A Lightweight Scheme to Mitigate Deauthentication and Disassociation DoS Attacks in Wireless 802.11 Networks

Haitham Ameen Noman, Shahidan M. Abdullah, Nazri Kama and Sinan Ameen Noman

Abstract—Wireless 802.11 has many flaws that expose the medium to various types of attacks. The absence of encryption at management and control frames exposes the medium to various types of inevitable Denial of service attacks at Data Link Layer. The attacker may spoof the unencrypted Deauthenticate/Disassociate message with the MAC address of the directed access point and continuously retransmitting it as a broadcast message to all designated clients to disrupt the connection with that particular node. Random bit approach was adapted and implemented in the proposed scheme to provide a layer of authentication in the management frames between the clients and the access point. The proposed scheme showed effectiveness in slowing the attack on both unencrypted and encrypted network by one hour and forty nine seconds without affecting the performance of the medium.

Index Term—Wireless 802.11, Deauthentication Attacks, Disassociation Attacks, Denial of Service.

I. INTRODUCTION

Wireless local area networks (802.11 IEEE Standard) also known as WLAN and WI-FI has become more eminent and prevalent than ever before, making it to be an essential and primary medium to connect various types of devices to the internet. Vividly, this can be noticed as it is rare nowadays to not find a wireless access point whilst scanning in a particular area. People need to stay connected wherever they go, in airports, restaurants, coffee shops and homes. Nevertheless of the arrival of new technologies the 3G and 4G networks yet people still prefer to rely on the 802.11 wireless network due to its convenient price and most importantly it consumes less energy than 3G and 4G networks do. [1]

WLAN layer two MAC control frame was designed to be divided into three frames, Management frames, Control frames and Data frames. Management frames are responsible for preserving and maintaining communication between the access points and wireless clients; moreover they are responsible for authentication, Deauthentication, Association and Disassociation. The control frames are responsible for ensuring a proper exchange of data between the access point and wireless clients, on the other side the Data frame carries the data on the wireless networks and whereby encryption algorithms like WPA/WPA2 implemented on. However, the encryption is applied only on the data frame in the meantime, both media control and management frames are designed to be utterly unencrypted, which gives the upper hand to the hackers to attack the availability factor of wireless in order to deny the users from accessing the service. Also the attack can leverage the attacker to lure the users to connect to a rogue access point to steal the client’s data or tamper it. [2], [3], [4]

Unfortunately wireless security experts have neglected the attacks that target the availability factor and emphasized only on both confidentiality and integrity security factors, which increased chances to the hackers to enhance, leverage and launch more sophisticated and varies types of wireless DoS (Denial of service) attacks to WLAN networks. IEEE 802.11 community has ratified the 802.11w standard in 2009. The new standard provides both authentication and encryption protection to 802.11 management. The main advantage of the new standards is to prevent DoS attacks that exploit spoofing of management frames only by implementing MFP technology (Management frame protection) [12]

A Station that supports 802.11w can easily distinguish whether the Deauthentication frame came from a genuine access point (If only the Access point supports 802.11w) or was impersonated by an attacker who spoofed the access point. It directly drops and ignore any spoofed Deauthentication frame so that it prevents the DoS attack from being carried out. Similarly, the authenticity and integrity of other impersonated management frames are guaranteed by the 802.11w standard as well [12]. Regrettably, the 802.11w standard is promising only to protect from DoS attacks that exploit spoofed management frames (Disassociation or Deauthentication). It does not provide protection from similar attacks that use spoofed control frames, RF jamming or media access. Another significant limitation can be addressed in the w standard is the standard does not provide a protection for open networks (public networks without password) also the standards is incapable of providing protection without causing a noticeable performance degradation to the network under high rate flooding. [2] Wireless Availability attacks can be broken down according to each OSI layer altogether risk level as illustrated in Fig.1. However, this paper sheds the light on Data link layer attack whereas the attacker is not conditionally connected to the network in order to launch a potential attack. The reason behind focusing on this particular layer is the shortage of concurrent solutions that mitigate DoS attacks on this specific layer. Different hard work and researches were conducted to mitigate the attacks on application, transport and network layers yet unfortunately both layer two and layer one were neglected and left to be exploited by hackers. [3], [4] Deauthentication/Disassociation attacks are both parts from layer two, however detecting these types of attacks requires a skillful network administrator consequently, the need for an automated monitoring tool raised to provide an easy way to
alert the regular user if there is an aired on going Deauthentication/Disassociation attacks. The attacker tends to launch periodic spoofed Deauthentication or Disassociation for the sake of divulging hidden SSID of the targeted access point also to obtain a handshake to be used later on in cracking WPA2 encryption. [2],[3],[4] Another practical justification for the attack is to prevent the client to connect to the legitimate access point and to lure the clients to connect to rogue access point in order to steal, redirect or tamper client’s data while en route. [5] Fig.1. Illustrates DoS attacks on each OSI layer alongside risk, mitigation and detection possibilities.

II. MAC LAYER DOS ATTACKS TYPES

A. Deauthentication Attack

The attacker spoofs the MAC address of a particular legitimate access point and launch periodic Deauthentication frames to designated connected client or to all clients as a broadcast message. In case the attack was continued, the clients will irrefutably not be able to establish a connection to the wireless network the attacker may also reverse the attack by spoofing the MAC address of a legitimate client and then to send Deauthentication frames to the access point [3], [6], [12]. The attack can possibly target a certain channel as well, causing a network disruption to multiple access points at a time. Fig.2. demonstrates the scenario of the attack. [15]

B. Disassociation Attack

Disassociation attack runs on the same concept as Deauthentication flood. A mobile station may be authenticated with numerous access points at once. Association procedure allows the mobile station to decide which access point will be used for communicating with the network. Disassociation when sent in its turn terminates this relationship. This attack is less efficient than Deauthentication however, it is functionally identical to it. [2], [3], [4]

C. Power Saving DoS Attack

Mobile WLAN clients (Tablets, Laptops and smart phones) are designed to set automatically into sleep mode whilst their WLAN radio is disabled to save battery life. Basically, the concept of this attack is based on tricking the designated access point into believing that the particular connected client is in power save mode. Consequently, the access point will buffer ordinated frames to the client, causing a partial disconnection from the network. When an associated client is in a sleep state, the Access point buffers the intended traffic for the client. The client wakes up every so often and queries the access point for any buffered traffic, which then the access point delivers and discards. An attacker can exploit this feature by sending an impersonated periodic power save query message, while the client is still in sleeping mode, causing the Access point to transmit and discard any buffered traffic. [7]

D. Authentication/Association flood attack

In this scenario, an attacker tends to use a spoofed source MAC addresses that attempt to authenticate and associate to a target access point. The attacker continually makes association or authentication requests, causing fully consumption of access point memory and processing capacity, leaving clients
with limited or no connectivity to the wireless networks. Several prevalent tools can launch the layer two DoS attacks. The most efficient one is based in Linux. However, aircrack-ng suite includes a tool called aireplay-ng, it can be used to send two sided Deauthentication/Disassociation packets against designated access point and the clients at the same time.[13],[14] Also it has the ability to send a flood of Authentication/Association request. [10] However, this paper considers shedding the lights on solely Deauthentication and Disassociation attacks. [5], [6]

III. ATTACK ANALYSIS

In order to design an enhanced WLAN scheme to protect against Deauthentication and Disassociation DoS attacks, an analysis need to be conducted on a real time attack. Wireless long ranged Alfa adapter was used under Kali Linux during the analysis phase alongside Wireshark network protocol analyzer tool. [11] The first step in the analysis phase will be conducted by launching a real time Deauthentication attack from a virtual machine that runs Kali Linux. Subsequently, Wireshark network analysis software will be run on another wireless interface and to be set in monitor mode to analyze the aired attack. The attack received packets then will be constructed into binary dump form. Further analysis will be conducted on the saved file for identifying the unused bit in the WLAN frame. The unused bit will be reused in the new proposed WLAN scheme to provide robustness against similar attacks. A custom build simulator in .NET was used to test the new scheme robustness level against both Deauthentication and Disassociation attacks to be compared with the current scheme (802.11 n). Fig.3. depicts research analysis phases.

As shown in Fig.4. The attacker sends numerous periodic Deauthentication packets to all connected clients to a designated access point with the presented MAC address. On the other side, the clients will instantly got deauthenticated which may grant the attacker a potential chance to create rogue access point in order to lure the clients to connect to it. While the attack is running, as shown in Fig.5. Wireshark network analyzing tool was used to analyze the real time aired packets.

By analyzing the whole MAC frame in Fig.5. Deauthentication DoS attack scenario, the following sequence of bit stream (208 bit) will be extracted using Wireshark as shown in Fig.6.

<table>
<thead>
<tr>
<th>Frame</th>
<th>Type/Subtype</th>
<th>Deauthentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>0010</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>0011</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>0100</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>0101</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>0110</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>1000</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>1001</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>1010</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>1011</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>1100</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>1101</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>1110</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>1111</td>
<td>00000000</td>
<td>00000000</td>
</tr>
</tbody>
</table>
The explanation of the outcome bits is as follows:

1) The first two bytes (8 bit) indicate protocol version (00), management type (00) and Deauthentication subtype (1100).

2) The second two bytes indicate the duration of the packet which set to be zero.

3) The third 6 bytes represent the MAC address of targeted clients which set to be broadcast to deauthenticate all clients.

4) The fourth 6 bytes represent the attacker MAC address which is a replica to the targeted access point one (the fifth 6 bytes)

5) The sixth 12 bit indicate the sequence number of the packet (left to be zero)

6) The last 20 bit represent unused feature in WLAN, the fragment number (4 bit) and the reason code (Two bytes) which is set to be unspecified in all Deauthentication and Disassociation attacks.

What can be observed from above scenarios, the values of Deauthentication and Disassociation values are both set to be fixed in each attack and sent in plain form (unencrypted) which consequently makes it so easy to get intercepted and replayed. Fig.7 illustrates the break down structure of Deauthentication attack in WLAN 802.11 n scheme.

IV. **THE PROPOSED SCHEME**

Although, the management frames are sent in plain text and in a static form as explained previously however, applying cryptography to this layer will not suffice as it will provide protection to solely WLAN networks that implement WPA/WPA2 encryption. A practical example of that gap can be noticed in the new WLAN 802.11 w standards. [8], [9]

The proposed solution to this dilemma suggests a radical and drastic change in the mechanism and the functionality of the last twenty bit in the WLAN MAC layer frame scheme (The Fragment and Reason/Status Code) since the fragment number (4 bit) is unused in all cases and the reason code length in case of Deauthentication/Disassociation attacks is a fixed value of 16 bit (2 bytes), thus those bits can be randomized and issued by the access point to every single client during authentication response step. Then the access point will generate a table to relate every connected MAC address with its random issued value so that when the client needs to deauthenticate from a particular access point, the client would need to send the exact generated value of that random bit stream back to the access point and in case it matched with the stored one. The access point would deauthenticate the client accordingly. Random number generating algorithm (MAX value) has been designed to generate random distributed values at each established connection (20 bit). The Random number generating (MAX value) algorithm is based on using system time (Seconds, Milliseconds and Microsecond followed by the factorial function of the current iteration number) to generate distributed range of numbers within the range from 1 to 20 bit. The formula of the algorithm is formulated as follows:

\[
\text{Generated Number} = \left( X \times (Y-C) - M + \text{Factorial}(C) \right) \mod 1048575 + 1 / (C+1)
\]

Where X= Current System Seconds, Y=Current System Millisecond, C= Counter, M= Microsecond

The formula generates random pseudo numbers ranging from (1 to 1048575 (20 bit)) and has been tested under Kali Linux and coded in Python and succeeded to generate up to one thousand distributed number with zero collision. By applying MAX value on the structure, the new WLAN MAC Deauthentication scheme will be functionalizing and structured as shows in Fig.8.

The proposed scheme will be applied and implemented on the new Authentication/Association procedures. The client sends a probe request to the designated access point. The access point responds with a probe response to indicate its presence and will respond with probe response. The probe response permits the client to provide the password to get authenticated. The client will then send an authentication
request alongside the password needed. The access point will validate the password and then will use MAX value to generate a random number of 20 bit length to be stored alongside the MAC address of the client in a specific table. The generated value will be sent to the client in the last 20 bit space of the proposed WLAN scheme. The client will store the value to use it later in the Deauthentication phase. Finally, the last phase will involve the association request that sent by the client to the access point. Similarly, the access point will generate another value to the client to be used when Disassociation value is requested. Fig.8. and Fig.9. represent the implementation of the proposed scheme in both Authentication/Association procedures between access point and client.

As mentioned previously both Deauthentication and Disassociation mechanisms are two sided ways, as frames can be sent from client to access point and vice versa. According to the new proposed scheme, when a particular client tends to Deauthenticate or Disassociate from an authenticated access point, the client would need to send the generated received random value (the last randomized twenty bit) from the access point and in case its match the stored value in the access point generated table. The client will be deauthenticated/disassociated accordingly. The proposed procedure is illustrated in Fig.10.

Similarly, in case the access point intended to Deauthenticate/Disassociate a particular client it needs to send the generated value alongside the Deauthentication/Disassociation frame, the client will then check if it matches the stored value, then Deauthentication/Disassociation to take place accordingly. As shown in Fig.11.

Since the new WLAN scheme is based on altering the mechanism of existent frames (Fragment and Reason frames) there seem to be a significant draw back in terms of justifying the reason behind disconnection ever since the Reason Code frame has been altered to provide authentication. However, both reason code/status code can be extracted from the control frames only when troubleshooting conducted using network analyzing tool like Wireshark. Fig.12. demonstrates the phases of both authentication and Deauthentication in the new proposed scheme.
V. BENCHMARKING

The benchmarking phase was conducted on the proposed scheme alongside MAX algorithm separately. However the concluded results was compiled in a single result to form the conclusion. The benchmark phase is divided into two phases. Phase one involves benchmarking the proposed WLAN scheme by first design and implement MAX simulator in .NET that simulates a real access point enhanced with the proposed WLAN scheme. The next phase involves launching Deauthentication and Disassociation attacks on the proposed scheme to test its robustness against the attacks. Phase two was conducted in a parallel way with phase two as the MAX value algorithm has been used in phase two. However, MAX algorithm was implemented and tested in python compiler under Kali Linux by generating one thousand different number to test the distribution level, the collision of the algorithm and finally the performance. The algorithm was compared with Microsoft random number generating algorithm and with the one that is used in Python library. In the end the generated numbers was used in the simulator to randomize the last twenty bit during the Authentication and Deauthentication of the proposed WLAN scheme. Fig.13. illustrates the benchmarking procedure.

A. MAX Algorithm Benchmarking

We benchmarked MAX algorithm on Linux with the pseudo random generation algorithm that used by Python standard library and the algorithm that used by .NET library. The benchmarking considered taking in consideration of two important factors during the evaluation of the algorithm. The performance of the algorithm and the number of existed collisions in the generated numbers. The test was conducted by generating “1000” number of 20 bit in a text file. A small script was written in Python to find the number of collisions in that particular text file. Moreover, three files were generated, each file has been given a significant name according to the algorithm that was used in the generation of the written list. The first file was named “MAX “the other was named “Python” and finally the last one was named “.NET”. The performance of the algorithms has been measured by monitoring the CPU utilization while running each algorithm independently. Table 1 illustrates the benchmarking of the three algorithms when generating 1000 numbers.
MAX algorithm proved to be the least one in terms of collision numbers. However, the algorithm that used by Python library was proven to be the one with highest performance. Subsequently, it has four collisions. In our scenario we do not need high performance as much as we need an algorithm with least collision when generating 20 bit. Reasonably, because we need to issue one value per each authentication request, which will be generated instantly.

B. Proposed Scheme Testing

In order to test the proposed scheme, we created a virtual custom built simulator in Microsoft .NET to simulate the communication procedure of the management frames easily between a particular client and an access point. The simulator runs in two modes; the first one is the regular mode, whereas WLAN scheme (802.11 n) is implemented and the second one is the proposed WLAN scheme. MAX simulator idea is based on presenting the exchange process of the management frames structure in binary format. Moreover, the generated attacking result shows that in the first scheme the attacker would need only two seconds to deauthenticate a designated client. On the other side, when the proposed scheme is implemented, the notorious attacker would need up to 3649 seconds in order to deauthenticate a specific client. Fig.14. and Fig.15. illustrate the difference between the two schemes in terms of time needed to deauthenticate a client.

The proposed scheme will not prevent the attack utterly as it will only slow it down by an hour and forty second. The attacker would need to guess the exact generated value by brute forcing the 20 bit (MAX value) in order to deauthenticate the client again. Moreover, the scheme provides a seamless protection against both Deauthentication and Disassociation attacks even if WPA2 was not enforced. However, the proposed scheme will lack both Status and Reason code as they will be both replaced by the MAX value to provide the authentication during the exchange of management frames. However, the regular users will not be affected or noticing the absence of these codes.

VI. CONCLUSION

In this paper we designed a proposed resilient WLAN scheme to slow down the Deauthentication and Disassociation DoS attacks on WLAN networks. Random bit approach based on custom built random generating algorithm (MAX value) was applied on both Authentication and Deauthentication procedures to provide a layer of authentication during management frames exchanges. The Scheme shows to slow down the attack by more than an hour and forty second with no need to enforce WPA2 encryption. Similarly, the research shows the more random bit can be used in the scheme the more difficult the Deauthentication and Disassociation attacks can be carried out.

ACKNOWLEDGMENT

This work was supported by Universiti Teknologi Malaysia (UTM)

REFERENCES


[7] Leandro Meiners, ”But...My Station is Awake! (Power Save Denial of Service in 802.11 Networks”, September, 2009


