ISSN: 2278-4632
Vol-12 Issue-05 No.02 May 2022

Design and Security Simulation of Wi-Fi Networks

Mrs. Kukkla Sireesha [1], Mr. Sirikonda Vamshi Krushna [2], Mr. Cheruku Murali Krishna [3]
Department of Computer Science Engineering, Samskruti College of Engineering and Technology

Abstract – Wireless networks milieu is sprouting into the market, and it is the principal way of accessing the internet. Design and security of these networks for an organization need to be considered to ensure mobility is accomplished. In this study simulation results of 802.1X with flexible authentication via secure tunnelling was performed. Opportunistic key caching which is preferred by many vendors was used transit the session information from the posterior access point to the prior access point to minimize the hand-off latency to allow continuous connectivity to avoid poor network performance. The simulation process was applied throughout the write up of this article without setting up the pricy real lab-test. After the successful modelling of the network, the outcome will be transferred to the real-life environment. The network simulator software was used to illustrate roaming while Cisco Packet Tracer was engaged in the layout design of the wireless nodes. This research applies to network administrators and engineers worldwide to save time and the cost of the network appliances.

Index Terms – Simulation, Security, EAP-FAST, 802.1X, EAP Types, WLAN, RADIUS.

1. INTRODUCTION

Wireless is the recommended mobility way of accessing the internet by users. Wi-Fi users spend about 80 percent of their daily activities interacting with wireless devices in various tasks [1]. The availability of wireless fidelity (Wi-Fi) enabled devices has made it a wanting resource. In day-to-day operation of an enterprise, Wi-Fi is deployed to guarantee mobility and broaden the Wi-Fi coverage cell. Several organizations are still employing wired-based networks which do not guarantee mobility to users while on walking from point to point. Wi-Fi. This will ease the overcrowding of users in an organization from contending for positions inside a room with RJ45 cables to access the internet. Dissimilar IEEE 802.11 Task Working Groups continue to develop new standards to meet the need of users regarding the handoff speed, power conservation, security of data and quality of service. Security is a challenging factor in Wireless networks due to its broadcasting nature. In this scenario, the dominant defy is the security of these Wi-Fi networks. Security challenge becomes an unmanageable issue since data propagation is done via electromagnetic waves which bounce over the hackers' vicinity. This salient feature makes these networks insecure unlike in wired schemes where an imposter is demanded to have a cable connectivity to tap data packets. Apparently, IEEE 802.11ac and IEEE 802.11ad WIGig are the modern standards of Wi-Fi-based networks that are sprouting into the market space to provide the 60GHz with backward compatibility with IEEE 802.11n which was predominantly designed to boost Wi-Fi security features. The WLAN IEEE 802.11 protocols were build up as revealed in Figure 1.

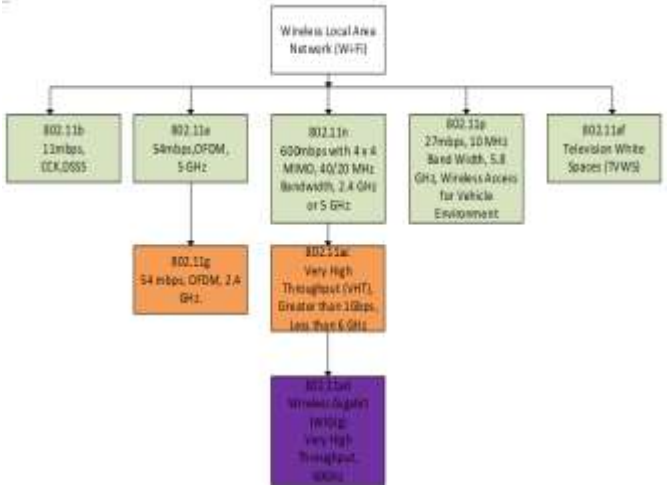

Figure 1 Chronological of IEEE 802.11 Standards for Wi-Fi

Security protocols started to spring into existence in 1999 in the wireless milieu. WEP flawed and its keys recovered [2], [3]. WPA was ratified as an interim protocol to address the problem of WEP. In 2004, Robust Security Network or WPA2 was officially launched to supersede WPA. It is the contemporary protocol used today and all Wi-Fi CERTIFIED apparatus verified as from 2006 are compatible to WPA2 and provides Wi-Fi clients' to access the most advanced and superlative security-based systems. Table 1 below shows the Wi-Fi Alliance proposed security standards protocols

ISSN: 2278-4632
Vol-12 Issue-05 No.02 May 2022

highlighting the comparison of WEP, WPA, and WPA2 salient features.

Standard / Features	WEP	WPA	WPA2
Period of Approval	1999	2003	2004
Encryption/Cipher	Assigns the key manually, scramble shared secret keys by employing Rivest Cipher 4 (RC4) nonentity stream	None linear TKIP- based on RC4 nonentity stream	Counter-Mode with Cipher-Block Chaining Message Authentication-Code Protocol (CCMP) of 128-bit AES block cipher
Integrity of Data	CRC-32	Michael (MIC)	CCM
Size of the keys in bit	40	128	128,192 or 256
Scrambling for Packet's Key	Linear hashing	Mixing Function	Scrambling of the packet is optional
Integrity of the header	None	Michael	CCM
Management of the Encryption Key	No	EAP	EAP
Scheme of Authentication	WEP probe a client by a challenge message	802.1X/EAP authentication	802.1X/EAP authentication

Table 1 A Comparison of Wi-Fi Alliance Security Standards Protocols Salient Features

1.1. EAP Authentication Protocols

Since Wi-Fi Local Area Network (WLAN) security is crucial and EAP types offer a potential improved means of safeguarding the WLAN connection, vendors are expeditiously developing APs with EAP. Table 2 below summarizes innumerable EAP standards for Wi-Fi Alliance Accreditation program.

EAP Policies	EAP-TLS	EAP-TTLS	PEAP	EAP-FAST
Authentication	Yes	Yes	Yes	Yes
Delivery of dynamic Key	Yes	Yes	Yes	Yes
Security for Wi-Fi	Very high	High	Strong use of passwords	Medium to High
Rogue AP Detection	No	No	No	Yes
Vendor	Microsoft	Funk	Microsoft	Cisco
Deployment	Difficult	Adequate	Adequate	Adequate

Table 2 A Summary of EAP Types

1.2. Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP –FAST)

Cisco EAP-FAST proprietary is meant for client-server security structural design to replace LEAP due to its flaws and to offers security as PEAP and EAP-TLS. It is composed of three phases;

Phase 0 - also called Automatic Protected Authentication Credential (PAC) provisioning phase. It is not mandatory since manual provisioning can be used. It provides the end user with PAC to join the network.

Phase 1 - In this phase, ACS and end-user established a secure TLS tunnel based on the user's PAC credentials

Phase 2 - user credentials a securely carried using a sequence of type/length/value (TLV)-encoded information from the supplicant to the AS and vice versa. MS-CHAP, GTC, and TLS are the only inner EAP-FAST types supported.

The Authentication server usually a radius server (Cisco ACS, Funk RADIUS and Microsoft IAS) is used to generate PAC by using the master key and the username of the client device. The components of PAC include:

PAC – Key: Is a 256-bit pre-master secret key used by the client device to attain the TLS tunnel. This key is sturdy entropy of 32-octet keys arbitrarily generated by the AS.

PAC – Opaque: Comprises of PAC's key and peer identity which the server employs to recoup essential information for validating the authentication and of the peer by the server.

PAC – Info: A capricious length-field used to grant the least authority of identity or issuance of the PAC by the specified PAC server. This information is used to determine the renewal of PAC-Key by the AS.

In this study, the interest is in designing a secure enterprise WLAN that uses 802.1X through a RADIUS server using EAP-FAST to enhance mutual authentication in the link layer and physical layer to generate a secure and advanced encryption standard key. The EAP-FAST's PAC is managed dynamically and renewed by the authentication server. The delivery of PAC to the user is either done manually by a storage device or automatically through the air. Cisco Wireless LAN Controllers was preferred to register our access points and Cisco Secure ACS server to stores the Lightweight Directory Access Protocol (LDAP) and RADIUS databases. RADIUS/LDAP will be configured to enable a web page login mechanism. EAP-FAST transmit verification data between the supplicant and the AS. EAP-FAST uses PAC to establish a secure TLS tunnel and a sequence of TLV to encrypt user's authentication during transmission. Figure 2 demonstrates how EAP-FAST messages are interchanged by the supplicant, authenticator, and authentication server.

ISSN: 2278-4632
Vol-12 Issue-05 No.02 May 2022

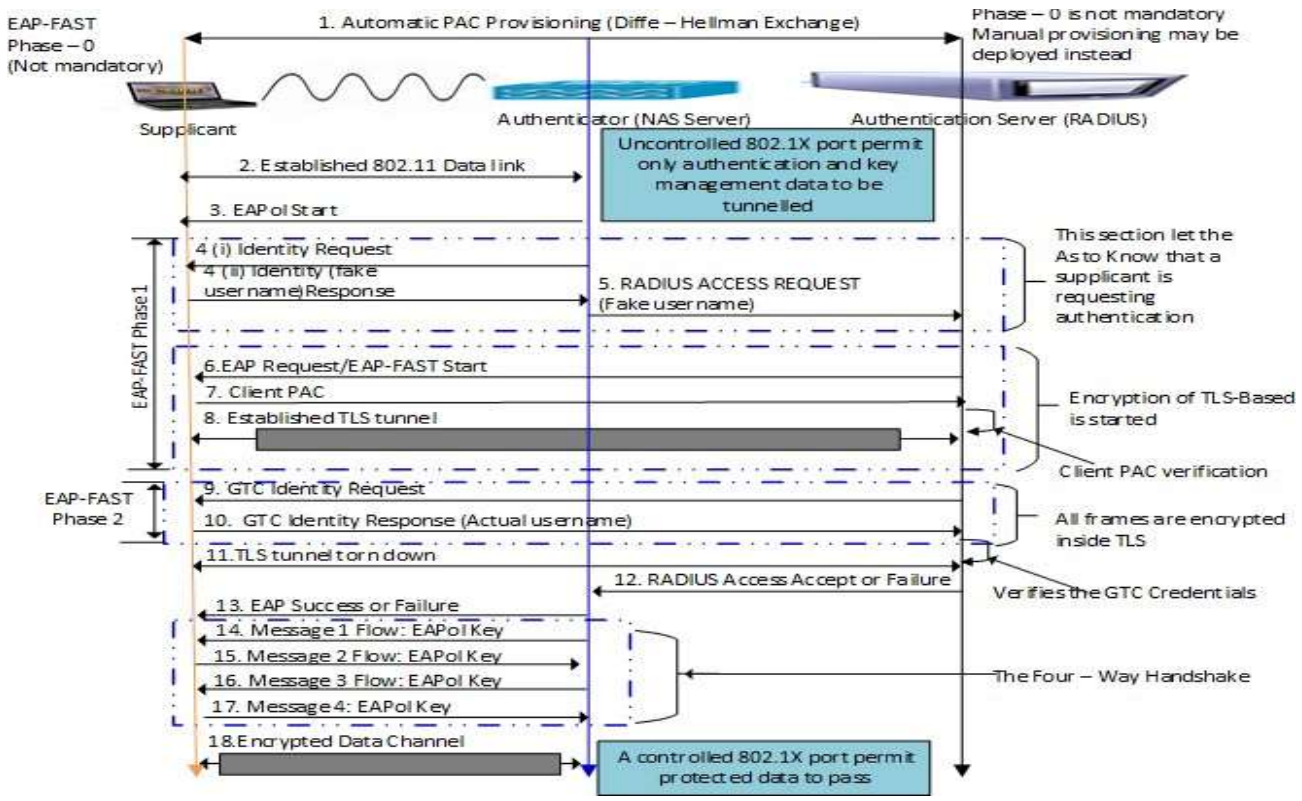

Figure 2 EAP-EAST Messages Exchange for Supplicant, Authenticator (AP) and AS (RADIUS)

1.3. Overview of IEEE 802.1X Authentication Process

The clarification of 802.1X/EAP authentication processes that take place between the supplicant software, the authenticator and the authentication server has been exhausted in Figure 2. For this process to materialize three mandatory processes must take place to open the controlled port to access the internet. These processes include; (a) the open system authentication (OAS), the 802.1X/EAP process, and the 4-way handshake. The subsequent sections 1.4, 1.5 and 1.6 illustrate these procedures.

1.4. OAS

In OAS the authenticator (AP) broadcast it beacons frames at an interval of every 10 seconds. If the wireless client received the beacons frames, the exchange of response and request take place thru un-controlled port as shown in Figure 3.

The OAS is now complete. From this point, if the network does not have any captive portal asking for credentials then the client can surf the network. In this point, IEEE 802.1X standards pop in to bolster the authentication mechanism by alerting the authentication server to close the radio and block the supplicant from accessing the network until the authentication server agrees to open the virtual security port. Once the radio communication port closes, the IEEE 802.1X authentication process begins. In this scenario, it is compulsory that the OAS process is obligatory to prompt IEEE 802.1X authentication process which in turn brings the authenticator into play. Figure 4 outline some necessary steps of 802.1X/EAP authentication scheme.

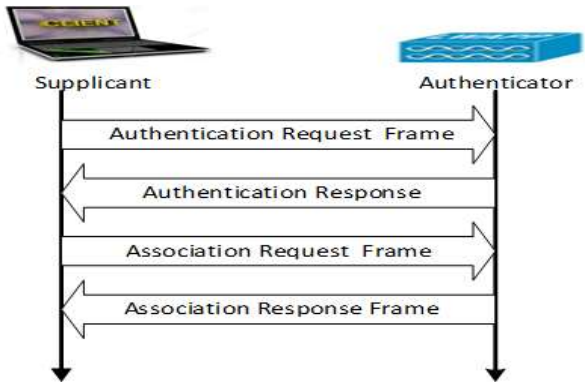

Figure 3 Open Authentication System (OAS)

Once the IEEE 802.1X authentication is accomplished, the Master Key (MK) is worked out at AS and the supplicant. This MK will be not disseminated to all clients in the entire network. It will be availed to the client requesting the service only and previously substantiated, and it will be bound to the entire session.

ISSN: 2278-4632
Vol-12 Issue-05 No.02 May 2022

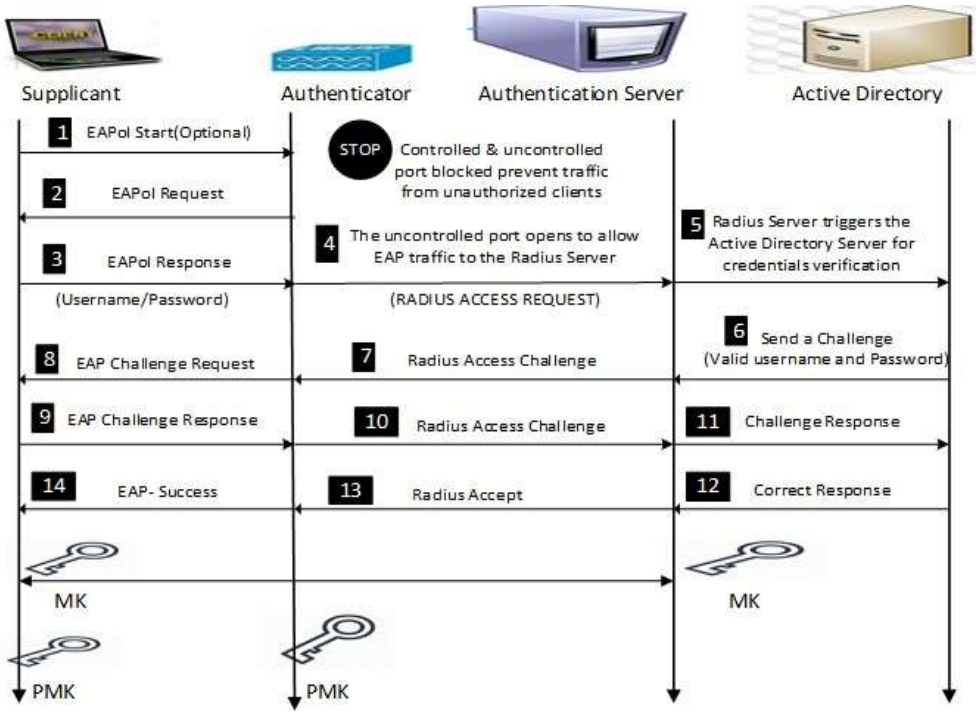

Figure 4 802.1X/EAP Messages Swap

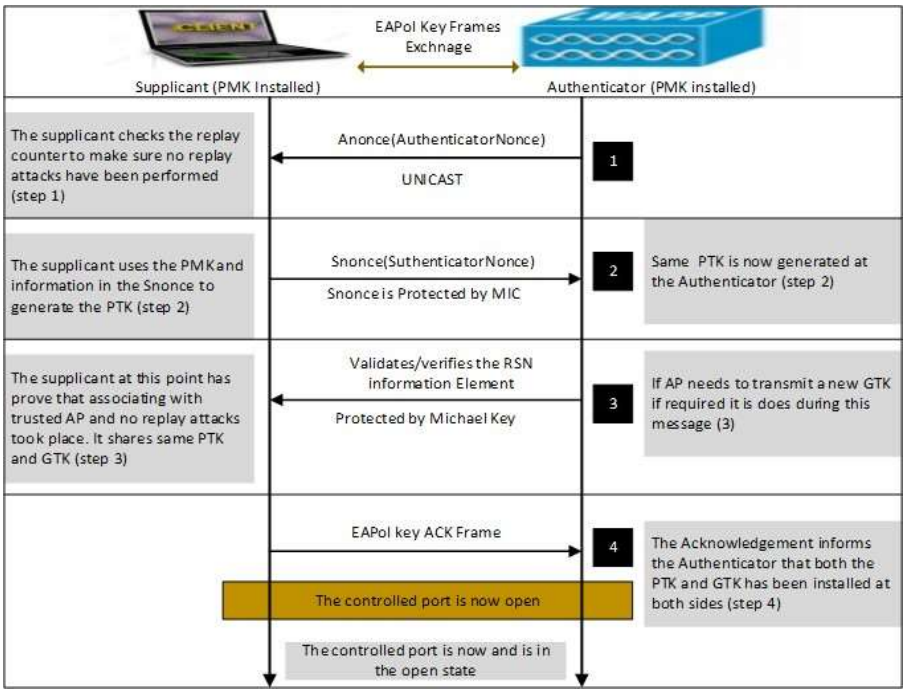

Figure 5: The 4 -Way Handshake Mechanism

The MK key calculated hitherto is used to generate the pairwise master key (PMK) on the side of the supplicant software and authentication server software. The AS distribute the PMK to the authenticator in a distribution system. This PMK generated, will be used in the subsequent process known as the 4-way handshake after a success EAP message. If the authentication

ISSN: 2278-4632
Vol-12 Issue-05 No.02 May 2022

is not fruitful, the process is terminated and loops back to the OAS state. Figure 5 depicts the four-way handshake mechanism.

In the above process, EAP encapsulation over LAN (EAPOL) fundamentally transmit EAP frames from the supplicant to AP directly by a LAN MAC service in four steps as shown in Figure 5. The supplicant employs the Anonce from the Authenticator and PMK to generate the pairwise transient key (PTK) to decrypt and encrypt unicast traffic for this session only. The PTK is not shared amongst the clients but only between the supplicant and the AP sending an association probe. Transmission of this key is by the wired medium system to the destination node to prevent sniffing of the key's packets. Alternatively, the Group-Master Key (GMK) produced is used to calculate group temporal key (GTK) for multicast or broadcast distribution within the administrative domain for multiple clients to obtain a copy.

1.5. Three-Party Mechanism

In the above process, it can be illustrated in a three-part scenario to simplify how the messages were interchanged between the parties involved. In the process the client (supplicant), the security guard (authenticator) and the boss (authentication server). The client wishes to meet the boss, and at the entrance, the guard verifies the client's details such as names by checking the identification cards. After verification and security check-up, the guard notifies the boss of the client's arrival.

The boss inquires from the guard whether an appointment date was booked for that particular client. If the appointment was preserved, the boss orders the guard to grant access to the client. If the appointment is not valid, then permission isdenied.

In this scenario, the guard does not do anything but only passes the information between the client and the boss. This is related to the authenticator whose primary responsibility is to authorize the communication between the supplicant and the AS.

1.6. Major Threats to Wireless Network Security

The threats to networks vary according to the need of the attacker. These attacks can be active or passive. Many Linux-based arsenals are available on the internet as free source codes thus heartening attacks to take place to break confidentiality, integrity, and availability [4]. Table 3 below summarizes some of the attacks imposed by the black hat hackers.

Imposters are taking advantage of wireless networks that have not been fully configured, open authentication or with weak security protocol standards used. They are armed tools and with software that can be downloaded to the internet to sniff and capture packets. They will later analyze the packets to get more information to attack the network. Due to this, right security is superlative when scheming and employing an enterprise Wi-Fi network.

Attacks Category	Illustration
Man-in-the-Middle (MITM) Attack	Imposter dynamically mimics several authorized parties, such as impersonating to be a client to an AP and vice versa. Allows Imposter to capture communications between authenticator and supplicant, to get valid credentials and information
Misappropriation	Imposter steals or creates unsanctioned use of services
Masquerading	Imposter mimics a legitimate user and achieves certain unauthorized rights and roles
Denial of Service	Imposter averts or limits the usual use or management of the networks and its networks' devices
Message Modification	Imposter modifies a legitimate message by obliterating, adding to, varying or reorganizing it
Traffic Analysis	Imposter passively screens transmission to identify communication designs and partakers
Eavesdropping	Imposter passively screens the network communications for information, including login details such as passwords and usernames
Message Replay	Imposter passively screens transmissions and retransmits messages, behaving as if the Imposter was an authorized user.

Table 3 Major Threats against Wireless Network Security

2. RELATED WORK

The main aim of security for wireless networks is to enhance the core principles such as availability, confidentiality,integrity and mutual authentication [5]. Wi-Fi Protected Access 2 (802.11i standards) embraces the use of IEEE 802.1X/EAP for authentication [2], [6]. On the other hand, data encryption and integrity rely AES - CCMP or AES - Galois Counter Mode Protocol (AES - GCMP) for WIGig networks [7]. Virtual private networks (VPN) and IEEE 802.1X/EAP are widely deployed in enterprise's WLAN to boost authentication and access control salient [8]–[10] when configured with authentication, authorization, and accounting (AAA (Triple "A")) servers to monitor traffic and provide guest access. The current standards such as 802.11ac and 802.11ad also adopt the 802.11i security standards. AAA servers such as secure access control server (ACS) to provide the internal database to store login credentials for legitimate users.

EAP-FAST is the current IEEE 802.1X/EAP type deployed widely due to its gain of accepting weak passwords, and digital certificates are optional as detailed in RFC 4851 [11], [12]. This protocol encrypts EAP execution with transport level

ISSN: 2278-4632
Vol-12 Issue-05 No.02 May 2022

security (TLS) tunnel between the client and the servers such as RADIUS or Diameter. EAP-FAST utilizes protected access credentials (PAC) which hoard credentials and data used to guard the authentication process. Parts of the PAC are ciphered by the server and are not observable to other objects. Clients are projected to hoard PACs locally for use throughout authentication mechanism. It is fast that EAP-TLS since it uses symmetric encryption mechanism.

Simulation tools such as Cisco Packet Tracer, Network Simulator and Huawei's enterprise network simulation program (eNSP) are widely network simulators in designing network topology, performance and security in virtual environments that make it easier to adopt it in the actualenvironment [13], [14]. Simulation has been carried at the MAC layer to test its performance regarding handoff to a client roaming in a proximity where several access points exist usingOMNet++ to determine the latency of role transfers between the access points and transfer of session keys to ease rekeying credentials within the APs [15]–[18]. OPNET a commercial tool for Linux has also been used to design secured wireless LANs mesh topology as indicated by [19], [20] to evaluate packets dropped during PING between the devices within the network. Simulation is affordable and also saves time if compared to the real testbed as noted by [21] which extensivelystudied various simulation tools.

Wireless security consideration is needed to protect the wired networks. Also, VLAN should be configured to allowdedicated IP subnet only. If an attacker tries to unplug the authorized device and plug in a rogue device, the port will automatically shut down, thus thwarting the attacker fromaccessing services as well as accessing the networks' configurations [22]. The primary VLANs applied in enterprise/organizations are the medium access control based or port-based to set a user to the particular group of IP subnet [8]. The ports for routers, authentication servers, switches, hubsand APs are the targeted ports for performing the port-based security to achieve authentication and authorization as portrayed in [23].

3. LOGICAL DESIGN OF THE ENTERPRISE WLAN

Figure 6 is a diagrammatical representation of the logicaldesign for the proposed topology for an organization WLAN with six bases. One AP was installed in each base as shown inFigure 6 and parameters illustrated in Table 4.

The following steps were adopted to ensure roaming of clients within the building was achieved without disconnection of the clients by using a WLC web graphical user interface.

1. Construct a similar standard WLAN on both WLC controllers.
2. Configure similar mobility administrative groups on the controllers by interchanging their member MAC Address and member IP address of WLC2 to WLC1 and vice versa. The MAC address and IP Address for WLC2 are 00.1b.d5.69.39.20 and 10.20.1.100 respectively whereas WLC1 are 00.1c.58.89.6c.20and 10.10.1.100 respectively.
3. Confirm virtual interfaces is analogous to both controllers.
4. Configure Access point 1, 2 and 3 to use the controller with service port interface 192.168.1.200/24. Also 3, 4 and 6 to use the same controller with service port management 192.168.1.201/24.

Floor	AP Label	VLAN Name	VLAN IP Subnet
1st	AP1	VLAN10	10.20.1.100/24
2nd	AP2	VLAN20	20.20.1.100/24
3rd	AP3	VLAN30	30.20.1.100/24
4th	AP4	VLAN40	40.20.1.100/24
5th	AP5	VLAN50	50.20.1.100/24
6th	AP6	VLAN60	60.20.1.100/24

Table 4 Simulation Requirements for logical design of an Enterprise WLAN

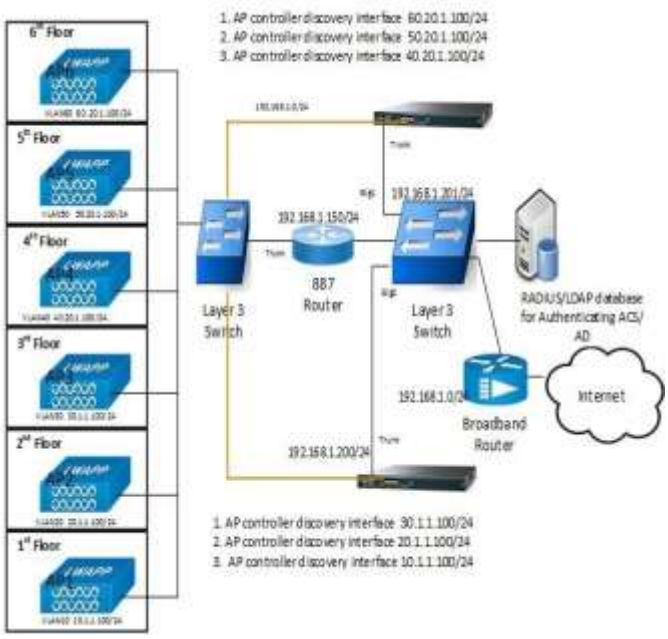

Figure 6 Flat Logical Design of Enterprise WLANs with Six Bases

IEEE in July - 2008, builds upon the IEEE 802.11i security by providing faster and secure key hierarchy based handoffs in microseconds when a client roams from current APs to the target AP. IEEE 802.11K is also required to enable roaming between different bands for instance from 5GHz to 2.4 GHz.

ISSN: 2278-4632
Vol-12 Issue-05 No.02 May 2022

Strong security can be achieved by configuring WLANs using the Cisco WLC as shown in Figure 6 above. The following operations were performed;

1. A VLAN was created on each floor of the building with a WLAN profile name roaming. Layer 3 policy was configured as web policy for authentication.
2. Configured the WLCs for external web login page by redirecting the login window to a web page to inputs fields for required login details.
3. The RADIUS/LDAP servers' databases were configured to query credentials from Active Directory such as the Cisco Secure ACS server capable of providing Triple "A" services as well as storing the login web page which allows users' credentials interface.
4. The LDAP/RADIUS databases were designed for wireless clients to connect to the internet via a redirection login web page.

3.1. Fast Roaming with Opportunistic Key Caching (OKC)

Several vendors are coming up with a non-standard OKC to reduce handover latency for the client to disassociate the old AP and associate with the target AP. This sounds good since the 4-way handshake will be skipped. In this process, the clients decide that it is time for roaming and the AP authenticated to the client sends the PMK to the target AP before the client drops the old AP connectivity. The target AP and the client symmetrically calculate their new PMKs. Upon the re-association, the target AP validates the MAC address of the client sending the request message. If the PMKs match, the client gets connected. Figure 7 shows a screenshot explaining how OKC helps in exchanging cryptographic keys as well as providing a secure roaming environment between the client and the AS.

In Figure 7 James is downloading a video using his TabletPC-PT (mobile node), and he is on 1st Floor and wishes to walk to where Bob is on the 3rd floor and return to his office. For James to continue with video downloading process, roaming feature must be considered during the design of WLAN. The larger circles represent cell coverage for APs **A**, **B** and **C** whereas the smaller circles labelled **X** and **Y** represents the best overlap regions where roaming occurs. For James to continue with the video download, the following measures takes place;

a) OKC forwards the PMK of access point A to access point B which is dependent on the WLAN design and usually triggered by WLC or AP itself using proprietary protocols.

b) Before the client roams, it fast computes a new PMKID by adding current AP B's PMK, the target AP B's MAC address, and the IPAD MAC address. Supplicant launches a re-association request frame to the target AP B with a novel PMKID.

c) On the other hand, Target AP B analyzes at the MAC address of the IPAD that is sending and a re-association request and computes new PMKID using the similar formula. The target AP B replies with a re-association response.

d) Here the four-way handshake of 802.1X/EAP hasbeen avoided and final keys required generated.

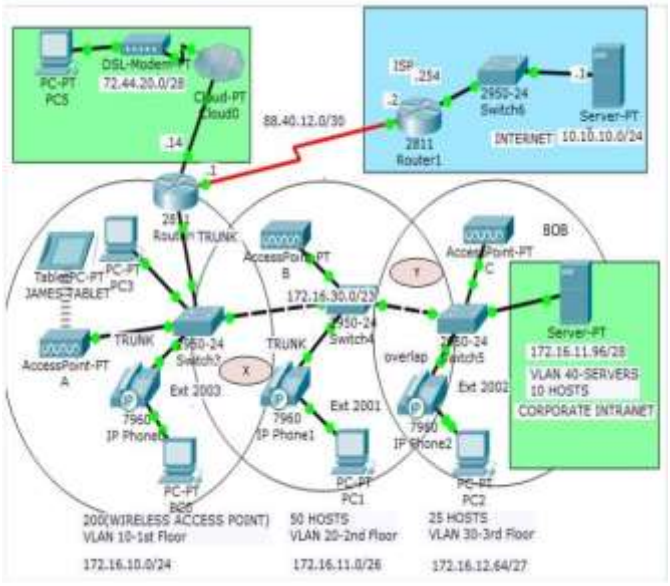

Figure 7 Roaming Description Using OKC

4. SIMULATION OF THE ENTERPRISE WLAN

Network simulation is an essential element in communication engineering. It helps engineers to develop and test network performance [24] before deploying it in the real environment to save time as well as minimizing the cost. Table 5 shows the simulation strictures setup.

Floor	VLAN Name	VLAN IP Address	Number of Clients
1st	VLAN1	172.16.10.0/24	50
2nd	VLAN2	172.16.11.0/26	50
3rd	VLAN3	172.16.11.64/27	50
4th	VLAN4	172.16.11.128/29	50
5th	VLAN5	172.16.11.160/30	50
6th	VLAN6	172.16.11.192/31	50
Intranet Parameters			
	VLAN Name	VLAN IP Address	Number of Host
Internet	VLAN80	176.16.11.96/28	10

Table 5 Simulation Parameters

Figure 8 below shows the screenshot of the simulated parameters using Cisco Packet Tracer (CPT). CPT is a

ISSN: 2278-4632
Vol-12 Issue-05 No.02 May 2022

powerful tool developed for simulating both LAN and Wi-Fi topologies.

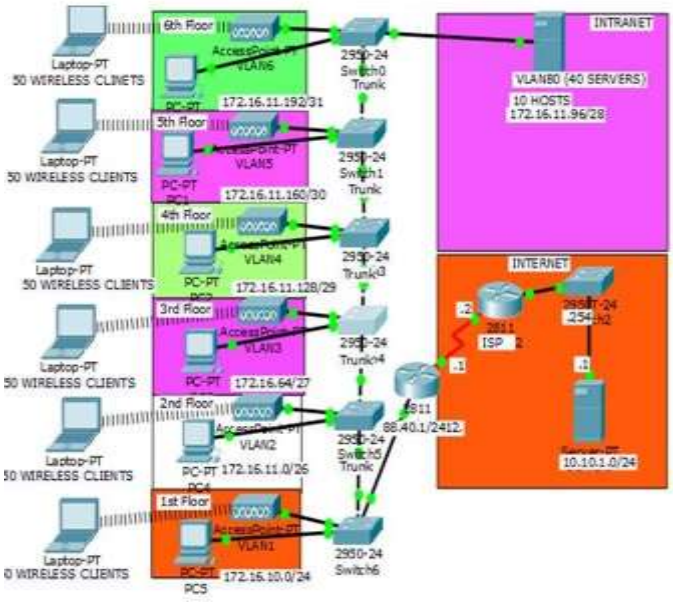

Figure 8 Simulation of the Proposed Enterprise Wi-Fi

In this scenario, six APs were deployed to create the VLAN per each floor for practical purposes. In the intranet side, the Cisco Secure Access Control Server was used to provide triple "A" services. In this server, an installation of RADIUS and LDAP databases was performed to provide clients' login details. In each client's computer, a VPN software was installed to provide a VPN secure tunnel between the APs and the VLAN. An 802.1X/EAP was enabled to establish a secure RADIUS tunnel between the authenticator and the supplicant for messages conveyance.

Users who roam from 6th floor to 1st floor utilizes layer two roaming for VLANs connected to one WLC and layer three roaming for VLANs connected to different WLCs. When users roam within the wireless network cell, their IP addresses remain unchanged whereas WLCs distribute the credentials to the available APs. The trust relationship agreement between the WLCs should be created to ensure that the communication is not interrupted. However, zero packets loss is impossible to prevent during the handoffs mechanism. The credentials remained unchanged throughout the roaming process, henceforth ensuring mobility and secure tunnel within the network to inhibit denial-of-service attacks and crucialretrieval of the key during the 4-way handshake procedure.

When designing a WLAN by simulation process, the following roaming guidelines should be followed to improve the overall network performance;

- An AP can only exchange information with client devices that support its wireless protocol standards.
- All APs ought to have the identical network name to support client roaming.
- All APs and the supplicants should have an analogous security setting to communicate.
- All APs in the similar position must make use of a distinctive and autonomous channel.
- APs that use the same channel should be installed as far away from each other as possible to avoid or reduce potential interference.
- The APs' coverage cell should overlie at a percentage of 15 to 25 to guarantee that there are no fissures in the coverage area to ensure that the roaming client will always have a universal point of handoff that is predefined.

Mobility Simulation Using NS2

In this experiment, two APs and one mobile station were designed for simulation purposes by NS-2 Tcl script which is chiefly an object-oriented translator [25]. AP1 was placed at x=200 and y=100 coordinates. AP2 is placed at x = 600 and y=700 coordinates. The client was associated with AP1 at coordinates of (x=200 and y=150). Dynamic source routing protocol was used [26] since it is on demand [25] routing protocol. The client roams from AP1 to AP2 and stops at coordinates (x=600 and y=500) to be associated with AP2. This simulation was repeated for ten times by changing the source and destination coordinates and the results obtained are shown in Table 6. These results were examinable using the tracegraphv202 graphical user interface to analyze the network information.

Serial Number	Full-Authentication average(seconds)	Handoff Speed (Seconds)
1	5.5	0
2	0.62	0.041
3	0.87	0.052
4	0.83	0.012
5	0.85	0.058
6	0.91	0.03
7	1.2	0.05
8	0.71	0.033
9	1.04	0.021
10	1.12	0.018

Table 6 Full 802.1X/EAP Authentication and Handoff Speed

In the above experiment, serial number 1 with a result of 5.5 seconds indicates the full-authentication process whereas serial numbers 2 -10 indicates the re-authentication processes.

5. RESULTS AND DISCUSSION

In this section, the simulated results are discussed and analyzed. For practical purposes, 6 APs are fixed to cover a six-floor apartment. All APs are linked to a backbone IP Network,

ISSN: 2278-4632
Vol-12 Issue-05 No.02 May 2022

to where a RADIUS server, dynamic host configuration protocol (DHCP) server, domain name system (DNS) server are also attached. DHCP server performs automatic distribution of IP addresses to all devices connected to the network using DHCP Pool.

First, a consideration of the handover speed and full authentication prompt for three models as depicted in Table 7. The practical simulation result of [27] and [28] for EAP-TLS and EAP-ESIM full authentication was used to compare EAP-FAST authentication procedure to show its effectiveness regarding handoff speed.

Authentication / EAP	Full-authentication average Speed in seconds	Handoff speed average (seconds)
EAP-TLS	1.1	0.083
EAP - ESIM	0.876	0.039
EAP-FAST	0.815	0.035

Table 7 Full-Authentication and Handoff Speed Averages for EAP (TLS, ESIM and FAST)

A result of EAP-FAST full authentication speed of (0.815 seconds) was obtained using Network Simulator Version 2 (NS2) which is lower as compared to the previously proofed result of 1.1seconds and 0.876 seconds in the literature of [27] and [28] respectively. These results can be lower than the averaged latency time when tested in the real computing environment. Latency time is reduced by ensuring that an already established shared security key in the current AP is moved to the nearest target AP to reduce latency. This is done by the use of OKC where the PMK is moved to the targeted AP before re-association of the client takes place. OKC PMK caching enabled fast handoff in Wi-Fi networks since the PMK identifier created during full authentication is distributed to the entire APs through the AS. When the client triggers the roaming process, it fast computes the PMKID2 using the original PMKID1. On the other hand, the AP computes the PMKID2 using the original key send by the previous AP. During association, the target AP only checks the MAC address of the client and validates the key. EAP-FAST is fast but not as secure as EAP-TLS.

It is recommended that the latency should be less than 150msec (0.15sec) to support VoIP and video packets transmissions as described in [29]. This implies that the latency must be relatively low. In the simulation experiment, it evident that EAP-FAST speed up the handoff process to provide user's mobility seamlessly.

Mobility was to achieve by creating a trust relationship during the design of the wireless network. In Figure 7, the supplicant does not trust the authenticators in VLAN20 and VLAN30 for context information transfer. This problem was solved by placing WLCs as shown in Figure 6 to eliminate unnecessary re-authentication. In VLAN80, several servers are available for various purposes. For instance, a relational trust via shared secret key exists between AS and AP, the implicit trust coexist between the supplicant and the AP and trust via EAP-FAST co-occur between the AS and the supplicant. RADIUS server works in this scheme was to distribute shared secret keys ahead of the client via RADIUS tunnel.

A brink plane of 25% should be used to allow the client to make the roaming decision when the signal to noise ratio becomes low compared to the threshold. Wireless channel allocation is also vital. Adjacent APs must have a difference of five channels in between them to avoid channel interference as depicted in Figure 7. In simple, Access Point-PT A should be assigned channel one and Access Point-PT B should be assigned channel six.

In handoff process, AP discovery (probing) constituents about 90% of the roaming latency as illustrated by [30]. In the new scheme adopted in this article, AP scanning process was eliminated after an 802.1X/EAP full authentication technique. Thus EAP-FAST reduces the full authentication average by 26% as compared to EAP-TLS and 7% as compared to EAP-SIM. On the other hand, EAP-FAST handoff speed was also reduced by 58% as compared to EAP-TLS and 10% as compared to EAP-SIM. The EAP-FAST authentication protocol is the most appropriate to be deployed in a wireless enterprise environment.

6. CONCLUSION

In this study, an organization WLAN which deployed IEEE 802.1X with EAP-FAST by which digital certificates is not required was developed. EAP-FAST dormancy which is minimal as compared to EAP-TLS and EAP-ESIM was demonstrated. EAP-FAST utilizes the symmetric cryptographic keys which reduce latency. The main ingredient of Wi-Fi network is roaming without rekeying of usernames and password but providing handover login credentials of the user for faster authentication to avoid disruption of services such as video streaming or voice calls. Although EAP-FAST is the new technology from Cisco, it is still subjected to a MITM attack and if enough packets are captured, then it is possible to mount a dictionary attack. This is achieved by making sure the WLCs have been configured to transfer cryptographic keys from the current AP to the new AP before the association so that the two-way handclasp is used instead of the 4-way handclasp which entails numerous messages swap. A WLAN with several VLANs was developed to cover the six floors of the building to enhance handoff speeds to reduce latency. Client's machine is armed with VPN to bolster encryption. eNSP and CTP programs provided components that represent the physical devices which allow working with numerous network devices in a virtual setting. Alongside with this, there will be a more beneficial work to be done because no time wasted is incurred if it was carried out in the laboratory where cabling installations are mandatory to connect various wireless

ISSN: 2278-4632
Vol-12 Issue-05 No.02 May 2022

components with various network topologies. In the simulation, no much cost is required while setting up the virtual environment except minimal causes when purchasing some commercial network simulators if the need arises.

In the future, an extensive research should be done with an ambition of developing an EAP type that is secure and supersedes roaming latency and dictionary attacks imposed by the MITM attacks to scale-up the infrastructure performance as well as improving security. Graphical user interface (GUI) simulators need to be developed to incorporate all the devices used in wireless networks such as WLC whose icons are not available in various network simulators and emulators to appendage the authenticity of simulation.

REFERENCES

[1] B. R. Nishanth, B. Ramakrishnan, and M. Selvi, "Improved Signcryption Algorithm for Information Security in Networks," *Int. J. Comput. Networks Appl.*, vol. 2, no. 3, pp. 151–157, 2015.

[2] J. Bilger, H. Cosand, N. Singh, and J. Xavier, "Security and Legal Implications of Wireless Networks , Protocols , and Devices 2 . Introduction to Wireless Networking," pp. 1–52, 2005.

[3] E. Tews and M. Beck, "Practical attacks against WEP and WPA," *Proc. Second ACM Conf. Wirel. Netw. Secur. - WiSec '09*, pp. 79–83, 2009.

[4] U. Kumar and S. Gambhir, "A Literature Review of Security Threats to Wireless Networks," *Inernational J. Futur. Gener. Commun. Netw.*, vol. 7, no. 4, pp. 25–34, 2014.

[5] A. Chiornita, L. Gheorghe, and D. Rosner, "A practical analysis of EAP authentication methods," *9th RoEduNet IEEE Int. Conf.*, pp. 31–35, 2010.

[6] Q. Qiongfen and L. Chunlin, "On Authentication System Based on 802.1X Protocol in LAN," pp. 2–5, 2010.

[7] J. Lázaro, A. Astarloa, U. Bidarte, J. Jiménez, and A. Zuloaga, "AES-Galois Counter Mode Encryption/Decryption FPGA Core for Industrial and Residential Gigabit Ethernet Communications," in *Proceedings of the 5th International Workshop on Reconfigurable Computing: Architectures, Tools and Applications*, 2009, pp. 312–317.

[8] W. Alliance, "The State of Wi-Fi ® Security," no. January, pp. 3–15, 2012.

[9] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 184–208, 2016.

[10] A. Laing, "The Security Mechanism for IEEE 802.11 Wireless Networks," *SANS Inst.*, vol. 1, no. November, p. 6, 2001.

[11] S. Sotillo, "Extensible Authentication Protocol (EAP) Security Issues," *Syst. Technol. East Carolina Univ.*, pp. 1–6, 2007.

[12] J. Salowey, N. Cam-Winget, D. McGrew, and H. Zhou, "The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST) Status," *Cisco Syst.*, pp. 1–64, 2007.

[13] S. M. Hashimi and A. Güneş, "Performance Evaluation of a Network Using Simulation Tools or Packet Tracer," *IOSR J. Comput. Eng.*, vol. 19, no. 1, pp. 01–05, 2017.

[14] G. F. Riley, "Using Networks Simulation in Classroom Education," *Proceeding 2012 Winter Simul. Conf.*, pp. 2837–2841, 2012.

[15] A. Nayyar and R. Singh, "A Comprehensive Review of Simulation Tools for Wireless Sensor Networks (WSNs)," *J. Wirel. Netw. Commun.*, vol. 5, no. 1, pp. 19–47, 2015.

[16] S. Woon, E. Wu, and A. Sekercioglu, "A Simulation Model of IEEE802.11b for Performance Analysis of Wireless (LAN) Protocols," *Proc. Aust. Telecommun. Networks Appl. Conf.*, pp. 1–4, 2003.

[17] B. Aslam, M. Akhlaq, and S. A. Khan, "IEEE 802 . 11 Wireless Network Simulator Using Verilog," *Proc. 11th WSEAS Int. Conf. Commun.*, vol. 2, pp. 393–398, 2007.

[18] M. A. Catur Bhakti, A. Abdullah, and L. T. Jung, "EAP-based authentication with EAP method selection mechanism," *2007 Int. Conf. Intell. Adv. Syst. ICIAS 2007*, no. December, pp. 393–396, 2007.

[19] K. Yang and J. Ma, "Implementation of IEEE802.1x in OPNET," *2008 Asia Simul. Conf. - 7th Int. Conf. Syst. Simul. Sci. Comput. ICSC 2008*, pp. 1390–1394, 2008.

[20] M. H. Noshy and A. Z. Mahmoud, "Performance Comparison between LTE and WiMAX Based on Link Level Simulation," *Int. J. Comput. Networks Appl.*, vol. 4, no. 5, pp. 121–128, 2017.

[21] J. Pan and R. Jain, "A survey of network simulation tools: Current status and future developments," *Washingt. Univ. St. Louis, Tech. Rep*, pp. 1–13, 2008.

[22] T. Jeffree, P. Congdon, and M. Seaman, *IEEE Standard for Local and Metropolitan area networks - Port-Based network Access Control*, Revision o. New York, USA: IEEE Computer Society, 2010.

[23] H. W. Lee, K. Kim, W. Ryu, and B. S. Lee, "Performance of an efficient performing authentication to obtain access to public wireless LAN with a cache table," *IEEE Int. Conf. Commun.*, vol. 5, no. c, pp. 2376–2381, 2006.

[24] S. T. Chandel and S. Sharma, "Performance Evaluation of IPv4 and IPv6 Routing Protocols on Wired, Wireless and Hybrid Networks," *Int. J. Comput. Networks Appl.*, vol. 3, no. 3, p. 59, 2016.

[25] P. Mittal, "Implementation of a Novel Protocol for Coordination of Nodes in Manet," *Int. J. Comput. Networks Appl.*, vol. 2, no. 2, pp. 99–105, 2015.

[26] S. Zafar, "Throughput and Delay Analysis of AODV , DSDV and DSR Routing Protocols in Mobile Ad Hoc Networks," *Int. J. Comput. Networks Appl.*, vol. 3, no. 2, pp. 25–31, 2016.

[27] C. T. Clancy, A. Mishra, H. M. Shin, J. l Petroni, and Wi. A. Arbaugh, "Proactive Key Distribution Using Neighbor Graphs," *IEEE Wirel. Commun.*, no. February, pp. 26–36, 2004.

[28] X. Liu and A. O. Fapojuwo, "An Efficient Sim-Based Authentication and Key Distribution Method for Wireless LANS," no. May, pp. 1169–1172, 2005.

[29] ITU-T, "Transmission Systems and Media Digital Systems and Networks," *Int. Telecommun. Union*, pp. 1–3, 2003.

[30] S. Shin, A. G. Forte, A. S. Rawat, and H. Schulzrinne, "Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs," *MobiWac '04 Proc. Second Int. Work. Mobil. Manag. Wirel. access Protoc.*, pp. 19–26, 2004.