SECURITY VULNERABILITIES OF WLAN PROTOCOLS: A REVIEW

Abstract:
This study reviews a significant number of known attacks with the security methods that are currently available for wireless local area networks (WLANs). After a thorough review of more than a dozen literature on the security issues affecting WLANs, it was found that the architecture of the WLAN itself has a vulnerability that hackers can exploit, especially the wired equivalent privacy (WEP) protocol. WLAN attacks are a combination of human and technology behavior. Human network compromise is still a serious danger to wireless technology, although new encryption technologies are being developed to counteract threats, they are not enough to address the issues at hand because hackers are constantly coming up with inventive ways to breach networks and undermine the standards. Therefore, it is advised to integrate more sophisticated and pervasive multidimensional AI algorithms at different wireless protocol layers as well as through certified ethical hacking experimentation standards in order to improve detection capabilities, identify unauthorized entry through their behaviors, and safeguard wireless connections and data. Also, Cyber security professionals should take note of this report and be proactive in their search for a sophisticated solution to the current issue.

***Key Word**: WLAN, protocol, Networks, Detection, attacks, encryption, authentication, WEP.*

I. Introduction

Wireless area networks are among the most fascinating and revolutionary technologies that have improved the globe in the last 20 years. People all across the world's behaviors, communication styles, and business orientations have all changed for the better as a result of it. Particularly in an information-driven era, the mobility, comfort, ease of communication, and seamless connectivity have naturally lent themselves as a remarkable and patronizing advantage. Nowadays, wireless local area networks, or WLANs, are the norm for data and mobile communication for the majority of network infrastructures in residences, small offices, and large corporations. This is especially true in situations where short-distance connections are necessary, as well as with the increasing popularity of the internet of things. Radio or infrared signals are used by wireless networks in place over conventional network wires. In order to establish a wireless local area network (WLAN), an access point (AP) or other device that complement an access point placed at the edge of a wired network so that client devices can communicate with one another using a wireless network adapter that performs similarly to a conventional Ethernet adapter. The smooth connectivity made possible by these wireless configurations satisfies the need to maintain a connection to one or more networks while still allowing for mobility. A network of co-located computers or other devices that creates a network using radio waves instead of wires is called a wireless local-area network (WLAN). WLAN gives users mobility and facilitates rapid as well as easy information retrieval. In addition, the rapid expansion and rising demand for mobile devices across several domains, coupled with their necessity for human endeavors, has prompted the development and enhancement of wireless local area networks (WLAN).

Observably, the market for wireless networks has expanded and is currently growing, however, there are persistent worries about its security and this is a significant obstacle. Intentional compromise as well as Hackers' Operations represent a major setback. Numerous studies have been conducted to find solutions to the security challenges, and significant approaches and technologies have been suggested and adopted to mitigate the difficulty yet there is still opportunity for improvement as new vulnerabilities are found. As previously mentioned, a number of inherent security issues and elements that have surfaced in recent decades have tarnished the benefits of wireless local area networks. These elements include how to secure information and guarantee legitimate transmissions; security issues related to transmission are essentially protocol challenges; these protocol issues appear to be quite a closed system, and this is a system that hackers are well-

aware of. Consequently, numerous institutions have incurred significant financial costs to address security challenges in order to prevent their vital data from being compromised, corrupted or a combination of these. Vulnerabilities in wireless local area networks can be caused by a variety of factors. They can be gaps in the cybersecurity measures that allow hackers to exploit them, or they can be defects in the programs used to implement the technology that a hacker can use to destroy the systems. In an effort to take advantage of this infrastructure, hackers are checking systems and networks for vulnerabilities more frequently. Although cyber security experts are using a range of experiments to try and overcome the inherent security issues offered by wireless vulnerabilities, this is a major difficulty for wireless technology businesses. Increasing network security is a continuous effort. In the modern world, everyone is concerned about security, which is why precautions against risk must be taken.

In view of the aforementioned, this paper reviews the main security concerns pertaining to wireless local area networks and offers suggestions for users. It is necessary to give a brief overview of wireless local area networks and evaluate the security risks associated with them.

II. Material And Methods

(a) Wireless Local Area Network and Its Set up

Configurations of computer networks or communication devices that utilize wireless technology to connect across a small geographic region are known as wireless local area networks, or WLANs. These are co-located sets of network connections that do not require cables; they are built similarly to a traditional Ethernet local area network, but they employ wireless access points and interfaces instead of cables or wires. It enables radio wave communication instead of wires for data or other information sharing across a local network of computers or devices. It can extend a wired LAN or, more frequently, replace one. In the contemporary world, wireless LANs currently make up a significant share of the market for local area networks. Many businesses have discovered that in order to meet the needs for mobility, relocation, ad hoc networking, and coverage of hard-to-wire sites, wireless connections are required in addition to regular cable LANs. In locations where wired networks are not practical, wireless networks built on IEEE 802.11 standards can be used. Installation problems with wired networks are possible, which naturally favors wireless network installations, which have shown to be less troublesome than wired networks, especially when adding nodes. According to Larsson & Waller (2003), there is a perceived cost difference between wireless and wired network equipment over time, as well as a cheaper maintenance expense for wireless networks.

A wireless bridge—which connects two or more buildings together when necessary—wireless network interface cards (WNICs), wireless access point(s), and other components are necessary for setting up wireless local area networks (WLANs). A wireless network card is connected to an access point and is typically incorporated into or linked to mobile computing devices. Wireless clients can connect to the wired LAN backbone via an access point, which is essentially a hub. To maintain a coverage area, more than one access points may be required in cell structures of cell phone providers to maintain a coverage area. Wireless bridges, on the other hand, enable high-speed long-range outdoor links between buildings. Based on line-of-sight, wireless bridges are not affected by obstacles such as freeways, railroads, and bodies of water, which can pose a problem for copper and fibre-optic cable connections.

The wireless devices are connected to the wireless LAN access point (AP) by means of their wireless network interface cards (NICs). Any device that must operate in compliance with the 802.11 standard must do so in one of two modes, the Ad hoc mode or the Infrastructure mode[4]. When devices are connected in ad hoc mode, they are able to communicate with each other directly over a small distance. It is sometimes referred to as the IBSS topology and is essentially a peer-to-peer WLAN. The networks do not require any pre-planning or site inspection, and this ad hoc method may

eliminate the need for an access point. Typically, this means that the network is small and only has the capacity to transmit the necessary information.

In order to connect to a different network, the devices in infrastructure mode communicate with one another through access points. The client stations or devices communicate with the access point, which forwards the frames to the selected station, rather than directly connecting with each other. An access point, sometimes referred to as a base station, is linked into the network backbone. The 802.11 standard calls this kind of configuration, which is simple and uses a single access point, a BSS topology. The wired network, wireless computers, and wireless nodes will all communicate with each other through the AP. To exchange data, wireless clients and APs need to establish a connection or association. Data sharing between the two wireless stations is contingent upon their formation of an association. The transmission of frames between WLAN devices is managed by the access point. The access points not only interact with the wired network, but they also manage wireless network traffic in the nearby area[14]. To connect to an access point and join a BSS, a client (device) must wait for messages identifying the access points within its range. In order to connect and exchange data, a client can also use a service set identifier (SSID) to search for or send a request for an access point.

(b) Wireless Local Area Network (WLAN) Security Issues and Vulnerabilities

Network security technology known as wireless local area network security was created to protect networks from intrusions brought about by wireless broadcasts. Due to the many advantages that wireless networks offer, WLAN usage has increased. This has given hackers plenty of chance to take advantage of the vulnerabilities that are there. WLAN signals lack physical boundaries, which makes them easily compromised and open to illegal access to network resources, exposing private and sensitive data. In contrast, wired networks are protected by physical boundaries. WLANs use radio frequency waves or infrared to broadcast messages that carry data, which their clients listen to. Anyone within the signal's range can easily intercept these messages with the right tools. Moreover, wireless technology seems to make it simple for hackers or attackers to keep an eye on the network and compromise the integrity of data sent across it [18].

Numerous security controlling methods, including invisibility, encryption, authentication, and other administrative security rules, have been established in WLANs to address security issues; nonetheless, issues seem to be unsolvable, and more improvements must be made soon. Adoption of WLAN in commercial and corporate settings requires the implementation of extra security measures in order to recognize, stop, and handle different methods and approaches used in security breaches. These security lapses can be caused by both active and passive attacks, such as eavesdropping, denial of service (DoS) attacks, IP and MAC spoofing, session hijacking, and unauthorized access.

To lessen or eliminate WLAN security issues, a number of common authentication techniques and encryption solutions have been developed and deployed in conjunction with other access control mechanisms. These protocols, methods, and practices are thought to offer a reasonable and almost identical level of WLAN security when compared to wired LAN security. However, the question of confidentiality looms large with wireless communications because anyone could potentially be a passive listener to the radio transmission. This poses a risk to the network and could be the catalyst for a hacker or other attacker's attack.

(c) Known Wireless Local Area Network (WLAN) technology attacks

The goal of anyone or hackers who breaches wireless security is to undermine the network's availability, confidentiality, or integrity of data or important information. As was previously noted,

there are two main types of WLAN attacks: active attacks and passive attacks. A logical attacker obtains partial or complete access to the target network, with read/write permissions, unrestricted access to network resources, and the capacity to capture and decrypt encrypted data, in order to logically launch or carry out an attack, especially an active attack with often sadistic intentions. With read access, an attacker can read and intercept network traffic, which enables him to target security protocols like authentication and encryption.

Active Attacks

Malicious attacks that aim to get unauthorized access to network data and modify its contents are known as active attacks. It happens when an attacker alters packets, data streams, files, messages, or attempts to create false or fraudulent information in order to obtain unauthorized access to a resource or network or to interfere with the proper operation of a network service. Such evil behavior causes serious harm to any institution. Since the attacker's true objectives are known, active attacks on wireless networks are the most worrying. The confidentiality and integrity of the organization are threatened by these hostile attacks. These are some of the most typical active attacks, though there are many more types of active attacks:

***Denial-Of-Service (DoS)* or distributed Denial of Service (DDos): These attacks stop authorized users from using their services by sending a large number of authentication requests with erroneous return addresses via the network. The attacker forbids the regular use or administration of communication facilities. Every now and then it attacks a certain section of the network, making it unavailable. DoS attacks can range from physically destroying equipment to disrupting particular network services to a specific person or system, banning a specific individual or group from accessing a service, and flooding a network, thereby prohibiting legitimate network traffic [5]. Denial of service attacks, which are generally hard to identify and prevent, are frequently used to initiate passive attacks that start packet drop attacks. As a result, they are widely used to attack wireless ad hoc networks. An attack known as a Distributed-Denial-of-Service (DDoS) floods the victims with massive volumes of incoming traffic from many sources after infecting multiple computers. DDoS attacks can result in application attacks (which deplete the application layer's resources) and bandwidth assaults (which deliver massive amounts of trash data). DoS in WLANs can take the form of radio frequency (RF) or wireless jamming, 802.11 Beacon Flood, 802.11 Authentication and DE authentication Flood, Virtual carrier-sense assaults, Fake service set identifier (SSID), and access point (AP) theft [15].**

***Masquerading*: This is an active attack where the perpetrator poses as a legitimate user or, worse, assumes the identity of an authorized user in order to obtain unapproved access. The primary causes for this type of attack are stolen login credentials, broken programs, carelessness on the part of users, poor setup of wireless networks, hacking of the authentication system, or manipulation of data by an authorised user who compromises the system and opens a backdoor for a hacker to gain access to the network. Put simply, an attacker impersonates a legal user and gains unauthorized access to wireless networks. This gives the attacker the ability to alter or even delete data, software, network settings, and routing details. Session hijacking is a well-known illustration of a masquerade WLAN attack. The attacker can use the session for any purpose for a long time, and this frequently happens in real-time. Due to 802.11 networks' inability to authenticate the source address, or the Medium Access Control (MAC) address of the frames, masquerading is feasible on WLANs, giving attackers the ability to spoof MAC addresses and take over sessions [13].**

***Replay Attack:* This is a non-real-time exploit that gains access to the WLAN by using real authentication sessions. In order to trick the recipient into performing unauthorized actions like false identification or authentication or a duplicate transaction, the attacker first records the authentication of a session and then replays the authenticated sessions later to obtain network access without changing or interfering with the original session or sessions.**

***Message modification*: An authentic communication is altered by the attacker by deletion, addition, modification, or rearrangement.**

Passive Attacks

Conversely, passive attacks are used to keep an eye out for vulnerabilities and open ports on network systems. The goal of passive attacks is typically to obtain sensitive data about the target system or the system under observation rather than to take direct action on the target system (e.g., changing the message's content or the system itself). The hacker tries to gain access to data that the network is sending out or receiving [20]. Because no information or data is actively altered, a passive attack is the kind that is hardest to identify. To counter or lessen this kind of attack, prevention through the use of encryption mechanisms is essential [6].

Categories of Passive attacks

Especially when it comes to wireless area networks, a number of attacks are classified as passive. These attacks fall into two main categories:

(a) ***Eavesdropping:*** **To monitor the transmission of information content, such as packets and messages, wireless signals between the access point (AP) and the wireless client are monitored and intercepted. With this kind of attack, the attacker can read messages delivered over the network and gain access to network traffic. The payload and the wireless session are passively observed by the attacker. The attacker will eventually be able to decipher the message if it is encrypted. Information about the packets, such as their source, destination, size, quantity, and transmission time, can be discovered by the attacker. More importantly, under the right settings, 802.11 transmission signals can be scanned and detected from great distances using commonly available devices like antennas. Even with effective physical security measures, it is impossible to stop this attack [11].**

(b) ***Traffic Analysis*: Also referred to as packet analysis, this type of passive attack is carried out to gather intelligence by examining transmission signals for communication patterns. This is feasible even in cases when the messages are encrypted and unintelligible, although they are typically similar to messages that are not. Many powerful sniffing tools are utilized to intercept and decipher the target system's communication patterns in order to carry out this kind of assault. For example, a packet sniffer can record network packets and track their performance and trends. Three types of information are obtained by the invaders through traffic analysis. They start by figuring out if there is any network activity going on. Secondly, he or she ascertains the number and placement of access points in the vicinity. The AP transmits its SSID within the wireless network to enable wireless nodes to connect if it is not disabled for broadcasting. A passive sniffer such as Kismet may obtain all network information, including the name, location, and channel used by each access point, even when it is turned down. Lastly, traffic analysis allows the attacker to discover the kind of protocol being used for the transfer as well as the quantity, size, and kind of packets being sent.**

Traffic analysis comes in one or more forms that includes the following:

Foot printing: Foot printing is usually the first step in gathering as much information about a target network especially for a penetration test for vulnerability. Information such as IP address, domain name system information and user's ID and records and so forth. This attack determines the communication load, the number of packets sent and received, the size of the packets, and the source and destination of the packets sent and received.

Spying. When a hacker poses as an authorized network user and switches the network adapter to promiscuous mode in order to intercept all encrypted data traffic on a network, this is the act of passively monitoring network traffic.

War Driving: War Driving is a type of passive attack that is typically carried out from a moving vehicle with the specific goal of using a portable antenna to scan the area for Wi-Fi networks that could be vulnerable. It is feasible to steal or break into an internet connection, therefore this could be a practice run for a future attack on weak Wi-Fi networks.

Dumpster Diving: Like war driving, but with passwords found in trash cans or recycle bins, or information on abandoned equipment accessed by intruders. The data is then utilized to enable unauthorized access to a system or network.

Table .1: Comparison between Active and Passive attacks

S/N	ACTIVE ATTACK	PASSIVE ATTACK
1	Controlling the media or the network physically is necessary for this attack.	Does not physically manage the media; instead, it monitors network communication.
2	Its goal is to compromise system resources while also causing harm to the network.	Monitoring network activity and drawing conclusions from it is its goal. It doesn't change or damage any system resources.
3	The CIA's availability and integrity components are in jeopardy.	Compromises the confidentiality aspect of the CIA.
4	Since it alters information, it is simple to identify and necessitates prevention-focused measures.	It is difficult to detect, thus detection attention is needed.
5	Highly complex and quick completion time to meet its goals.	Has a lengthy duration and less complexity.

Given the severity of WLAN attacks discussed above, it is sufficient to say that WLAN technology has built-in security flaws. Additionally, the interaction between client stations and access points (APs), which require beacon frames to announce their presence, creates opportunities for listening parties to intercept confidential data. This allows the RF signal to escape and makes it accessible to everyone nearby. In an effort to lessen the risks associated with unauthorized access to WLAN signals, new security mechanisms have been introduced, including strong access control protocols and encryption technology; these mechanisms offer a quantifiable level of security, and users are encouraged to implement them. Nevertheless, a constant challenge in the wireless industry is the vulnerability of many of the existing wireless security mechanisms. The section that follows examines some of the security protocols used by WLANs, along with their vulnerabilities and solutions.

(d) Known Wireless Local Area Network (WLAN) Security Protocols, Vulnerabilities and their Solutions

Wireless connections use radio frequency (RF) bandwidths, or free spectrums, that range from 2.4 GHz to 5 GHz and do not require any special licensing. Compactible devices are required to adhere to its specifications in order to use these spectrums. The Institute of Electrical and Electronics Engineers (IEEE) developed the 802.11 series of protocols, which are also known as standards. Over time, 802.11 has evolved into the a, b, i, n, and g protocols. These variations all have different transmission rates, although the original transfer rates for all of them are 1 Mbps for infrared devices and 2 Mbps for those that are still in use today.

Upon the introduction of the 802.11b wireless network standard, the *Wired Equivalent Privacy (WEP)* security features or mechanisms were incorporated. WEP was created in 1999 and was designed to prevent hackers from listening in on wireless communications or networks, from intercepting and decoding wireless messages, and from ever connecting to the network. When WEP was first released, it made use of a common 40-bit encryption key, which is typically iterated using the Rivest Cipher 4 (RC4) algorithm. This meant that the access point (AP) and the wireless client would both use the same key. In order to ensure that only receivers possessing the proper encryption key can decrypt the data and get access to the network, the information transmitted over the signal is encrypted to increase security. Since the key is known on both ends of the communication link, this key approach is static in nature. This clause leaves a gap that allows hackers to access the wireless network. In the end, WEP switched to more secure encryption methods like 128- and 256-bit keys. WEP was developed to offer many levels of security for wireless communication by employing integrity, confidentiality, and authentication. Nevertheless, by falling short of meeting the fundamental security criteria of confidentiality, integrity, and authentication, WEP has revealed certain intrinsic security flaws.

(e) Vulnerabilities of Wired Equivalent Privacy (WEP)

First off, the Integrity Check Value (ICV) of the RC4, a CRC-32 checksum that is used to determine if a frame's contents can be altered while in transit, is vulnerable to compromise because it is not encrypted. During encryption, this value is added at the end of the frame. As the recipient decrypts the packet, the checksum is sent to confirm the contents. As long as the necessary bits in the ICV can be created, the data payload can be altered. This implies that information can be falsified and altered.

Secondly, because all WLAN users share the same static WEP encryption keys. Despite WEP's poor key management technique, cryptanalysis makes it simple to retrieve the encryption keys. Since it takes time and effort to change the keys on every device as a security precaution, a lost or stolen device on the WLAN increases the risk of hacking or other dangers to the wireless connection. Additionally, many users especially those who are unaware of it may not be aware that the WEP function is deactivated by default and that using it is optional. As a result, they may never enable encryption, which can offer them some degree of security.

Third, there are certain restrictions on the Initialization Vector (IV). Because both sides of the communication utilize the same key and it remains constant throughout the session, it is a small, limited length key that is easily sniffed by passive attack using widely accessible software tools [12]. Additionally, after only a few hours of data collecting, an attacker can compromise the encryption of an entire network by repeating initiation routes to decrypt encrypted data without knowing the encryption key.

Fourth, there is no defense against replay attacks offered by WEP. By merely collecting and retransmitting WEP packets, an adversary can create forgeries without changing any data in an

existing packet. One kind of forgery attack that can be used to learn more about the encryption key and the data it protects is replay.

Fifth, authenticated messages are easily falsifiable due to the weakness in the RC4 algorithm used to establish encryption security.

Because WEP-only devices are limited to supporting the 11Mbps 802.11b standard, skilled hackers can now easily gain access to wireless networks. Overall, WEP technology should not be utilized as the only means of protecting wireless networks, as both the original and upgraded WEP processes have drawbacks. Rather, it should be used in tandem with other security technologies to reduce security concerns.

(f) Wired Protected Access (WPA and WPA2)

The wired protected access (WPA) standard was developed with its initial version in 2003 in response to the complaints and flaws of the wired equivalent privacy (WEP). The standard was intended as a temporary security measure and incorporates some WEP characteristics. Similar to WEP, WPA employs the Rivest Cipher 4 (RC4) encryption technology for its keys; however, in contrast to WEP, it allows optional authentication servers and alters the original key for increased security. WPA devices support both the 802.11g and 802.11a wireless protocols and are compatible with WEP. WPA's use of encrypted authentication techniques ought to aid in preventing unauthorized users from joining to the wireless network. Additionally, it employs a dynamic encryption key rather than a straightforward common key. It is a bit challenging to break because of this feature. Temporal key integrity protocol (TKIP) is the term for the process that constantly changes the key. Compared to the static key that is known on both sides of the communication link and used by WEP standards, this key changing mechanism makes it harder for hackers to understand the keys used by the wireless network. In order to ascertain the validity of the network packet and its original source, WPA also incorporates an integrity check. WPA2 uses the Advance Encryption Standard (AES) block cipher and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) in place of TKIP. The WPA's RC4 stream cipher is replaced by AES [20].

(g) Vulnerabilities of Wired protected Access (WPA and WPA2)

Despite being more secure than WEP, WPA and WPA2 are still susceptible to brute-force and dictionary attacks, regardless of the mode in which they are used (Personal or Enterprise mode). WPA2-AES is still thought to be quite secure, however it fails to satisfy the availability check criterion and is susceptible to internal, offline dictionary, and DoS attacks. Furthermore, the management frames are not currently covered by the WPA encryption standard; it only applies to data frames. This indicates that some types of attacks, like replay and message modification assaults, can target management and control frames. Furthermore, WPA2 necessitates increased processing power, a hardware upgrade, or a total hardware replacement, which adds to the expense.

(h) Wired Protected Access (WPA3)

In 2018, the Wi-Fi Alliance developed WPA3, the third generation of the WPA security family, with the goal of both improving upon and addressing the problems of its predecessors. As listed below, WPA3 comes in a variety of types to suit the needs of different Wi-Fi users.

WPA3 Personal: **It employs the Simultaneous Authentication of Equivalence (SAE) encryption technology and is password-based. A quantifiable defense against brute force attacks is offered by this method. By creating keys that are wholly unique for every authentication, WPA3 SAE replaces**

earlier iterations of WPA's pre-shared key (PSK) authentication method. Because of this, adversaries are prevented from launching large-scale assaults on packets that have been captured in an attempt to get past the target network's defenses, and even network members are unable to listen in on one another's communications.

***WPA3-Enterprise*: This mode requires all connections to use the Protected Management Frame (PMF), building upon the robust foundation set by WPA2-Enterprise. This security measure protects against dangerous intrusions such as eavesdropping and honeypot attacks. To better protect the most sensitive data, WPA3 Enterprise has an optional 192-bit mode. A better level of security is offered by this option.**

***Wi-Fi Enhanced Open*: This kind allows unauthenticated data encryption through the use of Opportunistic Wireless Encryption (OWE). Since there is no password required, unauthenticated data encryption maintains the simplicity of public WiFi networks and there is no reason not to enable it. Instead of the 128-bit encryption used in earlier versions, the WPA3 protocol requires GCMP-256 encryption. Using this technique, it is very difficult for one person to listen in on other people's conversations.**

In general, WPA3 is compatible with previous iterations; however, it comes with more guidelines for usage and enhanced security features, like Synchronous Authentication of Equals (SAE), which makes it harder to intercept passwords and prevents users from prying into the private information of others.

(i) Vulnerabilities of Wired Protected Access (WPA3)

WPA 3 is not perfect. Although it is a relatively recent security protocol in the Wi-Fi family, there are some worries regarding its intrinsic vulnerability to cheap hacks, which reveal network passwords and are believed to be caused by protocol program errors. Additionally, not many devices have WPA3 built in, which means that all of them need to be upgraded and would result in higher WLAN expenses. WPA3 remains susceptible to disconnection attacks, and network-based and dragon blood attacks are intercepting traffic in simultaneous authentication of equal public key (SAE-PK) due to a side-channel leak in the dragon fly handshake of WPA3, which also allows offline brute-force attacks [19].

Table .2: Comparison table for WEP, WPA, WPA2, and WPA3 Security Standards

S/N	WIFI SECURITY PROTOCOL	AGORITHM USED	ENCRYPTION SIZE	KEY MANAGEMENT TECHNIQUE
1	WEP	Rivest Cipher (RC4)	64, 128bit or 256 bit key	Static keys
2	WPA	Extended Rivest Cipher (RC4) with Temporal Key Integrity Protocol (TKIP), also supports Extensible Authentication Protocol (EAP)	128-bit, 192 or 256 bit key	Dynamic keys

3	**WPA2**	**Advanced Encryption Standard (AES)**	**128 bit or 256-bit**	**Dynamic keys**
4	**WPA3**	**Simultaneous Authentication of Equals(SAE) using the Galois-Counter Mode protocols (GCMP)**	**192 and 256-bit**	**Dynamic(unique , individualized data encryption)**

III. Result and Discussion

Review of Related Literature

[8] investigated security in wireless networks: vulnerabilities and countermeasures used in Sweden by conducting a case study with a specified target group of Network and Security Managers working at medium and large firms in Sweden. The purpose of the thesis was to illustrate security flaws and how they can seriously affect enterprises and their resources. It also aimed to highlight the need for more wireless security, which would save money in the long run. It was found throughout the examination that there was a lack of knowledge in Sweden about wireless network security. With an emphasis on the Wired Equivalent Privacy (WEP) security protocol, they looked at a number of flaws. They found five known vulnerabilities, including a short Initialization Vector, inadequate RC4 technique utilized in WEP, and issues with key management and size. The authentication messages are easily forged, and the Integrity Check Vector technique is inefficient. WEP was susceptible to WEPCrack codes and war driving attacks. WEPCrack is an open source program for obtaining the secret keys of the WEP protocol and revealing its vulnerabilities. They also mentioned the usage of virtual private networks (VPNs) as an addition to WEP's inadequate encryption. They did, however, suggest that using a single security line was better than combining VPN and WEP security methods.

In a literature review on Wireless LAN Security Threats & Vulnerabilities, [20] talked about the security concerns and vulnerabilities related to the IEEE 802.11 security standard and thoroughly detailed the most common attacks and threats to home and business wireless LAN systems. They contended that because protecting wireless networks is an ongoing and never-ending task, it is a challenging and even impossible undertaking to update information and counter WLAN security threats. They contend that the game of WLAN security will always include striking a balance between allowable risk and protective measures to reduce it. Improved security solutions are a result of recognizing business risk, defending against the most significant and frequent attacks, and following industry best practices. They also asserted that hackers would always research new technologies, look for flaws, and then take advantage of them as there isn't a single effective security solution that has been appropriately developed to handle all security issues in WLANs. They propose adding another layer to WLANs by constructing virtual local area networks (VLAN) as a way to apply security policy in conjunction with authenticating network access control (NAC) in 802.11 specifications. A wireless intrusion detection and prevention system was promoted as a crucial instrument for identifying intrusions and alerting the system administrator to attacks since there are known ways to stop passive sniffing on the network using a standard firewall. Consequently, the deployment of wireless intrusion detection or prevention systems can serve as a watchdog against emerging threats and malevolent conduct.

In their paper titled "The Insecurity of Wireless Networks," [16]) emphasized how vulnerable different encryption algorithms used in wireless local area networks (WLANs), such WEP and WPA/WPA2, are to attack. Additional attacks on these security measures were discussed, along with the ways in which they compromised the availability, integrity, and confidentiality of data, networks, and

messages. They looked into the Beck-Tews, Halvorsen-Haugen, hole 196, chop-chop, and brute force attacks in great detail.

In his 2008 thesis Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures, [11] outlined known WLAN threats, showing that even wireless LANs with WEP, WPA, and WPA2 security mechanisms implemented are susceptible to a range of attacks, from passive to active. In his research, he also suggested that the majority of Wireless LANs would benefit from a combination of security technologies as the best security solution. He also said that risk analysis and vulnerability assessment are essential for creating an enterprise-wide security policy that works and for choosing the right security measures to reduce risks.

In his article Wireless LAN Security problems and Solutions, [4] claimed that human mistake and shoddy network design account for most WLAN security problems. The paper gave careful consideration to the human element since people are both network administrators and users. Intentional data theft and data manipulation by acquaintances or other network users with access to the network are examples of these human errors. Additionally, he discussed some of the potential drawbacks of technological flaws or breaches, which he thinks can be avoided by enacting tight wireless security standards that must be adhered to and by making security solutions easily accessible.

[13] included background information on the advantages of wireless networks over wired Ethernet networks in their analysis of WLAN security issues. They also noted that the need to extend physical boundaries and the evolving nature of wireless connections to larger areas have created opportunities for access by both authorized and unauthorized users, creating a loophole that renders wireless networks less secure than wired networks. Nonetheless, the majority of the WLAN vulnerability growth can be attributed to the initial WEP security standard. On the other hand, these problems can be resolved by creating more secure 802.11x standards and a structure for efficient user authentication and encryption key management. However, depending on their desired level of protection and budget, WLAN users can already protect their networks by putting some of the security protocols' activities into practice.

In his article, [7] compared various tools used for system and wireless network vulnerability detection, along with two methods for network vulnerability scanning: Active Probing and Passive Scanning. The Nessus and OpenVAS tools are well-known for their capacity to handle network plugins and to detect, identify, and analyze false-positives and false-negatives.

War driving is a strategy that [3] utilized to ascertain the availability and security status of a given geolocation. The study was carried out in Northern Cyprus, and the information gathered from the results could be utilized to forecast the future of WLAN security systems, provide recommendations and guidelines for enhancing WLAN networking security in a dynamic setting, and obtain insights into WLAN availability and security. They went on to say that the weak WEP mechanism was the direct cause of a WLAN system break. Although wireless network scanners can circumvent the advantages of changing the network's SSID, the procedures that follow can aid in discouraging casual listeners and bolster the security of the wireless network. They did, however, provide several recommendations for future study aimed at improving security algorithms and at addressing some of the pressing issues related to the present and key parts of rising security concerns in WLANs through the use of artificial intelligence (AI) and machine learning algorithms.

[1]looked at a range of known threats and WLAN security issues. They suggested more research be done there because hackers are interested in it and it's a rapidly growing field of telecommunications. Important information for further WLAN security research was provided by their report. They also made a comparison between traditional human crime and security threats, claiming that since

hackers will always devise new ways to circumvent security measures and will never stop planning, similar efforts to create new technologies that will give network users better security options are needed.

[2] expressed special worry about security issues pertaining to privacy in wireless networks, and they assert that improvements in security technology already in use proceed in tandem with privacy and security issues in wireless networks, often even more quickly. Their findings indicate that the majority of security research minimizes the importance of privacy and security reinforcement and wireless network growth; thus, hackers have consistently targeted this as a means of gaining access to networks. They looked studied a DDoS attack on the well-known code management website GitHub in 2018 to support their conclusions. Mem caching, a technique that includes delivering a false packet to a potential target and then bombarding the server with aggressive traffic, was used to carry out the attack. 129.6 million Data packets were sent to GitHub's servers in this period. One of the biggest DDoS attacks ever seen occurred during this one. But because GitHub has DDoS mitigation software installed, the company's servers were only unavailable for 20 minutes during this attack. This illustrates how a preventative action can help lessen the harm done to an organization if it is implemented. They also mentioned how people's worries about coronavirus information were exploited by phishing efforts to breach the privacy of public sector workers in Mongolia. An email and a word document purporting to be from Mongolia's Ministry of Foreign Affairs were used in the attack. Upon opening the spoof file, malicious code will be installed, giving the hackers remote access to the victim's device and control over it. Hackers have the ability to listen in on the system, steal private information, and launch more attacks. Additionally, they support the development of cyber security specialists' expertise so that they may consistently thwart the growing skill set of cybercriminals by working to uphold a strong system of privacy and security.

Cyber security experts can utilize the Deep Learning-Based Intelligent Mechanism provided by [22] in their investigation of Real-Time Intrusion Detection in Wireless Networks to handle security issues that arise in real time in WLANs. They proposed a timely-based algorithm with a faster detection rate and accurate detection since they were concerned about the poor detection rate of the existing wireless intrusion detection system. They proposed an intrusion detection approach based on Conditional Deep Belief Networks (CBNs) that could identify real-time wireless network intrusions and distinguish attack aspects.

The use of one-dimensional convolutional neural networks (1D-CNN) for threat detection in wireless local area networks was suggested by [9]. They suggested building and deploying a machine learning system that could identify different network risks at the IEEE 802.11 wireless network's MAC layer by analyzing traffic patterns. The suggested 1D-CNN model was found to be comparatively easy to use, extremely fast, and yields superior results. It showed to be more successful in identifying injection, flooding, and impersonation attacks against WLANs and the data they contain.

In a study, [10] examined security threats and challenges that are used to compromise the confidentiality of the client's data and make the network unreliable. They also stated that a number of organizations classify their security vulnerabilities according to perceived models or, occasionally, functional practices. Several other protocols, security challenges, and solutions have been developed through research to address WLAN security issues. There are several other types of security flaws that might cause this, including deception, statistical data fabrication, data loss or theft, web-based hacking, and manipulation by inside staff. They offered a soft computing security algorithm to help in the detection and prevention of network intrusion and other attacks, even though the majority of businesses have solid and easy-to-implement security policies and procedures.

Rather than using the conventional 4-way greeting method, [21] proposed a 3-way handshake model for the 802.11i protocol. They described how their countermeasure may prevent de-authentication, disassociation, and memory/CPU DoS attacks, among other DoS threats.

According to [17], war driving techniques can also be used to evaluate the security and vulnerabilities of residential wireless networks. They also suggest that war driving attacks, which can be exploited for corporate networks, should be given careful consideration.

Based on the literature review and study of WLAN vulnerabilities mentioned above, it seems that there are further attacks that are not covered by the security protocols that have been developed by the Wi-Fi alliance. Even though technology has advanced to address current security vulnerabilities, there are no clear protocols in place to handle human manipulation or network penetration that permits unwanted access. It is also mentioned that the WEP protocol is a single point of failure for all WLANs since it is costly to upgrade all of the hardware to a newer security standard, and WLANs will always be open to attack as long as there is a connection between outdated hardware and cutting-edge security technologies. This knowledge gap necessitates a more proactive approach to WLAN security and vulnerability issues. This study suggests that real-time virtual private network programming be included by manufacturers of wireless devices, and that ethical hacking experimentation be incorporated into the developing of new security standards.

IV. Conclusion

Wireless local area networks (WLANs) have a lot of promise, but security is still a major worry for users, especially large enterprises whose data is a valued asset. Even while known vulnerabilities and wireless security issues seem to be resolved by current security measures, hackers and cybercriminals continue to find ways to exploit these flaws for excessive rewards on a regular basis. There are established methods for getting unwanted access to a wireless network, and wireless signal security will remain a worry as more and more individuals prioritize convenience, flexibility, and mobility.

Passive and active attacks are the two main categories into which these wireless local area network (WLAN) attacks fall. Unless the target has a system in place to monitor and secure machine IDs, no data is modified during a passive attack, and the target is unaware that it has taken place. An active attack modifies or otherwise damages system data and resources, impairing regular system functions. Even though a user is more likely to become aware of an active attack than a passive one, it can be challenging to identify the underlying source of active attacks without appropriate monitoring and identity protection for both people and devices.

There will never be a fully addressed solution to security concerns with wireless networks in today's information-driven and technologically savvy world. Attackers and hackers are always searching for novel approaches to get beyond the security protocols of contemporary wireless networks. Still, there's a lot of space for improvement in order to enhance the wireless connection experience.

Recommendations

A WLAN's security is of utmost importance and ought to be taken into account at every level of the development lifecycle, from initial design and deployment to implementation, upkeep, and monitoring. In light of the aforementioned, the following suggestions are made here:

1. **It is advised that wireless networks and wired networks be kept apart using a specific firewalling system for users with WEP-capable hardware. Because WEP is the most susceptible technique to compromise and was designed to complement wired networks, this**

will help prevent intruders from accessing the entire network. Avoid using WEP security whenever as all possible.

2. **More developments in multidimensional artificial intelligence (AI) algorithms are needed for threat detection in wireless local area networks (WLANs). These algorithms should be integrated into all tiers of the protocols and tested through certified ethical hacking experiments. They should also have a demonstrated detection rate and guaranteed performance level and should be able to provide enhanced data integrity and security for wireless communications.**
3. **The network administrators should ensure that the WLAN client devices and access points (APs) of the organization have adhered to standard security configurations and are always in compliance with the security rules of the organization.**
4. **To measure the overall security of the WLAN, organizations should adopt continuous attack and vulnerability monitoring as well as periodic technical security assessments. This is the main goal of this work, and it can be accomplished by experimentation with ethical hacking.**
5. **In order to increase awareness of security issues and promptly address problems with wireless connection security, risk assessment and preventative techniques should be given top priority. This will lead to the development of a strong and effective security policy that will produce a quantifiable and noticeable level of protection.**
6. **For further security, people should explore the possibilities of employing real-time intrusion detection systems and virtual private networks (VPNs).**

References

[1] **Adamu A. Isah, A. A., & Awal, A. (2022). A review of wireless networks: WLAN Security and Threats. *Advance Journal of Science, Engineering and Technology (Adv. J. Sci. Eng. Tech) 7(7)*, 1-11.**

[2] Alya, H., Ahmad, K., Chuah, C., Yen, Y. & Fatima-tuz, Z., (2020). Security and Privacy Issues in Wireless Networks and Mitigation Methods. *Preprints*. doi:10.20944/preprints

[3] Etta, V.O., Sari, A., Agbotiname, L.I., Piyush, K. S., & Musah, A. (2023). Assessment and Test-case Study of Wi-Fi Security through the Wardriving Technique. *Hindawi Mobile Information Systems, Article ID 9863675,* 1-21. https://doi.org/10.1155/2023/9863675

[4] Feng, P. (2012). Wireless LAN Security Issues and Solutions. *IEEE Symposium on Robotics and Applications Malaysia,* 921-924.

[5] Jean-Paul, A. Yaacoub, A., Hassan N., Noura, A., Ola Salman, B., & Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems 3(1),* 280–308

[6] Kahai, P. & Kahai, S., (2004). Deployment Issues and Security Concerns with Wireless Local Area Networks: The Deployment Experience at a University. *Journal of Applied Business Research, 20(4),* 11-24.

[7] Kashim K. M., (2021). *WLAN Vulnerability Scanning Methodologies*. Middlesex University Mauritius.

[8] Larsson, J & Waller, I. (2003). *Security in wireless networks: Vulnerabilities and Countermeasures.* Thesis Blekinge Institute of Technology

[9] Natkaniec, M. & Bednarz, M. (2023). Wireless Local Area Networks Threat Detection Using 1D-CNN. *Sensors, 23,* 5507. https://doi.org/ 10.3390/s23125507

[10] Nazir R., Asif, A., Kamlesh, K., Shibin, D. & Munwar, A. (2020). Survey on Wireless Network Security. *Computational Methods in Engineering (CIMNE)*, Springer.

[11] Nwabude A. S. (2008). *Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures.* Thesis (MSc), Blekinge Institute of Technology.

[12] Ogletree, T.W. & Soper, M.E., (2006). *Upgrading and Repairing Networks (5th Ed.)*. Que Publishing.

[13] **Prashant, S., Mayank, M. & Barwal, P.N., (2014). Analysis of Security Issues and Their Solutions in Wireless LAN.** ***ICICES*****- 1-21**

[14] **Rafidah, A. H., (2020). Wireless LAN: Security Issues and Solutions/ GIAC Security Essentials Certification (GSEC) Practical Assignment Version 1.4b Option 1** ***SANS Institute*****, 1-20.**

[15] **Ruighaver, A & Tao, Z (2005). Wireless Intrusion Detection: Not as easy as traditional network intrusion detection.** ***IEEE Region 10 Conference, Melbourne, Australia*****, 1-5**

[[6] **Sheldon, F., Weber, J., Yoo, S., & Pan, W. (2012).** ***The Insecurity of Wireless Networks. IEEE Computer Society, 10(4)*****, 54-61.**

[17] **Stimpson, T. Liu, L., Zhang, J., Hill, L. Liu, W. & Zhan, Y., (2012). Assessment of Security and Vulnerability of Home Wireless Networks.** ***IEEE 9th International Conference on Fuzzy Systems and Knowledge Discovery, Chongqing*****, 2133-2137.**

[18] **Suroto, S., (2018). WLAN Security: Threats and Countermeasures.** ***JOIV: International Journal on Informatics Visualization, 2(4)*****, 232-238.**

[19] **Vanhoef, M. (2022). Attacking WPA3: New vulnerabilities & Exploits.** ***HITBSecConf, Singapore*****.**

[20] **Waliullah, W. & Diane G. (2014). Wireless LAN Security Threats & Vulnerabilities: A Literature Review.** ***(IJACSA) International Journal of Advanced Computer Science and Applications, 5(1),*****16-183**

[21] **Wang, L., Srinivasan, B., & Bhattacharjee, N., (2011). Security Analysis and Improvements on WLANs.** ***Journal of Networks,6(3),*** **470-481**

[22] **Yang, L. Li, J. Yin, J. Zhonghao, S., Yufei, Z., & Zhoujun, L., (2020). Real-Time Intrusion Detection in Wireless Network: A Deep Learning-Based Intelligent Mechanism IEEE** ***Access, 8(1),*** **170128-170139. Doi: 10.1109/ACCESS.**