International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 08 - 16, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1002

An APN Authentication Model for a Secure Enterprise Wireless Local Area Network

Robert Mwenda
Department of Computer Science
Chuka University, Kenya

Dr. Lucy Waruguru
Faculty of Computer Science
KCA University, Kenya

Dr. Joseph Mbugua
Department of Information Science
Garissa university, Kenya

Abstract

The Use of Wireless Networks is on the rise and many organizations are deploying WLANs to support their critical business applications. With the rising demand and use of wireless local area networks and the subsequent implementation of these networks by organizations, enterprises have been exposed to a lot of challenges and we have seen an increase in cybercrime and most of these attacks have been launched from wireless networks. Therefore, in this paper we will investigate the security threats and vulnerabilities that are there due to the inherent open nature of wireless communications and come up with an effective defense mechanism that will improve the wireless network security. The open system authentication architecture will be subjected to penetration tests and the results will be compared with those from other schemes like the pre- RSN and RSN methods to select the best model for WLAN authentication. The results inferred that the proposed model of authentication that is achieved by adding a nonce to the access point and therefore referred to as access point nonce (APN) authentication scheme is more effective and offer better security.

Keywords: WLAN, wireless security, APN, Authentication model IEEE 802.11, PMK

1. INTRODUCTION

A WLAN is a network that allows devices to connect and communicate without the use of cables and is heavily reliant on radio frequencies for the purpose of data transmission. The devices that are in communication broadcast data frames over a radio frequency interface. A WLAN uses access points and routers to make a connection between devices. All devices that have WLAN enabled on them and are within range are able to receive data frames. Wireless networks are very popular because they have the advantage of client mobility and thus avoid the cost of cabling that would otherwise be incurred by wired networks. The emergence of mobile devices such as laptops, tablets and smartphones that are portable has contributed largely in making WLAN very popular. The paper will measure and test the strengths of IEEE.802.1X EAP authentication and other variables that will be manipulated under the test-bed experiment. There is an effort to build other models like the Pre-Robust Security network designed by IEEE 802.11(1997) Pre-RSN architecture requires a wired equivalent protocol (WEP) is implemented first. This mechanism was expected to provide reasonable security strength that could match the security of wired network. This security solution seemed to have met its goal but it has been found that the security features are very weak. Even with its weaknesses pre-RSN is widely implemented and deployed by users to allow connectivity to hotspots. Pre-RSN models allow the selection of RC4 as their confidentiality protocol and CR-C32 enciphered as their integrity protocol. Wireless implementers are therefore left with the option of selecting either an open or pre-shared key this makes it limited in scope because it focuses on securing the wireless path between a client device and an access point.

The other model which is the robust security network architecture, provides a system of enhanced authentication mechanism for the access point and client station. It has a session specific key derivation and management framework and it also implements an enhanced data encryption. RSN requires that all the client stations on wirelesses network to be configured with TKIP or CCMP cipher suites and that also the stations create a pre-shared master key (PMK). RSN insists on the selection of EAP method for IEEE 802.1X authentication, but there are many EAP methods with varying weaknesses and strengths. RSN fails by not having a guideline to be followed when selecting an EAP method for IEEE.802.1X authentication and this creates a problem of either having a likelihood of choosing a weak authentication method or even implementing a strong authentication method wrongly. RSN has the limitation of lacking a way of selecting or configuring security of important components.

These previous approaches therefore lack important components and they are not comprehensive enough to address the many security issues that are related to authentication and access control in wireless local area network. Again while the use of these approaches has enabled security implementers choose between suitable and unsuitable authentication methods, none of these approaches has been able to provide a tool that can enable an implementer to visualize the security level that is expected from implementing a set of security features and configurations. The rest of the paper is structured as follows, first we present the literature review, then materials and methods, then we discuss the results obtained from the lab experiments and then discussion and conclusion.

2. RELATED WORK

There have been past efforts by researchers in trying to solve poor implementation of authentication mechanisms and poor access control methods in WLANs. A number of models have been implemented and these are: Pre-Robust Security Network (Pre-RSN) Model was designed by IEEE 802.11(1997). It's the first security implementation approach. Pre-RSN architecture requires a wired equivalent protocol

(WEP) is implemented first. This mechanism was expected to provide reasonable security strength that could match the security of wired network. This security solution seemed to have met its goal but it was later established that the security features are very weak. Even with these weaknesses Pre-RSN WLANs are widely implemented and deployed in organizations like universities to allow users connect to hotspots.

Pre-RSN models allows the selection of RC4 as their confidentiality protocol and CR-C32 enciphered as the integrity protocol that they use. Implementers are left with the choice of selecting from two authentication mechanisms and access control methods; which are open and pre-shared key. It is therefore limited in scope because it focuses on securing the wireless path between a client device and access point.

Robust Security Network (RSN) Architecture this provides a system of enhanced authentication mechanism for the access point and client station. It introduced a session specific key derivation and management framework and it also enhanced data encryption. RSN requirement is that all the client's devices on a wireless Network be configured with TKIP or CCMP cipher suites and they be able to create a pre-shared master key (PMK)

Even though RSN insists on the selection of EAP method for IEE 802.1X authentication, there are many EAP methods with varying weaknesses and strengths. RSN does not have a guideline to be followed when selecting an EAP method for IEEE.801.1X authentication and this creates a possibility of choosing weak authentication method or implementing strong authentication method wrongly. RSN is limited because it lacks a mechanism of selecting/or configuring security features of important components like user databases, client drivers or client utility.

3. MATERIALS AND METHODS

The materials and methods used in this paper include a comprehensive literature search, data extraction, and analysis. The literature search was conducted using various online databases, including Google Scholar, IEE Explore, ACM digital library, and Science Direct.

The inclusion criteria for selecting article for this review paper was that they should be published in peer-reviewed journals, conference proceedings, or book chapters and be related to the wireless security and networks. The exclusion criteria were articles that did not meet the inclusion criteria or were not related to the research question. After conducting the literature search, the articles were screened base on their titles and abstracts. The selected articles were then reviewed in full and data extracted from them. The data extraction process included information on the authors, publication year, research methods, study objectives, key findings and limitations.

The data extracted from the articles was analyzed using a thematic analysis approach.

Data from the selected articles will be extracted using a standardized form that includes the following information: authors(s), year of publication, title, research question, study design, sample size, data sources, data analysis methods, key findings and analysis.

The limitations of this paper include the possibility of missing relevant articles due to the exclusion criteria and the potential bias in the selection and interpretation of the articles. To mitigate these limitations, we used a comparative literature search, screened the article based on strict inclusion criteria, and used a systematic approach to data extraction and analysis.

3.1 The problem formulation

Before setting a penetration testing lab, a lot of considerations must be made to include all the threats to be tested for; this will require some planning. A properly done penetration testing can provide very important information to security implementers about the areas lacking in security within their network. A good penetration testing would use the following process.

1. Reconnaissance- at this stage the attacker gathers as much data about the target network as possible. This would be done by a number of tools and techniques, but it is also possible to obtain information available publicly on the internet.
2. Enumeration-The initial step in attack on the network. This is where the attacker successfully establishes a connection to the target node. At the end of enumeration, the attacker will have obtained important data such as domain name, operating system version, user accounts, access port numbers and many others.
3. Exploitation- at this stage the actual attack based on the information acquired is carried out. The objective being to gain unlimited access to the network if possible.
4. Documentation- the vulnerabilities that were exploited are documented and a record kept.
5. Mitigation- when a solution is found based on vulnerabilities identified is found
6. Documentation- the mitigation steps are recorded and maintained

3.2 Setting up a penetration test-bed

This paper, we will use a test bed that will simulate an enterprise network. A selection of the required hardware and software will be afore mentioned. The section below will discuss this.

3.2.1 Required Resources

Wireless access points. The network to be attacked is a WLAN so the access point is of critical importance in identifying flaws.

- Targets with Wi-FI (Wireless Fidelity) compliant network cards to simulate an ideal enterprise WLAN environment, a number of nodes will connect to an access point to simulate a standard network activity and so they will be required to have a wireless network card on them
- Attack Computer the computer of the attacker will have a wireless network adapter which is able to do sniffing and packet injection. It should also be compatible to kali Linux which will be used to carry out the attack.
- Kali Linux –Kari Linux is a UNIX based operating system used for carrying out penetration tests and digital forensics. The operating system is equipped with all soft wares that are needed to carry out the

tests. It has tools like Air crack, Kismet, N-map, Wire shark, wids.py that are used for reconnaissance and infiltration.

3.2.2 Attacks to be carried out

The following attacks will be carried out. DOS (Denial of Service attack) and in this will use MDK3, a dos tool that is normally included in Kali Linux (Linux) and it will be used to carry out denial of service attacks through de-authentication WPA (WIFI Protected Access) Hacking- attacks against WPA2, which is a protocol that normally secures wireless communication, will be carried out using two tools- the air crack suite and pyrite. These tools will be installed in the back box operating system.

Phishing attacks-in this attack an evil twin access point will be set up and a de-authentication attack will be done and also vulnerable users will be tricked into divulging their password. This paper proposes a method of authentication that is achieved by adding a nonce to the access point and therefore referred to as access point nonce (APN) authentication scheme. This will improve on the existing open system authentication scheme.

3.2.3 Design implementation

A Simulation model, mimicking an enterprise WLAN network has been configured. Access points using WPA2 security, will be tested with different levels of protocol ability. There will be a web server on the network which will be subjected to denial of service attacks.

3.2.4 Attacking WLANs

The WPA2 protocol can have two modes, we focus on WPA-2 PSK (pre-shared key), and WPA enterprise. We will conduct a dictionary attack against WPA2-PSK, and then a brute force attack. However, because of limitations due to resources a full scale brute force attack will not be possible and thus only a proof of concept will be provided.

3.2.5 Attacking WLAN authentication

WPA2-PSK is widely deployed especially in home, and coffee shop networks as the standard authentication scheme. WPA2-PSK authentication is by a key known as PTK (Pairwise Transient Key) that encrypts sessions between the client and access point. The PTK is made up of the pre shared key, and these parameters: SSID (service set identifier), the A Nonce (a random number sent by the AP to the device to connect) the S Nonce (a random integer but generated by the client in response to the A Nonce), the client MAC address and BSSID (Basic service set Identifier) this is called a four-way handshake.

The WPA2 authentication process and the steps involved are as follows:

1. The AP sends an A Nonce to the client when it receives a connection request.
2. The client node sends a S Nonce+ a random integer
3. The AP constructs a GTK (Group Temporal Key) from this, and sends it with another randomly generated integer.
4. The Client responds with an acknowledgement of this value

An attacker eavesdropping on the network can be able to obtain all four parameters mentioned, leaving only pre shared key unknown. A dictionary attack will try a range of words included in a previously compiled list and tries against the captured file till there is a match.

4. WLAN VULNERABILITIES

A WLAN that is seen to be secure must have; confidentiality, integrity availability and access control and authentication. (Sheila et al, 2017) confidentiality ensures that all data frames before and after authentication are not accessed by any entity that is not authorized and integrity ensures that alterations are not made on data frames by entities that have no authority. Availability makes sure that at all times a legitimate client or individual user can access a WLAN resource uninterrupted. Access control prevents client devices or even users from accessing a WLAN resource when they have not been duly authenticated

Authentication proves that the device or individual trying to associate with the AP is who it claims to be (P Sathish, 2017).

For an intruder to launch an attack on a WLAN, they must be near and within the range of the coverage of the access point, unlike in wired networks where an attacker must gain physical entry. The access rights of a client station to the wireless network are denied until proper and secure authentication has taken place. The WLAN must also guarantee that a secure authentication takes place. There are a number of attacks that affect WLANs and the mainly exploit weaknesses in the authentication mechanisms that are in place. These attacks compromise the availability of a WLAN, and its Confidentiality and Integrity of the authentication and access control traffic

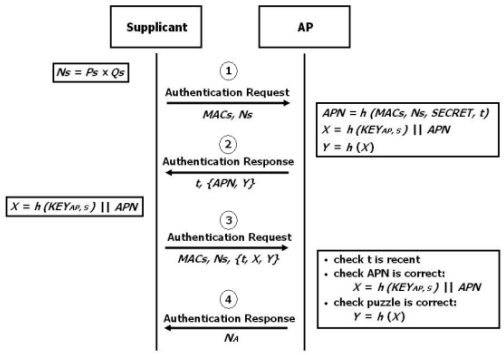
4.1 The APN authentication procedure

This paper has proposed a method of authentication that is achieved by adding a nonce to the access point and therefore referred to as access point nonce (APN) authentication scheme. This will improve on the existing open system authentication scheme. This method is of the assumption that there is existence of a temporary secret key and that this key is shared between the client stations and the AP. the reason why there is this pre shared key between these devices is so that a trust relationship is initially created between the client station and the access point with which it will associate with and with which it will later exchange the identity tokens

The shared key that is generated can only be used for a limited period of time because after the two entities conduct a successful mutual authentication, the key will be dynamically updated. Because of this these dynamic keys do not require to be proof to active attacks and they are made to be easy to implement and very simple

The APN method that is being proposed by the research will use the client machine which is the supplicant will in normal circumstances trigger the APN authentication once the discovery phase is complete and where the MAC address of the target AP has been discovered from the probe responses that the AP sends. the Supplicant will then generate two large primes (Ps and Qs) and then goes forward to compute its identity token (Ns=PsxQs) and from there the client will send the initial authentication request to the AP. to connect the management frame from the client will encapsulate the MAC address of the client and its identity token Ns as shown

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 08 - 16, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1002



4.2 The proposed authentication procedure

Once the target AP receives the authentication request, it will scan to find out if there is an existence of an AP nonce that has been attached to this request. If the request that was received to authenticate from the station lacks the nonce, then the AP will generate a nonce and this nonce will be derived from a cryptographic hash function that is computed using the client station MAC address, its identity token and a secret that can only be known by AP and the current timestamp.

A secret that is known to the AP only and the current time tamp. The secret is very important because it will help prevent the forgery of the nonce by a third party. The reason for this is because it is practically not possible for an attacker to be able to generate a nonce that is acceptable by the AP, while not knowing the value of this secret. Replay attacks are prevented by including a time stamp on the secret. The APN can be generated as shown below

APN=h (MACs Ns, SECRET,t)…….1

The next step is that the AP will bind the nonce and the identity of the client, so that the MAC address of the client cannot be trusted alone since MAC addresses can easily be spoofed. This is done by the AP validating the client by challenging it with a puzzle constructed in such a way that only a legitimate client that knows the shared key(KEYap,s) can easily solve it. This is achieved by the AP fist generating a pre-image through hashing the clients shared key and joining the output with the APN, then a puzzle image Y is computed by hashing the pre image

Pre- image: x=h (KEYaps) ||APN……2

Image y=h(x)……..…..3

The puzzle is meant to be difficult and this is achieved by removing the first 128 bits of X, this means that the access point nonce itself is used as part of the image that is used to form the puzzle but alongside Y. once the puzzle has been successfully constructed, the access point will attach a timestamp and the constructed puzzle to the authentication frame response which is sent to the STA. The authentication response frame contains a field called status code and this code is used to display the results of authentication request that were done previously.

The puzzle challenge will be required by the client station device when making the initial authentication request. If the APN puzzle solution is not attached to this request, the status code is set to a reserved code for that response. When on reserved code mode, it means that an APN puzzle challenge is needed and so the AP will terminate the session and will not store any information

The client station will obtain the puzzle from the probe response and it will go ahead to compute the puzzle solution for the challenge by hashing the shared key. Only legitimate clients know the secret key. To solve the puzzle then, the client is only required to generate the key digest and because of this only a single hash operation is required to be carried out at the client station.

Illegitimate stations that do not have access to the shared key and want to solve the puzzle, must conduct a brute force attack and search all of the 128 bits' key space and this is practically infeasible

The shared key must be refreshed each time the mutual authentication process is complete. The refresh update is done after every 400 milliseconds once the key digest is produced, this action protects against an attacker who manages to discover the 128-bit hash and obtains the key.

Upon the successful solving of the puzzle by the client, it will transmit another authentication request that has the similar identity token and time stamp and the puzzle solution (X and Y).

To ensure that the requests that come from the AP are legitimate the following checks are made:

- **TIME STAMP**

The access point looks at the timestamp attached to the frame to compare with the current time to ensure that it is recent. This checks against replay attacks and any attempt of reusing the puzzle.

- **APN**

Using a computation method, the AP will re compute an APN. For APN to be proved as valid, the computed APN must match with the last 128 bits of X. an APN that is not valid means that the nonce was forged or could also mean that the request was changed. All frames that have their APN as invalid are terminated immediately.

The Access point nonce, allows for the binding of the clients MAV adder together with its identity token. But since the MAC address cannot be trusted in the WLAN for fear of mac address spoofing, this binding requires another layer of protection that will make certain the identity token is mapped to the legitimate identity.

- **Puzzle Verification**

A client is considered legitimate only when they have the correct puzzle solution. In this puzzle the client identity token is bound with the trusted shared key. For this reason, when the client supplies a puzzle solution and the correct identity token that was attached to it, it is verified as a legitimate client.

When the client passes all the three checks above it is then viewed to be a legitimate device and it can be allowed to associate and access the upper layer authentication

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 08 - 16, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1002

5. RESULTS AND ANALYSIS FROM THE LAB EXPERIMENTS

This section will analyses the effect of attacks carried out on WLAN from the simulation. Attacks carried out were, WLAN DoS attacks like De- authentication flooding and association flooding. The results are then briefly presented.

The researcher used MDK3 which is available free on open source to perpetrate the attacks on the access point station.

MDK3 has several flooding modes available as shown by the figure below

The first attack is carried out when de-authentication frames have been spoofed with the access point (AP) real MAC address, are repeatedly sent to the client that is legitimately associated to the AP, from the attacker fake AP

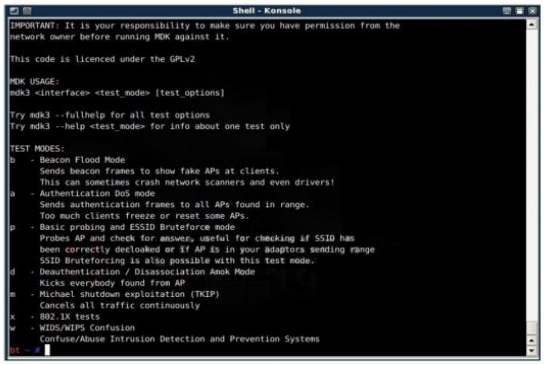


Figure. 1 Example of an image with acceptable resolution

Figure 2. De-authentication Flooding attack**.**

The diagram shown below, shows the de-authentication flooding attack being perpetrated using MDK3. The client MAC addresses are on the left hand column and the MAC addresses of the AP are on the right hand side. All the clients on the network associated to the AP are thrown out of the network and disconnected from the network up until when the attack is halted

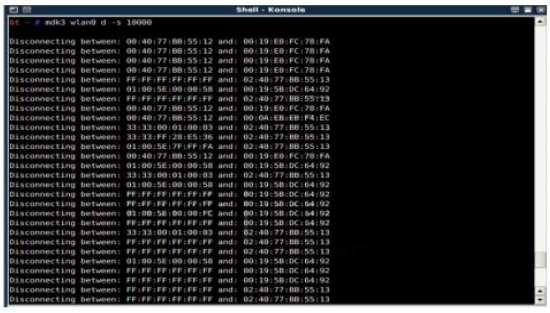
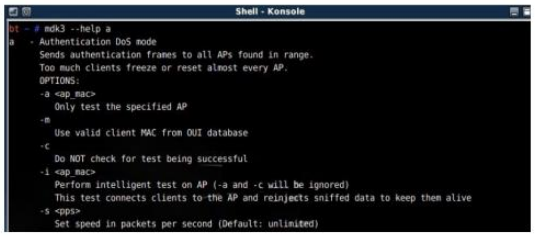


Fig 3. De-authentication/ Disassociation Attack Mode

From this experiment it is depicted that even at a very low rate, for example a transmission of a frame per second flooding, can be able to block the attacked client from associating to the AP. Whenever the client tries to re-establish a connection, the attacker sends another spoofed DE authentication frame that immediately ends the new connection. Because of this activity the throughput of the client drops to the lowest which in this case is zero during the attack duration MDK3 tool is also able to run in an Authentication DoS mode that enables it to generate a series of spoofed authentication requests that are continuously targeted to the AP being attacked. The attacked AP under this circumstance gets too busy processing fake requests in an attempt to provide normal service to legitimate clients. Figure 17 below illustrates the available options in the MDK3 Authentication DoS mode.



Under normal circumstances, when the client request to authenticate, these authentication requests are sent to the specified AP (MAC address shown with the –an option in the shell command line) and when it's at the maximum rate that is possible. A report on the AP status is done after each 500 packets are transmitted. On the launch of the first attack, the AP is still be able to respond to new connections that are legitimate. When the attack is continued for a further five minutes, due to the many clients that are connected, the AP is forced freeze. A reboot of the AP station is then necessary to bring the AP back to its normal operating state even after the attack had long been stopped. Figure 18 below shows the Authentication DoS attack in action

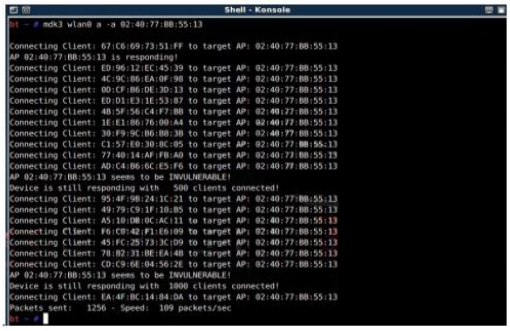


Fig. 4 Authentication DoS in Acton

For the purpose of measuring the effect of attack on the WLAN throughput, continuous TCP packets are generated by the station, and sent to the mobile clients. The moment the client station associated to the AP receives the spoofed de authentication frame, the client is immediately disconnected and it becomes unauthenticated, therefore disconnecting from the network. Figure 19 below shows how the through put of the client under attack remains at zero for whole attack period.

Immediately the attack is stopped, however the throughput returns to normal and the client node is reconnected back to the AP. There is similarity on a pair of results obtained when the network is subjected to authentication flooding, and its shown that during the process of authentication flooding attack (from the10th to 25th second) only a few of the legitimate packet are transmitted against a huge amount of flooding packets. This is the case because when traffic is flooded, it consumes most of the AP resources and this makes the completely very busy trying to respond to spoofed frames.

The AP through put then drops to as little as ten percent (10%)of its normal operating capacity during the fifteen (15) seconds its under attack and its through put remains low for a few seconds after the attack is stopped. When the attack duration is prolonged for a long period of time, the AP will then ultimately freeze and must then must be rebooted. Flooding with association

requests attack using void11, gives results that are similar to the figure below.

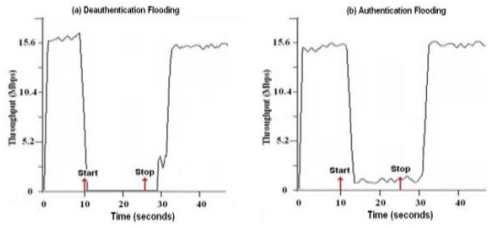
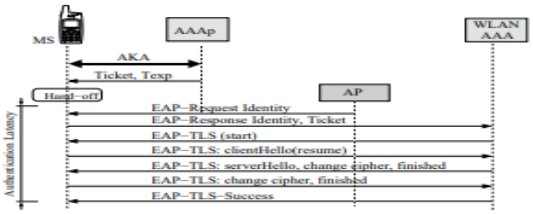


FIG 5. De-authentication and Authentication flooding

From this result, it is clear that a DE authentication flooding attack on WLAN is its most effective attack that causes most damage to the attacked WLANs throughput than damage that can be caused by authentication flooding and association flooding. When WLAN is under attack, the introduced Spoofed DE authentication frames can totally bring down the wireless network such that users who are legitimate are completely denied access to the network. The experiment carried out has demonstrated that it is easy to launch and attack WLANs by subjecting it to DoS attacks and when such WLAN are not properly protected, the WLAN becomes very vulnerable to many attacks and flooding attacks

5.1 Discussion of results

The 802.1x framework put in RSN allows for the exchange of the credentials of the client in a secure way. By this action any unauthorized access to the network is stopped because in this scheme, authentication of the devices is performed before a client is assigned with a network IP address. The standard ensures that the decision to allow authentication are made by the RADIUS server and this removes the need of configuring passwords in every station or Access point. This method therefore allows stations to be authenticates with credentials other than their MAC Address. The credentials of the supplicant (client station) are passed securely to the Access point (authenticator) through a secure EAP method. They are then channeled to the authentication server through EAP that is in RADIUS.



By use of proactive context transfer and ticket forwarding, the network latency is reduced to 36.8% and EAP-TLS latency to 23.1%.

Several previous research studies have proposed that to secure WLANs against DoS attacks, a way of authenticating management frames using the various cryptographic techniques be found. With such solutions there are a number of limitations because the only focus is on improving security with additional cryptographic methods and operations, but they lack the details on the possible overheads to security that come as a result of meeting the required quality of service for real time applications.

These solutions might also not be able to protect the networks against the high rate of flooding attacks and cannot also enable the visualization of the security features and their selection to a safer more, efficient WLAN implementation.

For implementers to enhance security of enterprises WLANs, and mitigate against many attacks like the DoS, a protection link layer, against attacks is necessary. Such protection should happen before the Access point gives any resources that can enable an establishment of a connection.

Denial of Service attacks are able to succeed primarily because they can be carried out before the 802.11x authentication completes. When there is a possibility of a lightweight authentication taking place prior to the process of association, all of the attacks mentioned earlier cannot occur, but the challenge is that to provide this link-layer protection.

It's unfortunate that a majority of the providers of WLAN services and wireless internet service providers do not implement link layer security, but instead relies on proprietary solutions that are based on web authentication.

5.1.1 Comparison with traditional results

A comparison between the three aspects of data confidentiality, Integrity and access control was done on the major kinds of wireless LAN security mechanisms as shown on table below

	WEP	WPA	802.11	APN
Data Confidentiality algorithm used	RC4	TKIP	TKIP, CCMP	TLS,TTLS
Key length	40 bit	128 bit	128 bit	128 bit
Key cycle	Common to all users and static	Dynamic per user per session	Dynamic per user per session	Dynamic per user per session with a time stamp
Key Management	Manual	Automatically distribute and manage	Automatically distribute and manage	Automatically distribute and manage
Security	Low, a lot of defects	Shortcomings high	Introduce AES, high	Introduces a Nonce
Data integrity Algorithm	CRC3	Michael Algorithm MIC	AES algorithm	Large factorization, and security puzzle
Access Control authentication mechanism	None, open authentication, shared key	802.1x PSK	802.1x	802.1x and AP nonce

For the purpose of evaluating the impact of the simulation model use of APN authentication and the use of frame validation on the bandwidth of the access point, we ran iperf so that we can be able to generate the various traffic loads ranging from 2 megabytes per second(mbps) to 54megabytes to a receiving station all the way through to an AP when an APN authentication and frame validation is enabled and when it is not enabled but instead using open system authentication, from the results as illustrated in the graph below fig. 6, indicates that it is possible for the bandwidth of the access point in the test bed can clock up to 18 megabytes per second; when the APN authentication is used and there is no effect on the bandwidth performance and therefore right to say that the performance of the AP is not degraded and also no effect on the maximum bandwidth.

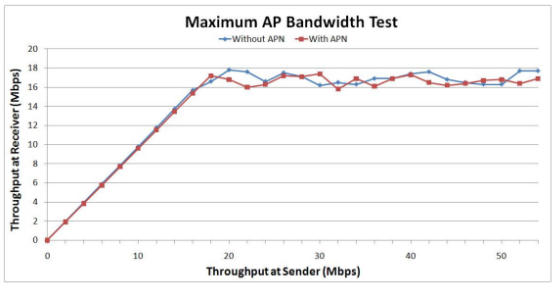


Fig 6 AP bandwidth with and without APN authentication**.**

For the purpose of further evaluating the whether the APN scheme is effective and can offer protection to the WLAN against the many different DoS attacks that are passively targeting the Stations and the access points, at the various stages during the RSNA attempt to establish a connection and using the various tools of attack as earlier mentioned to launch the attacks below.

Attacks carried out before authentication and association

1. Authentication flooding
2. Association flooding

Attacks carried out after securing the communication link

1. De-authentication frame flooding
2. Disassociation fame flooding

Attacks carried the process of authenticating and establishing key

1. Extensible authentication protocol over LAN (EAPOL) –begin flooding
2. Extensible authentication protocol over LAN (EAPOL) –logoff flooding
3. Extensible authentication protocol over LAN (EAPOL) - Failure flooding

The results from experiments that are shown by the table below show that APN can be effective in mitigating from DoS attacks

DoS Attack Type	Without APN Scheme	With APN Scheme
Authentication frame flooding	AP resource depletion	Successful mitigation
Association frame flooding	AP resource depletion	Successful mitigation
Deauthentication frame flooding	STA connectivity loss	Successful mitigation
Disassociation frame flooding	STA connectivity loss	Successful mitigation
EAPOL-Start flooding	AP resource depletion	Successful mitigation
EAPOL-Logoff flooding	STA connectivity loss	Successful mitigation
EAP-Failure flooding	STA connectivity loss	Successful mitigation

To examine how the access points, utilize resources when handling the flooding attacks at high rate, a series of high flooding authentication attack were carried out a rate of 18Mbps and this pushed the AP to its maximum bandwidth capacity. AP central processing unit and the effects on the utilization of the main memory were monitored when DoS flooding is introduced for a period of 10 minutes.

FIG 8 shows how the Access point and the CPU is utilized under the attack of DoS flooding, when the APN authentication is not being used, and the result is that when there is flooding, the load on the CPU is shoots up to almost 80%. This is as a result of the AP is responding to spoofed requests and allocating most of its resources for this purpose. However, when APN authentication scheme is enabled, CPU utilization drops to less than 40% under the same condition. This improved performance and drop in CPU utilization is as a result of the ability that the access point nonce scheme has to identify the attacking spoofed frames, and get rid of them without finding it necessary to store any state information of them. When other flooding schemes are introduced under the same conditions, the same level of load reduction on the CPU was observed.

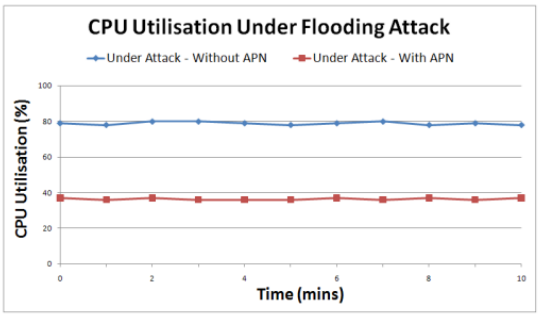


FIG 8. This figure shows the utilization of AP CPU when under a flooding attack

When the AP is not using APN authentication scheme, it is not equipped with the capability of

Identifying spoofed request and it will respond to them and this causes the usage of memory when the WLAN is under authentication flooding attack to continually rise as depicted in the figure 22. On the other hand, when APN authentication

is being used, the utilization of the memory of the AP becomes steady

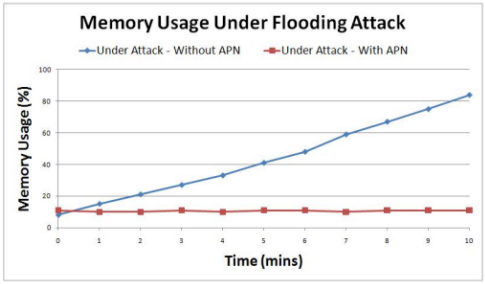


FIG 7. Aps Memory utilization under flooding condition

A de-authentication flooding attack was carried out on the client stations to do an evaluation of effect when stations are under DoS protection. These attacks were launched when stations are configured with APN authentication, and when this scheme is enabled on the AP. The WLAN was attacked with flooding attacks for a period of 15 seconds and as shown in the fig 9 below, when the AP is not configured with APN authentication, and the scheme is not in use, the station gets disconnected immediately on the start of the attack and during this period the AP throughput remains at zero for the entire attack period. On the Introduction of the APN authentication the stations throughput is no longer affected and this is because all the frames that are spoofed are dropped without having an effect on the other legitimate frames

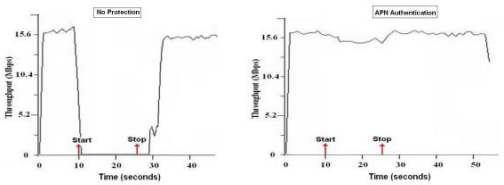


FIG 8 through put under DoS flooding attacks when protected with APN & when WLAN is under no Protection.

6. CONCLUSION AND FUTURE WORK

In this research the security of IEE802.11x was studied and it was found out that there exists a lot of vulnerabilities on the link-layer for DoS attacks that are specific to this standard. Experiments were carried out on the standard to determine and quantify and measure the impact of the DoS attacks that exploit these vulnerabilities. The research further analyzed the mitigation requirements and a number of potential techniques that could prevent network from spoofing and flooding activities. From the results obtained in the experiments carried out in this research, it can be concluded that to address the issue of DoS vulnerabilities, a frame authentication scheme that is lightweight and stateless and that introduces a nonce to the access point, APN authentication is introduced. s. The research recommended that a RSNA be established by the use of an introduction of an APN authentication scheme in preference to the open system authentication. In future since the APN method recommended in this research did not use an intra-domain handoff, that can support APN across multiple domains, we plan to look at this area.

7. REFERENCES

1. Imai, Shin SeongHan and K. Kobara, "Authenticated key exchange for wireless security", *Wireless Communications and Networking Conference 2005 IEEE*, vol. 2, pp. 1180-1186, 13-17 March 2015
2. **.**J.W. Branch, N.L. Petroni, L. Van Doorn and D. Safford, "Autonomic 802.11 wireless LAN security auditing", *Security & Privacy Magazine IEEE Volume 02*, no. 3, pp. 56-65, May-June 2004
3. **.**S.-H. Fang and T. Lin, "Principal component localization in indoor WLAN environments, " IEEE Transactions on Mobile Computing, vol. 11, no. 1, pp. 100-110, 2012
4. S.-H. Fang and T.-N. Lin, "Accurate WLAN indoor localization based on RSS fluctuations modeling, " in Intelligent Signal Processing, pp. 27-30, 26-28 2009.
5. S.-H. Fang, W.-J. Lai, and Y.-C. Liang, "N encryption-based approach for protecting privacy in network-based location systems, " International Conference on Machine Learning and Cybernetics, vol. 1, pp. 377-380, 2017
6. S.-H. Fang, C.-C. Chuang, and C. Wang, "Attack-resistant wireless localization using an inclusive disjunction model, " IEEE Transactions on Communications, vol. 60, no. 5, 2012
7. **1.**L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks", *Proceedings of the 9th ACM conference on Computer and Communication Security*, 2015
8. **.**J. Undercoffer, S. Avancha, A. Joshi and J. Pinkston, "Security for sensor networks", *CADIP Research Symposium*, 2016
9. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and Countermeasures", *Elsevier's Ad Hoc Networks Journal*, vol. 1, no. 2–3, pp. 293-315, 2014
10. H. Chan and A. Perrig, "Security and privacy in sensor networks", *IEEE Journal of Computing*, vol. 36, no. 10, pp. 103-105, Oct. 2003
11. R. Anderson, H. Chan and A. Perrig, "Key infection: smart trust for smart dust", *12th IEEE International Conference on Network Protocols*, Oct 5–8 2004
12. C. Perkins and E. Royer, "Ad hoc on-demand distance vector routing", *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 1999.

International Journal of Computer Applications Technology and Research
Volume 13–Issue 02, 08 - 16, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1302.1002