Journal of Theoretical and Applied Information Technology
30th November 2016. Vol.93. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A ROBUST SCHEME TO DEFEND AGAINST DISASSOCIATION AND DEAUTHENTICATION DOS ATTACKS IN WLAN NETWORKS

[1]HAITHAM AMEEN NOMAN, [2]SHAHIDAN M. ABDULLAH AND [3]SINAN AMEEN NOMAN

[1]Universiti Teknologi Malaysia, Department of Advanced Informatics School

[2]Universiti Teknologi Malaysia, Department of Advanced Informatics School

[3]Princess Sumaya University for Technology, Department of Computer Science

E-mail: [1]haitham.online@yahoo.com , [2]mshahidan@utm.my, [3]sinanameen@gmail.com

ABSTRACT

Wireless 802.11 (also known as WLAN) has many flaws that expose the medium to numerous types of attacks. WLAN control frame consists of three major parts; data, management and control frames. Data frame is whereby data carried on, in the meantime, management and control frames are both responsible for maintaining the communication between the clients and the access point. The absence of encryption at both of these two frames exposes the medium to inevitable various types of DoS attacks at Data Link Layer. The attacker might spoof the unencrypted Deauthentication/Disassociation message together with the MAC address of the targeted access point and keep retransmitting it to all clients causing a continuous disconnection in WLAN networks. Wireless 802.11w standards has succeeded mitigating the flaw by encrypting the frames, yet only when WPA2 encryption is enforced. In this paper, we developed an enhanced proposed WLAN scheme to mitigate Deauthentication and Disassociation DoS attacks on WLAN networks. The proposed scheme is based on modifying the last twenty bits of the management frame in 802.11n standard using an enhanced version of Linear Congruential Algorithm called MAX algorithm. This is to provide a layer of authentication with no need to enforce WPA2 encryption. The proposed scheme is evaluated using CommeView Simulator and showed to be robust by slowing the attacks in an average of 3551 second on both encrypted and unencrypted networks.

Keywords: *WLAN, Wireless 802.11, Disassociation Attacks, Deauthentication Attacks, Denial of Service.*

1. INTRODUCTION

Wireless 802.11 networks also known as WI-FI or WLAN is a ubiquitous medium. It is seldom nowadays to not find a wireless access point while scanning in a certain area. The need for People to stay connected wherever they go in restaurants, airports, residential places and coffee shops. In spite of the arrival of alternative technologies like 3G, LTE and 4G networks, thus far many people still opt to depend on WLAN networks because of its affordable price and most significantly, it provides better energy-saving than 3G, LTE and 4G networks do [1]. Data link layer (Layer two) in WLAN networks consists of three major parts, Management frames, Control frames and Data frames. Management frames part is in charge of sustaining communication between wireless clients and the access point; additionally, they are responsible for Deauthentication, Authentication, Disassociation and Association [2]. On the other side, control frames part is accountable for guaranteeing an appropriate exchange of data between the access point and wireless clients. Moreover, Data frame carries the data on the wireless networks whereas, cryptographic algorithms like TKIP in WPA2 implemented on [3]. However, in WLAN networks cryptography is enforced on the data frame only.

In the intervening time, media control and management frames are both designed to be entirely unencrypted, which is considered a given leverage to the notorious hackers to target the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

accessibility of WLAN networks in order to prevent WLAN clients from using the service [4]. Similarly, the attacker may use the attack to trap the clients to associate to a malicious node to intercept and collect their data and modify it as well [5]. Sustaining WLAN availability and defending it from hackers have been ignored by WLAN designers, abundant efforts were put to enhance and improve WLAN confidentiality and integrity factors. Eventually, it created potential odds to the attackers to develop and execute advanced types of WLAN DoS attacks. The community of IEEE 802.11 in 2009 has ratified and approved 802.11w standard [2]. The standard provides both cryptographic and authentication protection to 802.11 management frames in data link layer [4]. The standard has succeeded to prevent DoS attacks that exploit masquerading of management frames by simply implementing MFP technology (Management frame protection) [5] [6].

A client and access point that mutually support MFP can easily differentiate whether the Disassociation or Deauthentication packet is coming from a legitimate node. It immediately drops and ignore any impersonated Deauthentication packet, with the purpose of denying the DoS attack from impacting the network availability. Likewise, the authenticity and integrity of other impersonated management frames are ensured by the 802.11w as well [6] [7].

Unfortunately, MFP technology in 802.11w standard only provides protection from DoS attacks that target management frames (Deauthentication or Disassociation). It does not protect from alike attacks like RF jamming or power saving. Yet, another noteworthy limitation can be observed in MFP, is it does not provide a seamless protection to public networks similarly, the technology when implemented suffers from obvious performance degradation to the network [8] [9].

A central manager (CM) has been proposed by P.Ding in 2007 to work as an authentication server that centralized to manage the number of access points. The Access point will stop processing Authentication/Association request frame if it receives certain number of frames per second [18].

A normal Access point can receive and process around five 802.11 frames per second. limitation can be observed is the large network overhead caused by the approach. Detecting the attacker using network monitor tools like Wireshark and Tcpdump might not be feasible enough due to some legalization issues as the attacker (Deauthentication Transmitter) could be a neighbor of the victim, when the attack is detected the victim needs search warrant to catch the attacker red-handedly [19]. WLAN DoS attacks can be categorized based on OSI layers alongside detection possibility and risk level as depicted in Figure 1. However, the scope of this paper is on MAC layer DoS attacks, while the attacker is not connected to the WLAN network to perform a successful attack. Mitigating DoS attacks on this layer is important due to the lack of concurrent seamless solutions that defend against DoS attacks on this particular layer [10]. Numerous serious effort, work and researches have been conducted to countermeasure the attacks on application, transport and network layers yet regrettably, layer one and layer two were both almost ignored to be an easy target by deranged attackers [11]. The attacker leans towards executing continuous Deauthentication/Disassociation for many reasons like revealing hidden SSID of the designated access point. Another significant purpose from the attack is to receive a handshake for the sake of cracking WPA2 passphrase [6] [12]. The riskiest attack might be performed to terminate the connection between the client and the authentic access point to trap the users to connect to malicious access point to steal, or change the user's sensitive data. Figure 1. demonstrates the types of DoS attacks based on OSI layers.

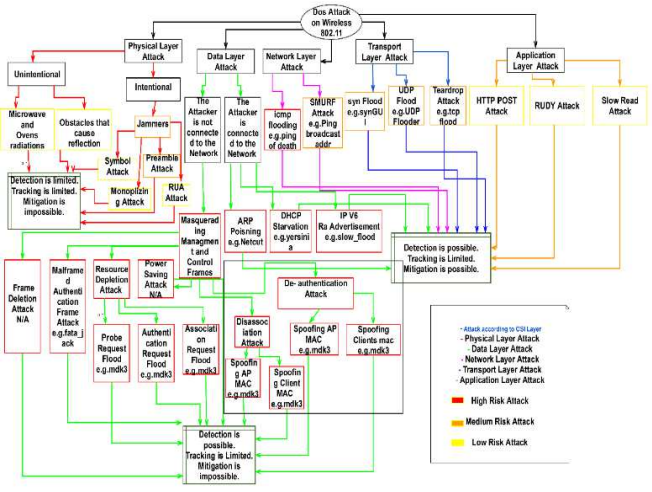

Figure 1: WLAN DoS Attacks According to OSI Layer.

The purpose of this paper is to enhance WLAN scheme to be able to defend against Deauthentication and Disassociation attacks

Journal of Theoretical and Applied Information Technology
30th November 2016. Vol.93. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

without the need of hardware upgrade on both sides; client and access point. Moreover, the scheme should provide the protection to both unencrypted and encrypted networks. This paper is divided into following section. Section 2 will explain layer 2 DoS attack types in details; Section 3 will discuss WLAN scheme analysis; Section 4 will discuss the proposed WLAN scheme; Section 5 will discuss the validation of the proposed scheme. Section 6 will discuss the conclusion. Finally, Section 7 will discuss the future work of the research.

2. LAYER 2 DOS ATTACK TYPES

This paper focuses on Layer two Deauthentication and Disassociation DoS attacks where the attacker is not connected conditionally to the WLAN network as shown in Figure 2.

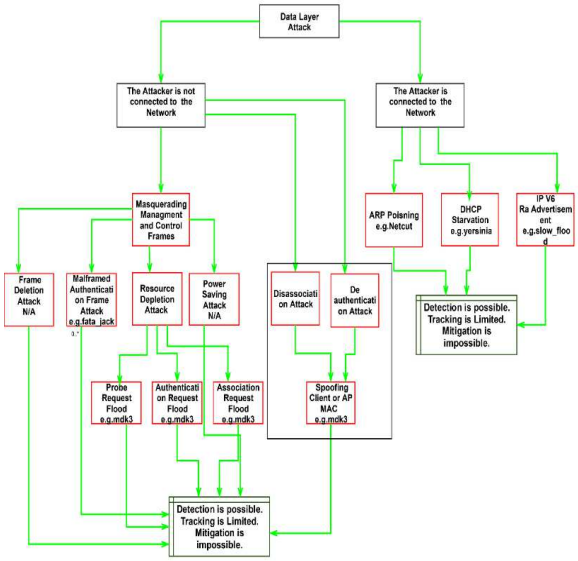

Figure 2: WLAN DoS Attacks According to MAC Layer

2.1 Deauthentication DoS Attack

The notorious attacker masquerades the physical address of a specific access point and execute continuous Deauthentication packets to every associated client. If the attack continued, the associated clients will unquestionably fail to establish a connection to the WLAN networks.

The attacker might invert the operation by impersonating the physical address of a genuine client and then start sending Deauthentication packets to the access point [3]. The attack can potentially target a designated network channel also, leading to connection disruption to several access points at the same time. Figure 3 illustrates the set-up of the attack [4] [7].

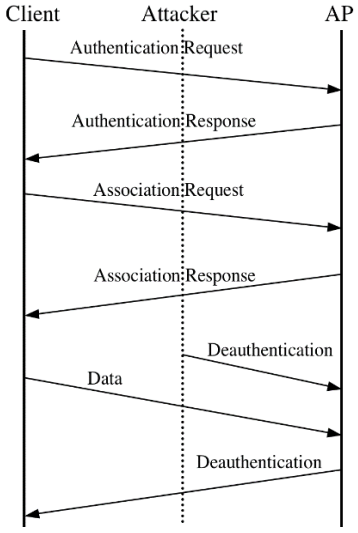

Figure 3: Deauthentication Attack Mechanism

2.2 Disassociation DoS Attack

Disassociation is as Deauthentication in terms of concept and functionality. As demonstrated in Figure 2, Association ensued by Authentication. A client might be authenticated yet still not fully associated with the access point. Once association procedure took place, a client can exchange data with its associated access point. Similar to Deauthentication attack, the attacker may transmit multiple Disassociation packets to disrupt the connection and get it back to Authentication phase, however, Disassociation attack has less impact, since it terminates the connection partially, leaving the client in a limited or no connectivity status. [8] [9]

3. WLAN SCHEME ANALYSIS

Wireless Alfa adapter with Wireshark network analyzer tool were used to dissect Deauthentication attack packets on WLAN networks. To construct the attack in binary format, Kali Linux was installed and set on virtual machine to simulate the attacker machine that transmitting periodic Deauth/Dissas packets.

Journal of Theoretical and Applied Information Technology
30th November 2016. Vol.93. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In the meantime, Wireshark tool will be run on another Linux machine to monitor and save the aired packets into a specific file. An intensive analysis will be performed on the saved file for recognizing the required bits that will be randomized in the WLAN layer two. The identified bits will be reused in the proposed WLAN scheme to provide authentication against spoofing attacks and Deauthentication/Disassociation as well.

Commeview for wifi simulator has been used to evaluate the proposed scheme robustness against Deauth/Dissas attacks to be benchmarked with Wireless 802.11n scheme [14]. Figure 4. illustrates research analysis steps.

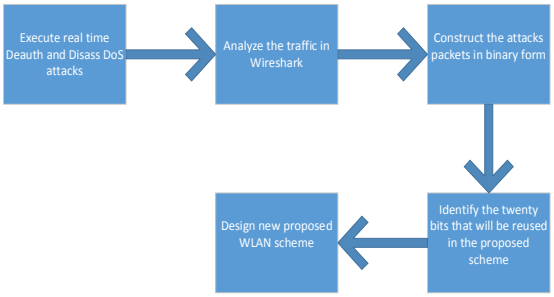

Figure 4: Research Analysis Steps

The first step of the analysis commences with transmitting broadcast Deauthentication packets to terminate the connection between the AP and the authentic associated client devices. The attack is executed by spoofing the physical address (BSSID) of the legitimate access point using airplay-ng tool [15] as shown in Figure 5.

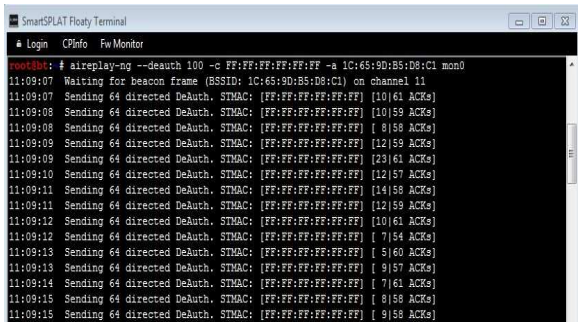

Figure 4: Deauthentication Attack in Airplay-ng tool

Since the attack is ongoing, the associated client's connection with the access point will be terminated immediately as a result of the spoofed Deauthentication packets.

At the same time, Wireshark analyzing tool [16] will be run on the other Linux virtual machine to analyze the attack as depicted in Figure 6.

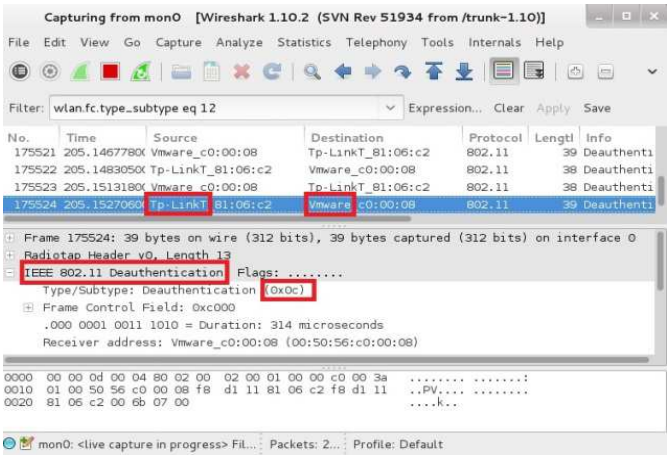

Figure 6: Wireshark Attack Analysis

Figure 7 shows sequence of bits (208 bit) were extracted from the explained attack to illustrate layer two scheme in 802.11n standard.

Figure 7: Deauthentication Attack Byte Structure

The first 16 bits specify protocol version zero, frame type and subtype which respectively set to be management frame and Deauthentication packet. The next 16 bits specify the duration the packet needs to consider for delivering in this case it set as zero as well.

The successive 48 bits indicate the physical address (MAC Address) of the designated clients. The fourth 48 bits specify the spoofed physical address by the attacker, which in this case represent the same address of the attacked access point. The next two bytes specify the sequence number of the transmitted packet. The last 20 bit are the most important in the proposed scheme as they specify the unused 4 bits in WLAN layer two; the fragment number (4 bits) and the reason code (16 bits)

Deduction from bit analysis indicate the values and pattern of Disassociation and Deauthentication are always fixed and unencrypted in each particular attack. Figure 8 shows the WLAN 802.11n scheme functioning the Deauthentication in low level binary format.

Journal of Theoretical and Applied Information Technology
30th November 2016. Vol.93. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

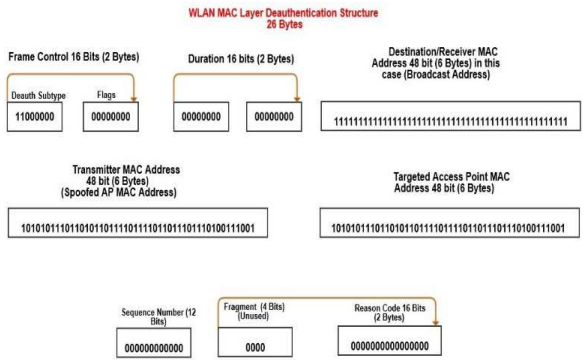

Figure 8: WLAN MAC Layer Deauthentication Structure

During Disassociation attack, WLAN scheme would be similar to the Deauthentication, the only difference is the subtype value, that supposes to hold the value of "1010" rather than "1100" [2] [5] [6].

4. WLAN PROPOSED SCHEME

Applying and implementing cryptography to layer two management frames will not be satisfactory, as it would expose the unencrypted networks that do not apply WPA/WPA2 to Deauth/Dissas attacks. A prominent example of this gap can be noticed in MFP technology in Wireless 802.11w standard. The proposed scheme is based on changing the functionality of the last twenty bits in WLAN layer two frame. The last twenty bits are deducted from Fragment number (4 bits) and Reason Code (16 bits) [13].

These bits are then being randomized and issued by the access point to the authenticated client throughout authentication response. At that moment, the access point will construct a specific table to relate each associated physical address alongside its random delivered value so when a specific client intended to get Deauthenticated from an access point, the client would need to verify its authenticity by sending the exact value of random value to the designated access point. The access point would terminate the connection with the client according to the validity of the received MAX value. An enhanced version of LCG (Linear Congruential Generator Algorithm) [17] was designed and developed called (MAX Algorithm).

MAX algorithm is responsible of generating random values within each connection. The value's length is 20 bits. MAX Algorithm was designed on Five steps; The First step specifies seed generation as the random values are selected according to system time, by multiplying system seconds and system milliseconds. In step Two, the distribution factor of the algorithm is enhanced by subtracting the value from the current microsecond and strengthen the formula with factorial function. Step Three, specifies the examination of the boundary of the generated value not to exceed 2^20 bits thus, modulo function was used. In step Four, three random values are being issued by MAX algorithm to feed the three variables of LCG algorithm. In conclusion, steps five involves the generation of a fourth generated value by MAX algorithm to be XOred with the LCG algorithm's final generated value to produce 20's bit value. The final generated value will be used in authentication response stage in WLAN proposed scheme. MAX Algorithm model can be illustrated in Figure 9.

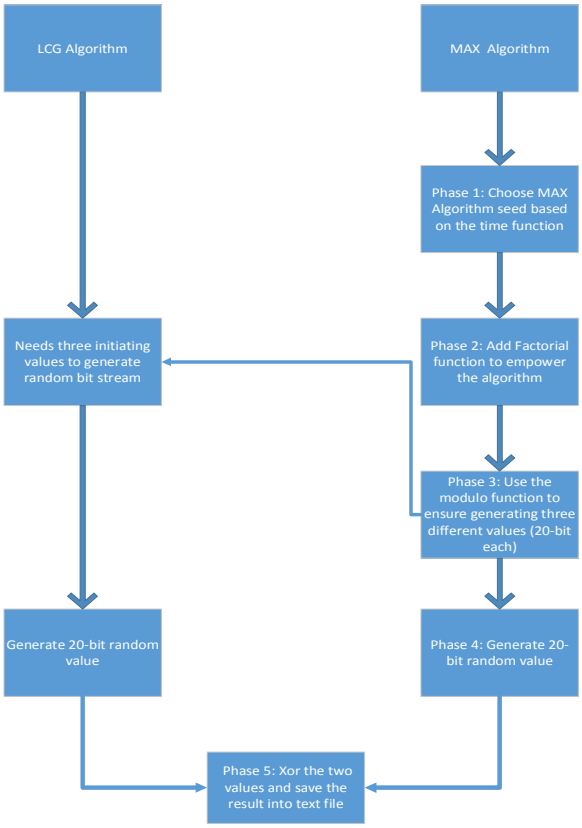

Figure 9: MAX Algorithm Model

MAX Algorithm generates the needed distributed values by the proposed scheme as ranged from 1 to 1048575. MAX Algorithm was coded in Python in Linux. The proposed WLAN layer two Deauthentication scheme will be functioned and structured after applying MAX Algorithm as depicted in Figure 10.

Journal of Theoretical and Applied Information Technology
30th November 2016. Vol.93. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

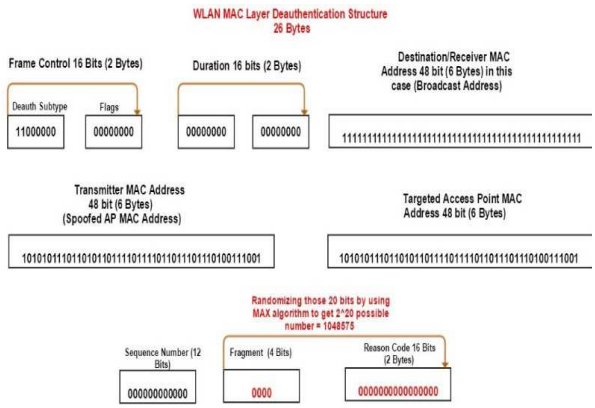

Figure 10: Wlan Mac Layer Deauthentication Structure

During Association and Authentication steps, the client would need to send a probe request to the access point that he desires to connect to. The access point will respond with a probe response to specify its attendance and to allows the client to provide the required passphrase for authentication. Afterward, the client sends an authentication request alongside the required passphrase. The access point will validate the passphrase and will generate a specific random value of 20-bit using MAX Algorithm.

The generated value will be stored along with the physical address of the designated client in a pre-constructed table. MAX generated value will fit into the last twenty bits of WLAN MAC frame and will be sent to the client. The client will then store the received MAX value for the purpose of using it later on during the Deauthentication phase. Lastly, in the association request, the access point will generate another value to the client to be used when Disassociation to take place. Figure 11, shows the implementation of the proposed scheme during Association/Authentication procedures.

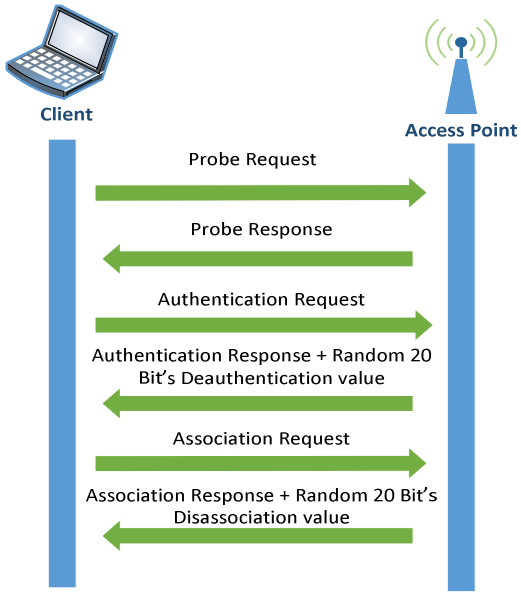

Figure 11: Proposed Authentication Procedure

Disassociation and Deauthentication DoS attacks can be performed in two-sided ways. The frames can be transmitted from the access point to the client(s) and vice versa. In the proposed scheme, when a particular client desires to terminate the connection from an associated access point, the client would need to send MAX value that was pre-received from the access point and only if its match a Deauthentication/Disassociation will take place successfully. The proposed procedure is demonstrated in Figure 12.

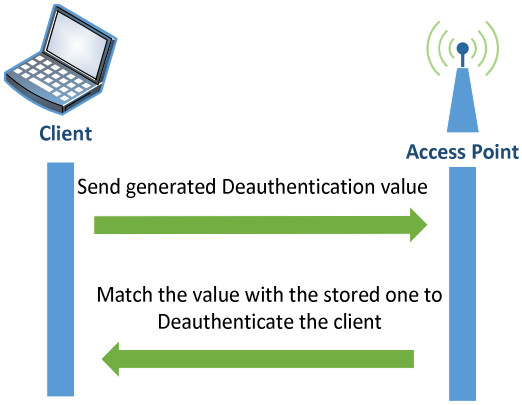

Figure 12: Proposed Deauthentication Procedure (Client To AP)

Correspondingly, when the access point desires for any reason to either Deauthenticate or Disassociate an associated client, it should send the MAX value with the Deauthentication or Disassociation frame, the client will check and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

validate the received value and accordingly a proper connection termination to take place as demonstrated in Figure 13.

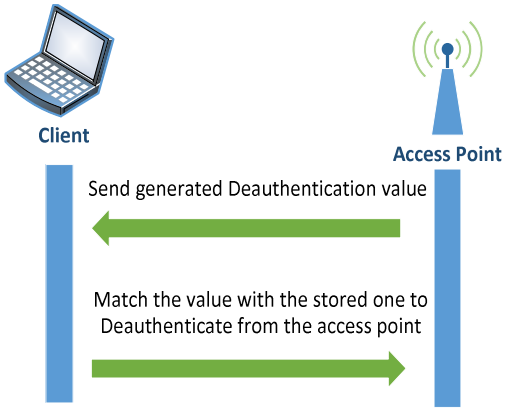

Figure 13: Proposed Deauthentication Procedure (AP to Client)

The proposed scheme as mentioned previously is based on changing the mechanism and functionality of both Fragment and Reason code. For that particular reason, a significant draw back can be shown in terms of justifying the reason behind any disconnection, since the functionality of the Reason Code has been changed and altered to provide a layer of authentication.

However, reason code and status code can both be extracted from the MAC frame when only troubleshooting performed using network analyzing tools. Figure 14, illustrates the phases of Authentication and Deauthentication in the proposed scheme.

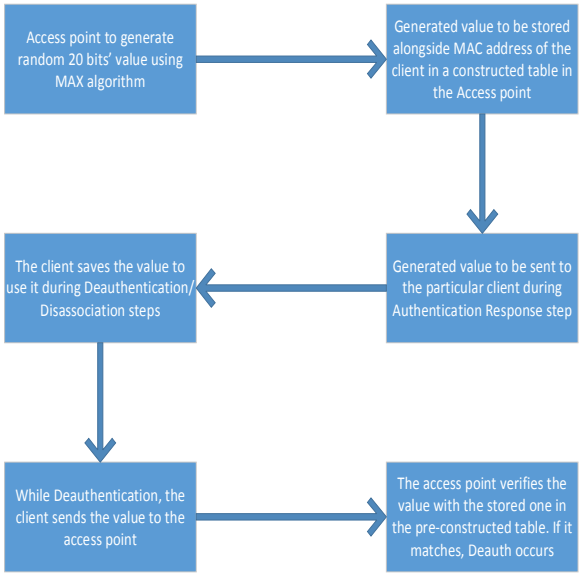

Figure 14: Authentication and Deauthentication Phases in the Proposed Scheme

5. VALIDATION

Validation phase is basically consisted of two major phases; Phase one specifies testing the proposed scheme by using CommeView simulator by performing Disassociation and Deauthentication attacks on the proposed scheme to evaluate the scheme robustness against the attacks. Moreover, phase two was conducted in a corresponding way with phase the first phase. Testing involves evaluating the algorithm's collision level, performance and finally distribution level. The algorithm was benchmarked with Mersenne Twister algorithm and LCG Algorithm.

In the end the generated numbers were used to randomize the last twenty bit during the Authentication and Deauthentication of the proposed scheme. Validation process can be illustrated in Figure 15.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

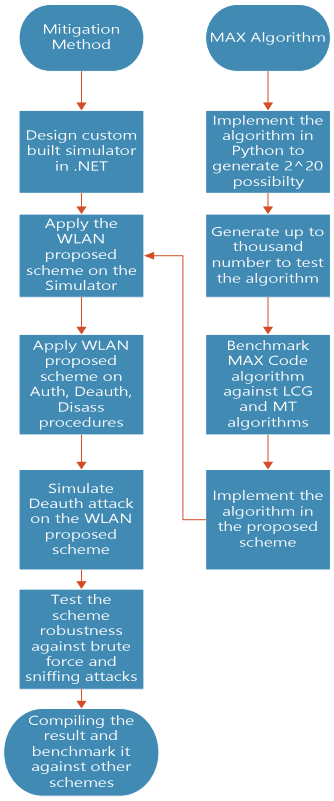

Figure 15: Proposed Scheme Validation Process

5.1 MAX Algorithm Benchmarking

During benchmarking, three thousand random number of twenty bits were generated. Each thousand number were generated using a particular algorithm and stored in a specific text file. Each text file was named according to its algorithm as follows; MAX Algorithm, LCG Algorithm and MT Algorithm. For the purpose of checking the number of duplication values inside each designated text file, a small script written in Python was used for this purpose "SIM Script". The three algorithms were written in Python language and tested in Kali Linux. The CPU utilization was measured by utilizing Linux process manager. Figure 16 illustrates extracted results of the test.

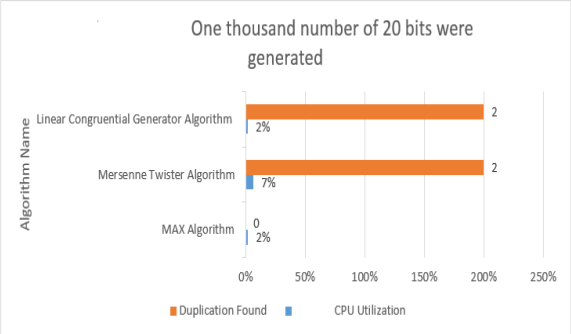

Figure 16: MAX Algorithm Benchmarking Results

During the generating of one thousand number with twenty bits' length, MAX algorithm shows to generate no duplications. In the intervening time, Mersenne Twister algorithm has two duplicated numbers and Linear Congruential Algorithm has two. Moreover, the deducted results show Mersenne Twister algorithm utilizes more CPU percentage than both MAX and LCG algorithms utilize combined. However, both LCG and MAX algorithm utilize the same percentage of CPU usage. Moreover, the common feature among the three algorithms is all of them generate distributed numbers. Results from the test cases deduct MAX algorithm to be as efficient as LCG algorithm in terms of distribution and CPU utilization. Additionally, MAX algorithm when tested on generating twenty-bit set of values showed to produce less duplicated values than both MT and LCG algorithms do. However, when generated eight-bit stream values, MAX algorithm showed to produce more duplicated values. This is caused due to "Time function" that responsible for generating the seeds in the algorithm. The bigger the bit-stream is; the less duplication are found in the generated numbers. Because the proposed scheme relies on twenty bits solely, it is highly recommended to use MAX algorithm in the proposed scheme rather than relying on LCG or MT algorithms as it produces less duplicated values. Producing less duplicated values means, it is less likely to have to associated clients with the same MAX algorithm's value. Another significant issue can be noticed in the three test cases, is the low percentage of CPU usage that MAX algorithm needs, compared with MT algorithm.

The reason behind that is because MT algorithm uses more variables than MAX algorithm does, on addition to the bit shifting techniques used by MT algorithm.

Journal of Theoretical and Applied Information Technology
30th November 2016. Vol.93. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.2 Proposed Scheme Testing

To validate and test the robustness of the proposed scheme, CommeView simulator was used to obtain the MAC address of both associated client and the access point together. ALFA wireless adapter was used to find out the precise time needed for the attacker to go through all possible combinations of the twenty bits' MAX value.

Three test cases were conducted by executing an incremental MAX algorithm's value with the Deauthentication in CommeView simulator. The value ranged from 1 to 1048576 (20 bits) as shown in Figure 17 and Figure 18. The attack was carried out and constructed in binary form using CommeView simulator as shown in Figure 17 and Figure 18

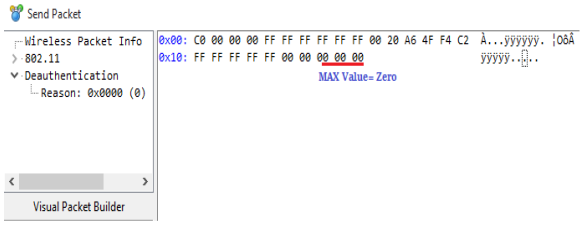

Figure 17: Deauthentication Packet with Smallest MAX algorithm's value

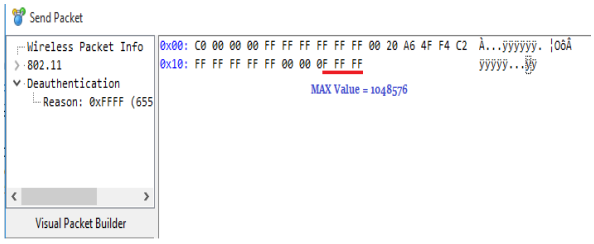

Figure 18: Deauthentication Packet with Biggest MAX algorithm's value

Each test case was run separately, the average time needed to go through all possible combinations was calculated, as results can be shown in Figure 19

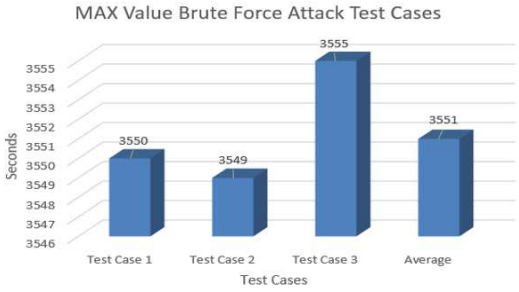

Figure 19: MAX Value Brute Force Test Cases Results

The extracted attack results from the three test cases show the average time needed to brute force MAX algorithm's value is 3551 seconds (Fifty-nine minutes and fifty-one second). This would prevent the attacker from Deauthenticating or Disassociating several clients simultaneously, as each particular associated client has a distinctive value, the attacker must guess. Since MAX algorithm is sent in unencrypted form, there still is still a possibility of intercepting the value and replay it. Wireless 802.11n scheme as mentioned suffers for the lackage of authentication and validation layer. Three test cases were conducted on Wireless 802.11n scheme by executing Deauthentication in CommeView simulator. Each test case was run separately. The average time needed to go through all possible combinations was calculated accordingly. Results of the test cases were extracted as shown in Figure 20.

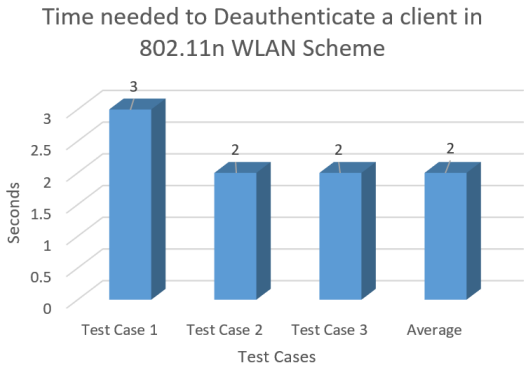

Figure 20: The required Time to Deauthenticate a Client in 802.11n Scheme

In test case 1, results show the time needed to Deauthenticate a client in 802.11n scheme is equivalent to 3 seconds. Meanwhile, on test case 2, the time needed is 2, a second less than the first test case. In the meantime, in test case 3 the time needed is again 2 seconds. The Deauthentication impact is due to the absence of the authentication. However, the extracted attack results from the three test cases indicate the average time needed to Deauthenticate a particular client in 802.11n scheme is 2 seconds. The more random bits are used the slower the attack will be executed. Realistically, the slowest the attack can be executed when the proposed scheme is enforced due to the larger randomized bits are used also the undependability of the scheme on the pre-shared key leads to provide the protection to both unencrypted and encrypted networks.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The impact of using random bits to provide a layer of authentication during the exchange of the management scheme as can be shown in Figure 21

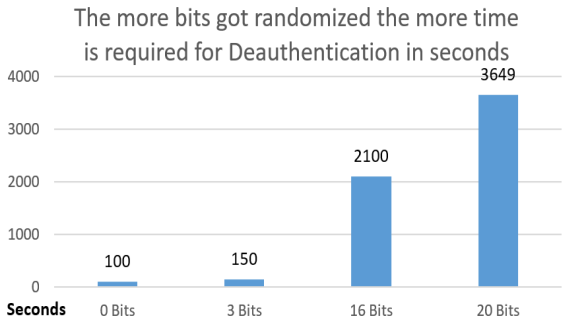

Figure 21: The Impact of Bit Numbers on Authentication Robustness

The more bits have been used in this mechanism, the slower the Deauthentication would be executed. The reason is because of the possibilities the attacker need to go through to guess the exact value. The attacker may tend to execute a man in the middle attack (MITM) in order to intercept MAX algorithm's value during the association response stage, since the value is sent not encrypted, so that to provide protection to unencrypted networks as well as encrypted.

The attacker would then resend or replay the obtained value to the targeted access point to Deauthenticate the impersonated client. Such attack is doable due to the nature of the wireless medium. However, the client will sooner reobtain another issued value within a short time and reestablish a new connection instantly. Subsequently, the attacker would need to repeat the process to successfully re-Deauthenticate the client.

The attacker will normally not to be able to execute a distributed denial of service on multiple clients simultaneously. The reason is because different values are needed to be obtained and sent individually, which considered an infeasible attack.

6. CONCLUSION

In this paper, we presented an enhanced WLAN scheme based on 802.11n. Unlike other WLAN schemes, the scheme showed to sustain the availability factor to the medium in both encrypted and unencrypted modes. However, the adopted method of randomizing the summarized bits would evidently slow down both Deauthentication and Disassociation attacks.

The last twenty bits when randomized using the enhanced version of LCG algorithm (MAX algorithm) would not necessarily require encryption key. This justifies the importance of providing a robustness to unencrypted networks as same as encrypted. MAX algorithm proved to randomize efficiently a value larger than sixteen bits by relying on MAX Algorithm by applying the proposed scheme on both access point and client. The attacker would not be able to execute evil twin attack as the attack cannot be sustained continuously. Additionally, the attacker will not be able Deauthenticate an entire channel or multiple access points and clients at the same time. The scheme will require updating the firmware only as it does not require hardware upgrade. The drawback of the scheme is both reason code and status code will no longer be available so that any disconnection will not be easily diagnostic by network troubleshooters. Providing a seamless and definitive solution to Deauthentication and Disassociation DoS attacks still needs some time to be accomplished on both encrypted and unencrypted networks.

7. FUTURE WORK

Although the proposed scheme has been implemented successfully to slow down both Deauthentication and Disassociation DoS attacks, yet the scheme could also be enhanced to be used to mitigate other types of serious WLAN DoS attacks on addition to spoofing in a more complete and seamless way. More random bits can be used to complicate the attacks for the attacker. Moreover, the distribution and performance of MAX algorithm can be enhanced to generate more efficient values.

REFRENCES

[1] Qachri, N. Comput. Sci. Dept., Univ. Libre de Bruxelles, Brussels, Belgium (2013). On the security of WLAN access points integrated in 4G/LTE architectures. Local & Metropolitan Area Networks (LANMAN).19th IEEE Workshop, pp. 1-6.

[2] IEEE Standard for Information Technology. (2009). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Protected Management Frames IEEE Std. 802.11.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] Agarwal, M., Biswas, S. and Nandi, S., 2015. Advanced stealth man-in-the-middle attack in wpa2 encrypted wi-fi networks. IEEE Communications Letters, 19(4), pp.581-584.

[4] Motorol White Paper. (2011). Can Wireless LAN Denial of Service Attacks Be Prevented? Understanding WLAN DoS Vulnerabilities & Practical Countermeasures.

[5] David Cossa. (2014). The Dangers of Deauthentication Attacks in an Increasingly Wireless World. Iowa State University, 537(), pp.

[6] Nisha Sharma. (2014). Study of DoS Attacks on IEEE 802.11 WLAN and its Prevention/Detection Techniques. International Journal of Engineering Science and Innovative Technology (IJESIT). Vol.3. Issue 3

[7] Stuart Compton and Charles Hornat. (2010). 802.11 Denial of Service Attacks and Mitigation. SANS Institute.

[8] J. Bellardo and S. Savage. (2003). 802.11 Denial of service attacks real vulnerability and practical solutions, proceeding of the 12th USENIX Security Symposium. pp. 15-28.

[9] Joshua Wright and Johny Cash. (2015). Hacking Exposed Wireless: Secrets & solutions.

[10] Thuc D. Nguyen, Duc H. M. Nguye, Bao N. Tran, Hai Vu and Neeraj Mittal. (2012). A Lightweight Solution for Defending Against Deauthentication/Disassociation Attacks on 802.11 Networks. Vietnam National University, Hochiminh City, University of Texas at Dallas, Richardson, TX, USA.

[11] Jie Yang,Yingying, Jennifer Chen and Wade Trappe. (2013). Detection and Localization of Multiple Spoofing Attackers in Wireless Networks. IEEE Transection on Parallel and Distributed System.Vol.24. 1

[12] Frankel, S., Eydt, B., Owens, L. and Scarfone, K., 2007. Establishing wireless robust security networks: a guide to IEEE 802.11 i. National Institute of Standards and Technology.

[13] G. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X.P. Costa, and B. Walke. (2010). The IEEE 802.11 universe. IEEE Communications Magazine.Vol.48. (1). pp 62–70.

[14] CommView Official website - http://www.tamos.com/products/commwifi/

[15] Aircrack-ng tool Official website: https://www.aircrack-ng.org/

[16] Wireshark network analyzer official website: https://www.wireshark.org/

[17] Rastogi, R., Mittal, S. and Shekhar, S., 2015, March. Linear algorithm for Imbricate Cryptography using Pseudo Random Number Generator. In Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on (pp. 89-94). IEEE.

[18] Ping Ding, (2007), Central Manager: A solution to Avoid Denial of Service Attacks for Wireless LAN. International Journal of Network Security. Vol.4. pp.35-44.

[19] Maynak Agrwal, Santosh Biswas et al. (2013). Detection of De-Authentication Denial of Service attack in 802.11 networks. Annual IEEE India Conference (INDICON).