mainly focussing on the De-authentication DoS attack in Wi-Fi wireless networks. The impact of the De-authentication (DoS) attack is very severe as the person who gets affected gets disconnected from the network. This Dos attack can be launched and removed easily using minimum resources. In this paper we propose an Intrusion Detection System (IDS) along with the Intrusion Prevention System (IPS) that detects the de-authentication DoS attack in a Wi-Fi wireless network and also helps the victim station (STA) to recoverse it swiftly from the attack. Our proposed IDS is lightweight and detects the attack with high accuracy & low false positive rate. Our technique can be easily deployed on open as well as encrypted networks**.**

Index Terms— to minimize the Denial of service attack in wireless networks.

1 INTRODUCTION

IEEE 802.11 [1] based Wireless LAN (WLAN) is being used extensively now-a-days. From corporates to coffee shops, from university to malls, users are hooked to Wi-Fi network while on the move. However, the benefits Wi-Fi network come at the cost of security. The designers of Wi-Fi standards concentrated more on providing the ease of network access, transparent roaming, device compatibility, thereby sacrificing security. The initial encryption technique proposed in the standard was Wired Equivalent Privacy (WEP) which was proven inadequate and could easily be broken [2]. The 802.11i standard released subsequently provided the users with Wi-Fi Protected Access (WPA) & WPA2 as the standard encryption techniques. Though WPA & WPA2 were robust than WEP, it only protected the data frames. The management and control frames remained un-encrypted. A prominent number of Wi-Fi attacks exploit the open and un-authenticated nature of the management and control frames. In this paper our focus in on the de-authentication DoS attack.

A. De-authentication DoS Attack

In a de-authentication DoS attack the attacker infuses a large amount of de-authentication frame(s) in the network. When the clients receive the de-authentication frame(s) they get disconnected from the network. If the attack is prolonged, the users would be unable to maintain the connection with the Wi-Fi network. An attacker can launch de-authentication DoS attack in various ways. Prominent among these are: · The attacker can construct spoofed de-authentication frame(s) and set the source MAC address as the victim STA's MAC address and destination MAC address as the AP's MAC address. Thus upon receipt of the frame, the AP thinks that a genuine user wishes to leave the network and disconnects the user from the network. The attacker can craft spoofed de-authentication frame(s) and set the source MAC address as the AP's MAC address and destination MAC address as victim STA's MAC address and inject these spoofed frames into the network. These spoofed frames upon reaching the users terminal disconnect the user from the network. · The attacker can craft a packet with source MAC address of the AP and destination as broadcast MAC address (FF:FF:FF:FF:FF:FF). This disconnects all the users associated with the AP. The impact of the broadcast de-authentication DoS attack is severe and leads to de-authentication of all users connected with the target AP in the network. The attacker can use a variety of available tools like *aircrack-ng* suite [3], file2air [4] etc. to launch the deauthentication DoS attack. All that the attacker needs to knowis the target client(s) MAC address, BSSID (MAC address of access point), SSID of the network and the channel number on which it is running. This information can be easily obtainedusing tools like Wireshark [5], tcpdump etc.

2. RELATED WORK AND MOTIVATION

Since the induction of the IEEE 802.11i standard in 2004, WLANs have been able to provide robust authentication of Wi-Fi devices and encryption of the communication traffic.

The802.11i standard uses the IEEE 802.1X Extensible Authentication Protocol (EAP) to ensure that only authorized devices are allowed to access the Wi-Fi network. It also uses the Advanced Encryption Standard (AES) to guarantee confidentiality and integrity of the data communications between authenticated devices. The drawback of 802.11i standard is that it only encrypts the data frames, the management and control frames are still left unencrypted. Management and control frames are vital frames that are required for establishing and maintaining connections. De-authentication frame is a management frame and hence left unencrypted. So if a network does not implement the 802.11w standard, there is no way of checking the authenticity of the de-authentication frame(s) received.

The 802.11w standard came in the year 2009, and hence a very small fraction of Wi-Fi networks employ this standard. There exists millions of legacy Wi-Fi networks which do not implement this standard and have no option but to terminate the client connection upon receiving a de-authentication frame(s).

The 802.11 standard specifies that de-authentication is a notification, not a request. De-authentication shall not be refused by either party. When a user(AP) sends a de-authentication frame to an associated AP(STA), the association ends. The attacker can also exploit the other management and control frames to launch a myriad of attacks, but in this work

978-1-4799-2275-8/13/$31.00 ©2013 IEEE
2013 Annual IEEE India Conference (INDICON)

we concentrate on how an attacker can exploiting the deauthentication frame(s) to launch the de-authentication DoS attack. On similar lines, an attacker can also launch a Disassociation DoS. Dis-association DoS has relatively low impact as compared to de-authentication DoS attack since in the latter the victim needs to re-authenticate as well as re-associate, whereas in the former the victim needs to only re-associate.

Wireless DoS can be performed at physical as well as MAC layer. At the physical layer jammers are used to disruptor prevent communication between stations. At the MAC layer media access vulnerabilities and the openness of the management and control frames are exploited to launch DoS attacks. Some of the solutions proposed in the literature to tackle the de-authentication DoS attack are listed below. · Bellardo [6] suggests modifying the authentication framework and authenticating all management frames. This approach can help prevent the de-authentication DoS attack but requires firmware upgrades on both the client and the AP. Adding authentication to each management frame would incur additional cost on both client as well as AP. Since authentication is an expensive process, authenticating every management message would in-turn quickly drain the batteries of handheld devices like smart-phones, PDAs etc. Bellardo also suggests another approach in which he proposes delaying the effect of management frames. If a de-authentication frame is received from a victim STA and subsequently a data frame is received from the same victim STA the previous de-authentication frame(s) is not honoured. However delaying the effect of all management frames may create association problems for roaming clients and may cause handoff issues. · Edgar Cardenas [7] proposes the use of Reverse Address Resolution Protocol (RARP) to detect spoofed frames. However an intelligent attacker can manipulate the IP address of the client to circumvent the RARP technique. Also in the case when multiple IP address are assigned to same NIC the solution fails[8], [9]. · Guo et al. [10], Wright[11], Mar et al. [12], Xia et al. [13] and Anjum et al. [14] have suggested various schemes for detection of spoofing attacks based on the sequence number analysis. However a clever attacker can predictthe sequence number in advance to escape detection. Also with the advent of attack cards it is possible for an attacker to send a frame with a desired sequence number. · Upgrading to 802.11w standard - This standard [15] authenticates the de-authentication and disassociation frames. The authentication prevents spoofing and hence can prevent the de-authentication DoS attack. However 802.11w is a very recent standard released in 2009. Upgrading all millions of Wi-Fi devices to support the 802.11w is a difficult task. · Nguyen et al. [16] have proposed a Letter-envelop protocol to prevent the de-authentication DoS attack . In their approach the client and AP share a secret key which is used for authenticating the de-authentication frame and Disassociation frames. This helps in alleviating the attack and does not incur too much load on either the client or the AP. However this method also involves firmware upgrades on both client and AP and hence proves to be costly. · A centralized framework like 802.1x can help prevent a variety of attacks including de-authentication DoS attack, however such centralised solutions suffer from single point of failure [17]. If the authentication server is compromised all the clients belonging to the network can be compromised. To summarize the drawbacks of the current approaches to detect or prevent the de-authentication DoS attack are listed as follows:

1) Expensive Deployment.
2) Requires modification in 802.11 protocol to support Authen -tication and Encryption of frames which are currently non-authenticated.
3) Patching client software.
4) Requires proprietary hardware.
5) Upgradation to newer standards.

From the above summary it is clear that a scheme to detect the de-authentication DoS attack is required having the following features.

- No modification of 802.11 protocol.
- Easy deployment to legacy as well as new networks.
- Hardware costs should not be exorbitant.
- Should not require patching of underlying operating system or installation of new software.

- Should be able to recover victim STA from the attack swiftly.

The summary of our contributions are:

1) We propose an IDS & IPS based approach that not only helps in detecting the existence of de-authentication DoS attack in a Wi-Fi network but also helps the victim stations to recover from the attack quickly. The developed IDS complies with the 802.11 standard. No protocol modification is necessary. We exploit the fundamental aspects and properties of the 802.11 protocol to detect the attack.

2) The only hardware requirement is a sensor capable of sniffing the wireless data. This ensures the technique is economical and cen be easily deployed.

3. PROPOSED SCHEME

A. Architecture

The architecture of the IDS is shown in Figure 1. The IDS is a wireless sniffer which monitors the incoming and outgoing network traffic in promiscuous mode. For every AP that needs to be protected, we use the setup shown in Figure 1. For each STA associated with the AP, the IDS keeps a track of the following parameters. · Moving average of the number of packet(s) sent/received by the STA. · Average throughput of each associated STA. · Number of de-authentication frames sent/received. Besides this the IDS maintain the following global parameters. · Rolling average of the number of de-authentication frame(s) seen in the network. · Average throughput of the network. The IDS is a sniffer that sniffs the wireless data packets and transfers them to the Analysis Engine. The Analysis Engine filters out unwanted packets from the received frames and based on various parameters like network throughput, STA throughput, de-authentication frame(s) received by a STA determines whether de-authentication DoS attack has occurred. The Analysis Engine also stores the vital information about the network statistics obtained in the Database(DB). If the Analysis engine infers that a de-authentication DoS attack has indeed occurred, it informs the IPS module about the same. If the de-authentication DoS attack is still in progress, the IPS module directs the AP to ignore the de-authentication frame(s) for the victim client. This helps the victim STA to recover quickly from the attack. In any de-authentication DoS attack

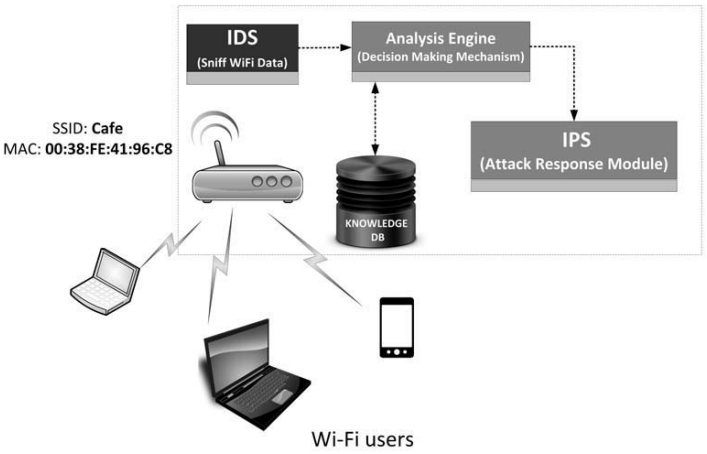


Fig. 1: IDS Architecture.

the attacker inundates the target client(s) with spoofed deauthentication frame(s). The consequence of this leads to the following observation:

- A stream of de-authentication frame(s) against targeted client(s).
- Radical fall in the throughput of the targeted client(s).

Our IDS makes use of these two characteristics of a deauthentication

DoS attack to detect its occurrence in the Wi- Fi network. We analyzed the SIGCOMM traces and othe 802.11 datasets obtained from crawdad website [18] to evaluate various characteristics of a de-authentication frame(s). We also conducted extensive in-house experiments to study the behaviour of the clients under normal and attack conditions. We plot the number of de-authentication frame(s) sent by the clients to the AP under normal network conditions. As seen from Figure 2, almost 96% of the time, the client needs at max two deauthentication frame(s) to get disconnected from the Wi-Fi network. In fact 88% of the clients get disconnected with a single deathentication frame. Recent Wi-Fi hardware

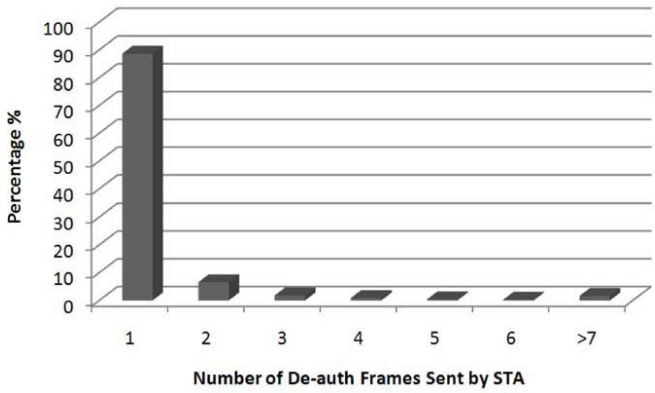


Fig. 2: Percentage distribution of the Number of

de-authentication frame(s) sent by clients. possess the ability to automatically re-connect to the same AP if the connection is abruptly terminated in the midst of an ongoing communication. So unless the attacker sustainsthe attack for an appreciable time, there are high chances that most of the clients recover automatically from the attack and re-connect to the same AP.

From the Figure 3 it can be seen that the throughput of the client severely degrades during the attack. After the attack recedes, eventually some clients recover whereas some remain in the dis-connected state. The mobile stations remain in dis-connected state and they had to be manually re-connected to the Wi-Fi network. Mobile stations do not recover automatically from the impact of the deauthentication DoS attack presumably because of their limited
processing capability. In the following section we discuss our approach in detection the de-authentication DoS attack and describe an algorithm for the same.

B. Methodology

In our proposed methodology, the IDS keeps track of the de-authentication frame(s) sent/received by each STA, through put for each STA, overall count of de-authentication frame(s) captured and throughput of the network. Depending on the needs of the network, the administrator can set a dynamic threshold or a static threshold. In our experiments we have set the threshold for the IDS to 5 which gives an accuracy rate of above 99%. Different values of threshold gives varying accuracy and detection rates as shown in Table I. We also modify the AP drivers so that it ignores the de-authentication frame(s) received for those stations from which it has received more than *threshold* number of de-authentication frame(s). We used the open source Madwifi drivers[19] available for Linux for modification and testing purposes. While the deauthentication DoS attack is in progress the throughput of the client degrades severely. The client has no option but the switch to a different Wi-Fi network. In case only one hotspot was available, the client is rendered helpless till the attack subsides. In this approach, once the IDS detects that a particular STA is under de-authentication DoS attack, and if the de-authentication counter for the STA is still increasing, the IDS ignores all the future de-authentication frame(s) coming from the victim STA towards the AP. As seen in the Figure 3, the user's throughput is degraded severely during the attack interval from 4 - 12 seconds. After the attack stops, all stations except the mobile stations (Apple iPhone 5 & Micromax A110) recover automatically. Figure 4 shows how our proposed approach helps stations to recover quickly from the attack. As against in Figure 3 where the stations recovered after the attack stopped, all stations except Apple iPhone 5 and the Micromax A110 Canvas recovered while the attack was in progress. The limited computing capability of the mobile stations must be the primary reason behind the inability of mobile stations to recover. The stations recovered around 10^{th} second while the attack was in progress till the 12^{th} second. Had the attack duration been longer, the speedy recovery of stations enables to overcome the de-authentication DoS attack and re-connect to the AP. However it could happen that while the attack is in progress, a victim STA may send a genuine de-authentication frame to get dis-connected from the current AP and switch to another AP. Since the AP is dropping the de-authentication frame(s) for the victim STA, even genuine de-authentication frame(s) would not be honoured. This would keep the association of the victim STA intact with the AP.

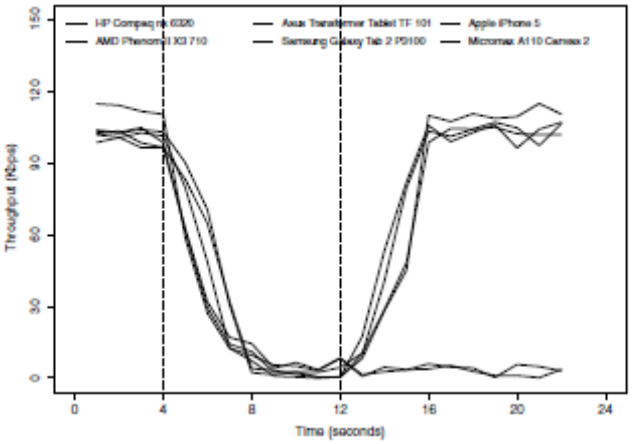
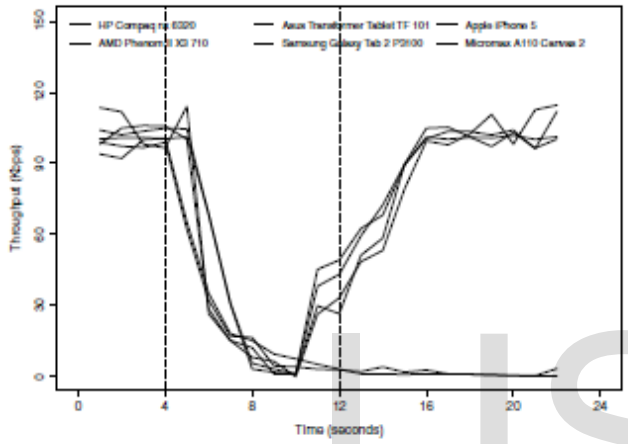


Fig. 3: Impact of De-authentication DoS attack on clients

However the victim STA would retry until the retry limit for the frame is reached and consequently upon reaching the retry limit, the victim STA discards the de-authentication frame(s) thinking the AP is not present in the network and the connection terminates. The proposed method is illustrated in Algorithm 1 and is explained below. As shown, the IDS sniffs the wireless packets pertaining to the AP being monitored (line 1). The IDS passes this information to the Analysis Engine. The Analysis Engine observes the packet and stores crucial information required to detect the de-authentication DoS attack into the DB (line 2). For each and every STA associated with the AP, the IDS does the following tasks and checks. If the number of de-authentication frame(s) received for a STA is within the threshold this situation is considered as normal and the deauthentication count for the STA and the de-authentication frame(s) count of the network is incremented (lines 4-6). In case the IDS receive broadcast de-authentication frame(s), it increments the counter of every associated STA. If the number of de-authentication frame(s) received for a STA is more than the threshold but the throughput drop is less than 50%, the IDS still consider this situation as normal. This is because in de-authentication DoS attack the throughput almost drops to zero and the client disconnects. In this case since the user is still connected to network, it might have been the case
that the packet was malformed and hence no impact was observed on the user. If the de-authentication frame(s) still continue for the victim STA beyond the threshold, the IDS ignores the frames. However the IDS does not update the deauthentication count for the STA(lines 8-11). The reason for not updating is that under normal circumstances, such amounts of de-authentication frame(s) are not observed. Modifying the counts will increase the de-authentication count average and

may result is false positives. If the number of de-authentication frame(s) received for a STA is more than the threshold and throughput drop for the victim STA is more than 50%, it is expected that the de-authentication DoS attack has occurred. The count of de-authentication frame(s) for the victim STA remains under observation. If the count still increases, it implies that the attacker continues the de-authentication DoS attack over extended period of time. This results in severe degradation of the throughput of the victim STA. If the victim STA still receives de-authentication frame(s) after the attack is ascertained, all the de-authentication frame(s) coming from



the victim STA are dropped (line 17). This ensures that the victim STA is able to recover quickly even if the attack is still on. This can be seen from Figure 4 where the stations recover quickly as compared to the scenario where shown in Figure 3 where the stations do not recover until the attack stops. If none of the above conditions are satisfied, the network is in normal condition. The IDS continues to collect useful statistics for associated STA and the network (line 17-18).

4. EXPERIMENTAL SETUP

Our network setup consists of a Cisco Linksys AP with SSID "Cafe" along with an IDS infrastructure placed as shown in Figure 5. The IDS is placed in vicinity to the AP to ensure that it captures maximum packets coming towards or leaving the AP. The attacker STA is configured with BackTrack5r3 [17]. The attacker uses the *aircrack-ng* suite[3] to launch the de-authentication DoS attack. Aircrack-ng suite is available as a standalone package or is pre-installed in most of penetration OS based on Linux. Our strategy focuses on inundating the victim station(s) with large number of unicast de-authentication frames. The attacker also makes use of broadcast de-authentication frame(s) to launch the de-authentication DoS attack on all the clients associated with the victim AP. The generic command used to inject a de-authentication frame in the network using aircrack-ng suite is:

```
aireplay-ng-0n-aMAC-OF-AP-c
MAC-OF-Victim-CLient wlan0
```

Where:

- 0 - Inject De-authentication Frame(s).
- n - Number of de-authentication frames to inject.
- a [MAC] - MAC address of the access point.
- c [MAC] - MAC address of the client to de-authenticate.
- wlan0 - Interface name

We also launched the attack using custom built Python scripts with the help of scapy. Scapy is a powerful interactive packet manipulation program that can craft and send packet of various different protocols. The attacker can employ various strategies to launch the de-authentication DoS attack. We assume that the goal of the attacker is to cause maximum damage to the victim STA. Hence the attacker targets those STA that continuously exchange data with the AP. The attacker can also target those STA which occasionally exchange data with the AP, however

Algorithm 1: DETECTION OF DE-AUTHENTICATION ATTACK & RECOVERY

Input: 802.11 Frames.

Output: Occurrence of De-authentication attack & Recovery it.

1. Collect Frames pertaining to the monitored AP using the frames.
2. Pass the collected information from the IDS to the Analysis Engine. Analysis Engine investigates the vital information regarding the frames. The Analysis Engine stores decisive information regarding the frames in the Database (DB).
3. **for** *Every STA associated to the AP* **do**
4. **if** *# of de-authentication Frames received < Threshold* **then**
5. Update the de-authentication count for the STA.;
6. Update the rolling average de-authentication count for the network. ;
7. **else if** *# of de-authentication Frames received ≥ Threshold & Throughput drop < 50%* **then**
8. Ignore the received de-authentication Frames for the STA ;
9. Do NOT Update the de-authentication count for the STA;
10. Do NOT Update the rolling average de-authentication count for the network ;
11. **else if** *# of de-authentication Frames received ≥ Threshold & Throughput drop ≥ 50%* **then**
12. Raise alarm "**De-authentication Attack**".;
13. Do NOT Update the de-authentication count for the STA.;
14. Do NOT Update the rolling average de-authentication count for the network. ;
15. Ignore the received de-authentication Frames for the STA ;

16. **Else**
17. Continue analysis of network frames by the IDS.;
18. Store the following information regarding STA: average throughput of STA, # of De-authentication frames receive Global count of the De-authentication frames received. ;

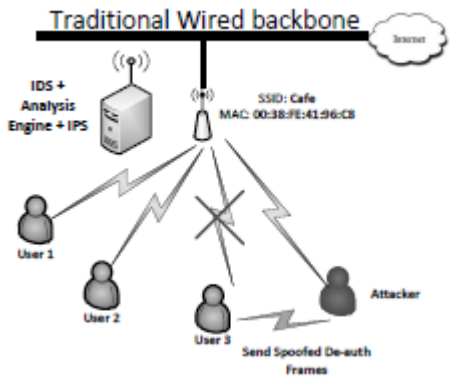


Fig. 5: Experimental Setup.

it would dampen the effect of the attack. Irrespective of the nature of victim chosen by the attacker, our detection methodology successfully detects the de-authentication DoS attack. To generate traffic and measure network throughput we used the iperf utility [18].

A. Test Procedure

The test procedure was consisted of the following steps repeated in a loop: Continuous monitoring of the network traffic for analysis and detection of de-authentication DoS attack.

- 4 Unicast de-authentication frame(s) per second directed to the target STA.
- 4 Broadcast de-authentication frame(s) per second directed from AP to STAs.

The de-authentication attack is launched for a period of 8 seconds between the time interval of 4 – 12 seconds as shown by dotted lines between these intervals in the Figure 3 and Figure 4. Our test bed consisted of the following devices. We used the original NIC shipped with each of the configuration.

- · HP Compaq nx 6320 with Windows 7.
- AMD Phenom II X3 710 Processor with Netgear Wi-Fi USB card & Ubuntu 12.04.
- Asus Transformer Tablet TF 101 with Android v4.0 Ice Cream Sandwich OS.
- Samsung Galaxy Tab 2 P3100 with Android v4.1 (Jelly Bean) OS.
- Apple iPhone 5 with iOS 6.
- Micromax A110 Canvas 2 with Android v4.1 (Jelly Bean) OS.

5. RESULTS AND DISCUSSION

A. Detection Rate and Accuracy

Table I illustrates the detection rate and the accuracy for different threshold values of the number of de-authentication frame(s) received for a STA. We can infer from the table that-with an increase in the threshold, the accuracy increases but the detection rate falls. This is because, if the attacker is able to successfully launch the attack with less than threshold number of packets, he would be able to evade detection. The accuracy increases with the rise in threshold values, since larger threshold implies a large amount of de-authentication frame(s) injected into the network, which is a clear indication of the eauthentication, DoS attack. On the other hand, the lower value of threshold can quickly detect de-authentication DoS attack, but would generate small amounts of false positives. This can be deduced from the accuracy results for the small threshold values. The detection rate is never 100% since it is possible for a victim STA to get dis-connected from the network even if the attacker injects one spoofed de-authentication frame for the victim STA. Also in normal network conditions, the clients require at least one frame to dis-connect from the network. Hence those de-authentication DoS attack that are launched using a single de-authentication frame are never detected, since setting a threshold of 1 is impractical and would generate a large amount of false positives. As a result those de-authentication DoS attack that are caused due to a single de-authentication frame are never detected and consequently the detection rate remains below 100%.

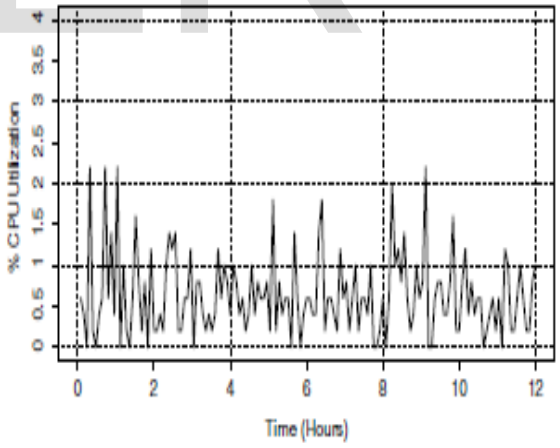


Fig. 6: CPU Utilization of IDS over 12 Hours

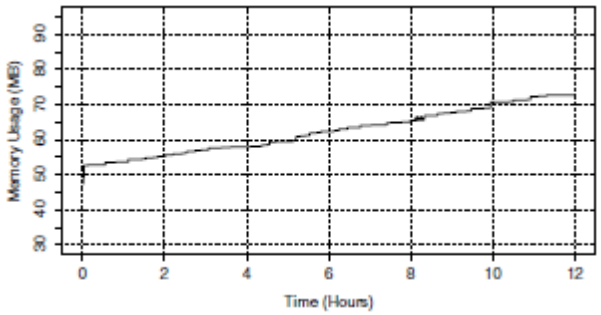


Fig. 7: Memory Utilization of IDS over 12 Hours

Threshold	Number of attacks launched	Detection Rate(%)	Accuracy (%)
2	2700	98.42	93.43
3	2700	97.15	96.22
4	2700	96.54	98.14
5	2700	95.25	99.43
6	2700	93.15	99.71
7	2700	86.54	99.83
8	2700	82.41	99.89
9	2700	76.54	99.91
10	2700	74.15	99.96

TABLE I: De-authentication DoS attack Statistics

B. Sniffer Characteristics

The wireless sniffer is written completely in C Language. We used MySQL as the database to maintain information about each client(s) and their network characteristics. The CPU & Memory usage of the sniffer is shown in Figures 6, 7. As we see the sniffer is lightweight in nature. Also it does not tax the CPU in terms of utilization as seen in Figure 6. The database(DB) usage by the sniffer is very low.We also flush the DB after 12 hours so that the size of database is always under limits. The lightweight nature of the sniffer makes it feasible for the administrator to easily integrate the module into their existing IDS without affecting the performance of IDS. In fact addition of the de-authentication DoS attack detection module will make the existing IDS even more robust.

6. CONCLUSION AND FUTURE WORK

In our work, we have proposed a novel de-authentication DoS attack detection methodology. The novelty lies in the fact that it can easily detect the de-authentication DoS attack without consuming much resources and also help victim client(s) to recover quickly from the attack. The only way to prevent deauthentication DoS attack is using authentication or encryption techniques for verifying the authenticity of de-authentication frame(s) or by upgrading to the 802.11w standard. Hence there is a need of an effective, lightweight technique to identify the de-authentication DoS attack in the network. Our methodology neither requires encryption, authentication or training the system previously. Our proposed methodology is lightweight and can easily be deployed to both open as well as encrypted networks. Coupled with the above features and the detection accuracy of our IDS, it makes even more attractive prospect for administrator to implement our IDS to secure their Wi-Fi networks.

ACKNOWLEDGMENT

The work is supported by Mrs. Anita Chopra, with full guidliance of her and under her view the paper work is done.

REFERENCES

[1] "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: 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, R.-P. Weinmann, and A. Pyshkin, "Breaking 104 Bit WEP in Less Than 60 Seconds," in *Information Security Applications*, ser. LNCS, 2007, vol. 4867, pp. 188–202.
[3] Aircrack-ng Suite. [Online]. Available: http://www.aircrack-ng.org/
[4] File2air. [Online]. Available: http://www.willhackforsushi.com/File2air.html
[5] Wireshark. [Online]. Available: http://www.wireshark.org
[6] 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*, ser. SSYM'03, Berkeley, CA, USA, 2003, pp. 2–2.
[7] Edgar D Cardenas - MAC Spoofing – An Introduction. [Online]. Available: http://www.giac.org/paper/gsec/3199/mac-spoofing-anintroduction/ 105315
[8] B. Aslam, M. Islam, and S. Khan, "802.11 Disassociation DoS Attack and Its Solutions: A Survey," in *MCWC*, 2006, pp. 221–226.
[9] C. Liu, "802.11 Disassociation Denial of Service (DoS) attacks," *School of CTI DePaul University*, 2005.
[10] F. Guo and T.-c. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," in *Recent Advances in Intrusion Detection*, 2006, vol. 3858, pp. 309–329.
[11] Detecting Wireless LAN MAC Address Spoofing Joshua Wright. [Online]. Available: http://www.willhackforsushi.com/papers/wlanmac-spoof.pdf
[12] J. Mar, Y.-C. Yeh, and I.-F. Hsiao, "An ANFIS-IDS against deauthentication DOS attacks for a WLAN," in *ISITA*, 2010, pp. 548–553.
[13] 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.
[14] F. Anjum, S. Das, P. Gopalakrishnan, L. Kant, and B. Kim, "Security in an insecure WLAN network," in *WCNM*, 2005, pp. 292–297.
[15] "IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Protected Management Frames. IEEE Std. 802.11w-2009, September 2009. ," *IEEE Std 802.11w-2009*, 2009.
[16] 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 *ICCCN*. IEEE,

2008, pp. 1–6.
[17] J. S. Park and D. Dicoi, "WLAN security: current and future," *IEEE Internet Computing*, vol. 7, no. 5, pp. 60–65, 2003.
[18] Crawdad - a community resource for archiving wireless data at dartmouth. [Online]. Available: http://crawdad.cs.dartmouth.edu/
[19] MadWifi. [Online]. Available: http://madwifi-project.org/
[20] BackTrack. [Online]. Available: http://www.backtrack-linux.org/
[21] Iperf - modern alternative for measuring maximum TCP and UDP bandwidth performance . [Online]. Available: http://code.google.com/p/iperf/

ABOUT THE AUTHORS.

Vipin Poddar: Mr. Vipin Poddar is an Electronics engineer and pursuing his master degree. He is currently working deep into the analysis of wireless protocols.

Mrs. Anita Chopra: Mrs. Anita Chopra is an Assistant Professor in Suresh Gyan vihar Un iversity. She has done specialization in wireless and digital communication, and she is having experience of more than 9 years.