10th International Conference on Control Engineering &Information Technology (CEIT-2025)
Proceedings Book Series –PBS- Vol 23, pp.292-302

# A Survey on Wi-Fi Protocols (WEP, WPA, WPA2 and WPA3)

Sedieg .A Elatab[1] , Azdihar A. Ahmed[2] , Rabee H. Gareeb[3] , Hajer A.Ali[4] , [5]Thiheebah A.Alwaer
[1]*College of Technology Engineering Surman, Libya*
[2]*Sabratha University, Faculty of Engineering, Libya*
[3]*Sabratha University, Economy College, Libya.*
[4]*College of Technology Engineering Surman, Libya*
[2]*Sabratha University, Economy College, Libya.*

[1]it2017cisco@gmail.com
[2]Ezdihar.alwheshe@sabu.edu.ly
[3]rabee@sabu.edu.ly
[4]Hajeramar437@gmail.com
Dehebaalwaer@gmail.com

*Abstract*- Local area networks, which were once only accessible through physical connections, can now integrate and communicate with distant devices via wireless local area networks (WLANs). This technology has fostered a new ecosystem of devices that frequently connect and disconnect, known as roaming. With advancements in technology and the emergence of 5G, Wi-Fi data transmission now offers speeds comparable to Ethernet connections. However, the challenge lies in achieving equivalent security; electrical signals transmitted over copper wires provide greater privacy than data sent through the air. Malicious actors can intercept this traffic, leading to information theft and the creation of deceptive malicious traffic that mimics trusted sources.

Despite the Wi-Fi Alliance's continuous efforts to enhance security protocols, vulnerabilities remain, particularly in the latest WPA3 protocol. This paper surveys the evolution of Wi-Fi security protocols—WEP, WPA, WPA2, and WPA3—highlighting the increased risks of cyberattacks, especially during the COVID-19 pandemic. Notably, WPA3 has been found vulnerable to attacks such as Dragonblood and downgrade attacks, hindering its widespread adoption due to user concerns about security and compatibility with older hardware.

The research problem identified is the existing vulnerabilities within Wi-Fi security protocols, which leave wireless networks open to breaches. The expected outcome is to analyze the current flaws in WPA3, replicate these vulnerabilities, and propose potential countermeasures to enhance wireless network security. In conclusion, while advancements in Wi-Fi security protocols have improved data protection, ongoing vulnerabilities necessitate continuous research and development. A proactive approach is essential to ensure that wireless networks remain secure against emerging threats, underscoring the importance of proper configuration and user awareness in mitigating risks.

*KEYWORDS* - WEP, WPA, WPA2, WPA3.

## I. INTRODUCTION: MOTIVATION AND OBJECTIVES

### *A. The importance and contemporary problems of Wi-Fi security*

Unmanned aerial vehicles (UAVs), smartphones, and the Internet of Things (IoT) are all using the Internet. Because wireless communication is so convenient and effective, even more cutting-edge devices are being created to use WLANs. Recent years have seen a sharp rise in hacking attempts for financial gain and information gathering in proportion to such WLAN usage. A study published in European Societies claims that since the Covid-19 pandemic, there has been a dramatic rise in attempts to compromise cyber-security for particular benefits due to the rise in indoor and telecommuting activities [1]. Hacking techniques like Man-in-the-Middle are used to commit cybercrimes like financial extortion through the acquisition of personal information, fraud based on identity theft, and intellectual property leakage attacks. The security protocols created by the Wi-Fi Alliance can stop most hacking attempts. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA), two


ISSN: 2961-6611

early security protocols, are susceptible to specific attacks, though. The Wi-Fi Alliance has continuously enhanced its security procedures to fend off these particular attacks since discovering them. Notwithstanding the Wi-Fi Alliance's efforts, new methods of taking advantage of protocol implementations are continually being discovered. To put it briefly, security protocols must keep changing as new vulnerabilities are found, or else they run the risk of revealing attack surfaces that could be used to damage network users or devices. Through ongoing research, the Wi-Fi Alliance is fortifying the Wi-Fi security protocol and currently offers the most recent security WPA3 protocol. Although the majority of security flaws in earlier protocols were fixed by the Wi-Fi Alliance, WPA3 is still not a widely used protocol. The main issue is that flaws in this new technology have been found before enough people have used it. People will be reluctant to switch due to vulnerabilities in this newly developed protocol, especially since WPA3 requires older hardware to be upgraded. Upholding the outdated security protocol amounts to settling for a technology that has been rendered inoperable because of a serious security flaw, leaving users open to attacks from outside sources. The quick switch to WPA3 is necessary to address serious flaws in Wi-Fi technology due to the rise in cybercrime.

*B.Technical objectives and Goals*

The Wi-Fi Alliance introduced the WPA3 protocol in 2018. The recently found flaws in the WPA3 protocol will be covered in this paper. The newly identified security flaw was called Dragonblood, a reference to the Dragonfly handshake technique used by WPA3 [2], according to recent research published by Vanhoef (2020).

The following sections make up the structure of this paper. The components of a basic WLAN network and an overview of Wi-Fi security are covered in Section 2. From the standpoint of challenge and solution, Section 3 explains the evolution of the most cutting-edge security protocols available today. Section 4 concludes by offering a conclusion and recommendations for the future course of the study.

## II. Background and Fundamental Concepts

### *A. Introduction to WLAN Technology*

The traditional transmission mode, which uses twisted pair copper wires, is being replaced by the wireless local area network (WLAN), which primarily uses radio frequency (RF) technology to send electromagnetic waves for data transmission. Users can integrate individual devices into basic information transmission structures for communications and data transmission with WLAN networks, including Wi-Fi networks [3]. Due to its notable benefits in terms of data transmission efficacy, security, and efficiency, 802.11n, which has been widely used in many different fields, stands out among many other communication protocols currently in use [4], [5].

### *B. Architecture of WLAN network*

The wireless local area network is generally composed of several parts, including wireless communication medium, devices, terminal stations, and access points as shown in fig.1.

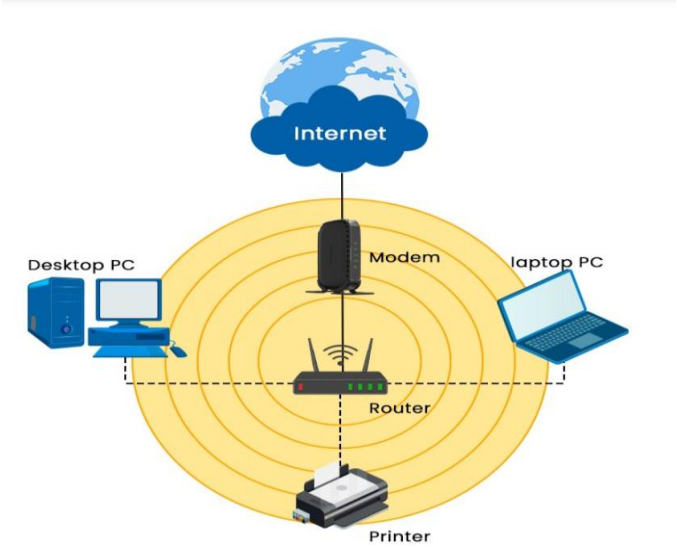


Fig. 1: Topology of a Typical WLAN Network


ISSN: 2961-6611

1. Station (STA)

STA is the basic component of the WLAN network. It generally, refers to the terminal device using the WLAN network, also known as the client, which can be fixed or mobile [5]. This includes mobile phones, computers, and workstations.

2. Access Point (AP)

The function of the AP in the WLAN is similar to that of the base station. The main function is to complete the communication between the STA and the distributed system. APs are often located in the center of BSA (Basic Service Area) and are nodes of wireless and wired networks [5].

3. Wireless Medium (WM)

The wireless medium is the transmission medium used for transmission and communication between the STAs and the AP. For example, the air is a typical WM for radio waves. In addition, the wireless medium can also be defined by the physical layer standard in the WLAN [5].

4. Distributed system (DS)

The physical layer coverage in the wireless local area network determines the communication distance of an access point. The basic service set (BSS) includes AP and the corresponding STA. Multiple BSSs connect through the network to form a network, and the network components used for connection are distributed systems (DS) [5]. As a critical component of WLAN networks, including Wi-Fi networks, the access point mainly plays the role of relaying signals of data communication and transmission in the WLAN networks. For wired networks, applied network architecture and protocols are essentially determined by physical structure and topology which makes it unnecessary to alter their processes, with access points designed to be physically connected to the network [5]. In the contrast, the designed AP technology for wireless networks is required to realize its functions with the characteristics of formatting and error checking calculations for wired and wireless data frames. This allows wireless connection to be capable of transferring, and verifying through calculation, data to the neighbor local area network without inputting the path table and parameters by administrators [3].

## III.BACKGROUND OF WLAN AND WI-FI SECURITY

Modern society's growth and development have provided wireless LANs with many opportunities for advancement, which has led to ongoing improvements in their features and security. Despite its widely used convenience features, there are numerous technical security concerns [6]. Enhancing wireless local area network security is also necessary to meet practical demands for WLAN security and resilience against cyberattacks, as people's awareness of the value of security and safeguarding personal data grows [7]. Network communication security is frequently pushed to the edge of the storm due to numerous instances of security breaches and information leaks that have become more common in recent years. With the development of technology and growing given the focus on contemporary wireless network security measures, these measures have also demonstrated a state of constant development. The security of the technology has consequently naturally grown to a previously unheard-of level [8]. The security methods, mechanisms, and protocols used for Wi-Fi communications have been popular subjects in both academia and industry since Wi-Fi is a common and extensively used wireless local area network communication technology. Since its launch in the year 2000, Wi-Fi technology has undergone four generations of encryption technology [6]. At the same time, Wi-Fi encryption schemes and security protocols have occasionally been shown to have security risks and vulnerabilities [6], [7]. To provide readers with a thorough understanding of Wi-Fi encryption technology and security threats from a technical standpoint, the purpose of this paper is to thoroughly examine and evaluate Wi-Fi security methods, procedures, and protocols at various phases.

## IV.ADVANCED ON THE STATE-OF-THE ART: CHALLENGES AND SOLUTION APPROACHES

Since the initial implementation of Wi-Fi encryption technology and security protocols in 2000, the Wi-Fi Alliance has gone through four technical stages, as indicated by various Wi-Fi security schemes [9]. WPA, WPA2, WPA3, and WEP are all included in this. The four stages can also be divided into weak-key, symmetric-key, and asymmetric-key stages based on the security level and iterative evolution of encryption techniques.


ISSN: 2961-6611

*A.WEP Security Protocol*

An IEEE volunteer group created the encryption algorithm known as WEP [10]. The WEP algorithm's goal is to enable two end users of a WLAN to communicate securely over radio signals. WEP uses two key sizes (40 and 104 bits) and the RC4 algorithm for encryption. A 24-bit Initialization Vector (IV) is added to each key size and sent directly. Once the cipher text and KSA and PRGA processes of RC4 are completed, the plaintext is XORed with the key stream at the transmitter side. The receiver side uses the same key to perform these steps in reverse order. As seen in figures 2-A and 2-B, WEP employs the CRC-32 algorithm to ensure data integrity.

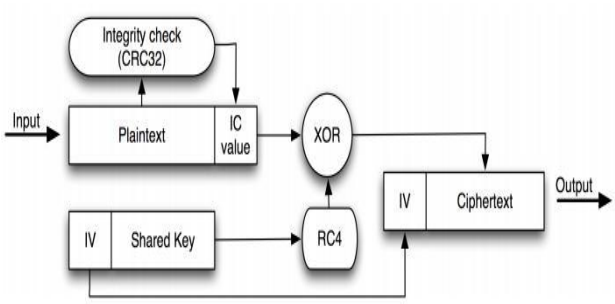


Fig 2-A. WEP Encryption

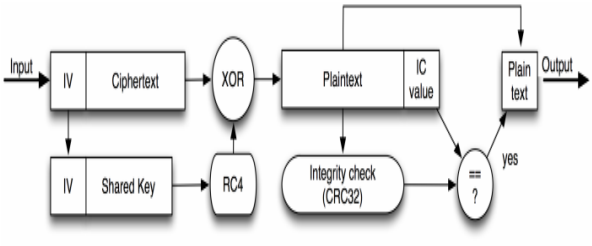


Fig 2-B. WEP Decryption

- *Attacking a WEP network*

WEP is crackable due to certain flaws. Along with the encrypted packet, the IV is transmitted in plaintext. Therefore, anyone can easily learn the first three characters or the secret key by sniffing this information out of the airwave. During the initial iterations of their algorithms, the PRGA and the KSA both divulge information. If the other two values are known, XOR is a straightforward procedure that can be used to infer any unknown value. B is the byte of the secret key that is being cracked, and the format is (B + 3, 255, x).

We must collect a large number of initialization vectors (IVs) in order to successfully crack a wireless AP's real-world WEP key. These IVs are usually not generated very quickly by normal network traffic. If you are patient, you could theoretically listen to the network traffic and save enough IVs to crack the WEP key. However, to expedite the process, we employ a technique known as injection in this work. Injection entails having the AP quickly resend a chosen set of packets. This enables us to quickly record a large number of IVs. We can use a large number of IVs that we have captured to figure out the WEP key. WEP cracking in practice can be shown with ease using programs like Aircrack.

Aircrack [7] contains four main utilities, used in the four attack phases that take place to recover the key:

1. airmon-ng : starts/stops the wireless network card in monitor mode .
2. airodump-ng: wireless sniffing tool used to discover WEP enabled network and capture raw 802.11 frames.
3. aireplay-ng : generates and injects packets into the network (not necessary in WEP cracking).
4. aircrack-ng- WEP key cracker using collected unique IVs.

*Procedure for Cracking WEP as shown in figures from 3 to 7 :*

1. airmon-ng start wlan0

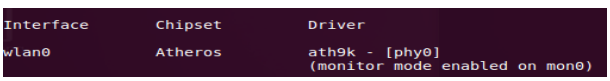


Fig 3: Snapshot output airmon-ng


ISSN: 2961-6611

2. airodump-ng –w testwep mon0

Here, testwep is the file name where packets are captured. Copy the bssid of the access point.

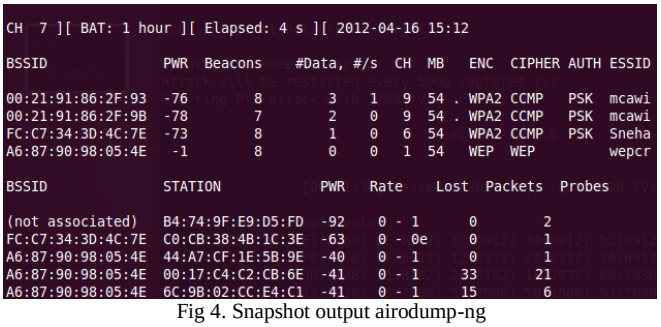


Fig 4. Snapshot output airodump-ng

3. Now check the access point channel and again restart the monitoring on this channel.

airmon-ng stop mon0

airmon-ng stop wlan0

airmon-ng start wlan0 6

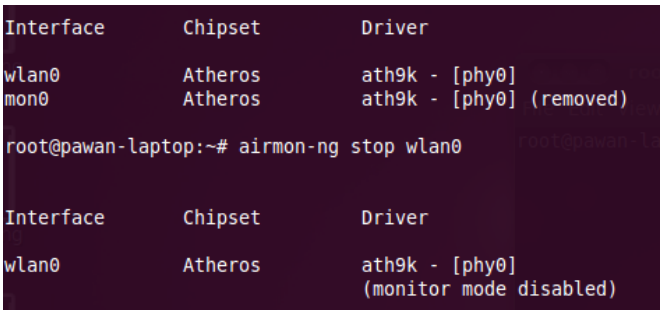


Fig 5. Snapshot output airmon-ng. i.e stopping.

4. airodump-ng –w testwep - - channel 6 mon0

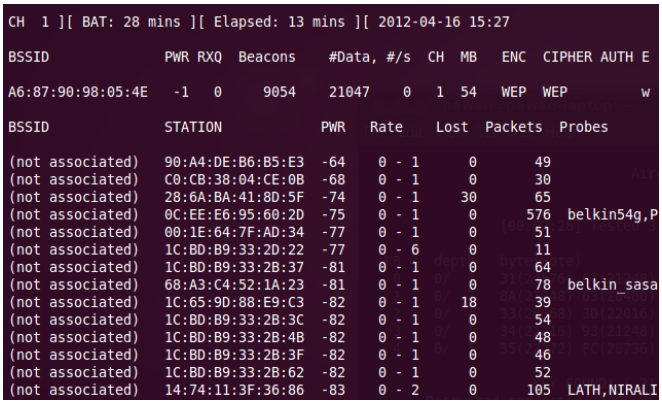


Fig 6. Snapshot output airodump-ng. i.e restart the interface on channel 6


ISSN: 2961-6611

5. Aircrack-ng –l testwep.cap

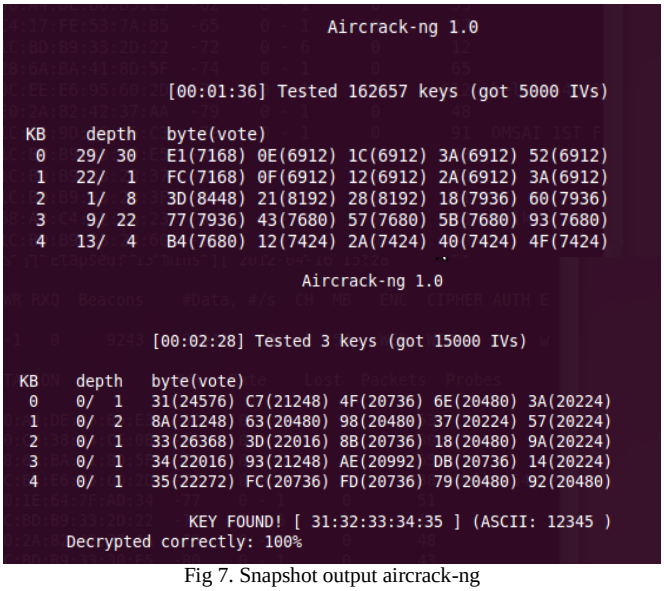

Fig 7. Snapshot output aircrack-ng

***Test Results:***
Security Mechanism: WEP (40 bit)
Time Required: 15-20 min
Mode: Adhoc.
Beacon frames:10000
IV's captured: 15000
Result: Successful.

- *WEP WEAKNESSES:* [3], [4]

- WEP does not prevent forgery of packets.
- WEP does not prevent replay attacks. An attacker can simply record and replay packets as desired and they will be accepted as legitimate.
- WEP uses RC4 improperly. The keys used are very weak, and can be brute-forced on standard computers in hours to minutes, using freely available software.
- WEP reuses initialization vectors. A variety of available cryptanalytic methods can decrypt data without knowing the encryption key.
- WEP allows an attacker to undetectably modify a message without knowing the encryption key.
- Key management is lacking.

*B.WPA security protocol*

WPA-TKIP was created to address the flaws in the WEP encryption scheme by introducing a number of new security features, such as the TKIP sequence counter (TSC) and message integrity check (MIC). Considering the stability of the Wi-Fi inventory market at the time, this was offered based on WEP encryption hardware with software updates [12]. Before the session is encrypted, the sequence count is added, the first round of encryption processing is completed, and the message retrieval information is extracted using the Michael calculation module. This technique can successfully lower the possibility of security breaches and stop message manipulation [13]. More precisely, if the message is altered or changed while being


ISSN: 2961-6611

transmitted phase, the extracted message is decrypted during message decoding in order to retrieve the information. The message itself will not be the same as the counter information. As a result, the recipient will quickly discover that the message has been altered or replaced [12]. In addition to introducing a 4-way handshake mechanism to distinguish between the user's network key and the session key, the WPA-TKIP encryption technology was the first to use pre-shared key (PSK) mechanisms [12]. WPA-TKIP's master key is a 512-bit key that can be divided into five groups for encryption, verification, and message integrity checking [13]. WPA-TKIP's session encryption scheme was derived from the RC4 encryption algorithm, which was used in WEP [14]. This design's initial goal was to satisfy the inventory market's need for Wi-Fi products, modules, and chips that are more secure. The Wi-Fi-enabled devices that are currently on the market did not become outdated by simply updating the encryption scheme with software upgrades because the hardware requirements of WPA encryption technology and protocol are comparable to those of WEP [12]. The WPA-TKIP encryption architecture's security level and handshake process design significantly outperformed the WEP encryption scheme. However, because RC4's encryption operation module is so simple, it is unable to successfully stop brute force attacks, such as preshared key traversal of password dictionary attacks [11].

### *C.WPA2 security protocol*

The Wi-Fi Alliance introduced WPA2 technology to the world in 2006 and used it as a wireless LAN encryption solution. The WPA2 encryption scheme encrypts the message using the AES encryption scheme instead of the RC4 encryption method. The most secure symmetric key encryption algorithm developed at the close of the $20^{th}$ century and the start of the $21^{st}$ was AES [11]. The WPA2 encryption technique divides the message subject into data blocks first, and then it performs several rounds of interleaving nonlinear encryption operations using the corresponding key array [15]. WPA2 encryption requires relatively little processing power, and the key installation process is likewise quick. WPA2 employs multi-round interleaving. non-linear encryption technique, which can guarantee the avalanche effect of superior key design and significantly raises the difficulty of reverse cracking. More precisely, the encrypted message is identical to the original message each time the encryption key is changed by one bit, creating strong defense against brute force attacks [13]. Simultaneously, the WPA2 encryption algorithm utilizes a higher level of security CCM and CBC-MAC calculation method to finish the extraction of the MIC code, and it also draws on the idea of information integrity security verification in the WPA encryption process design [15].

The most widely used Wi-Fi encryption technology to date is WPA2. By using block-based encryption, it is possible to guarantee that different encryption and decryption keys are used for data sent by the same user at different times [15]. To achieve a better encryption-decryption isolation effect, various wireless users within the same wireless LAN use different encryption and decryption keys. This makes it essentially impossible for adversaries to use popular brute-force cracking techniques, such as the dictionary cracking method, to crack the key [11]. As time has gone on, Wi-Fi networking with WPA2 encryption has progressively revealed two significant issues. The first issue has to do with management frame protection. The encryption system that WPA2 created by Certain management messages in the Wi-Fi networking environment are not adequately protected by the 4-way handshake, which is typically only used for data information in communication. In particular, the management frame message in the Wi-Fi communication network is transparently transmitted on the wireless air interface [15].

Typically, the management frame message contains important network data. The communication network will be harmed as soon as the information is made public, maliciously copied, or altered. For example, association/de-association and authentication/deauthentication request and response frames are two crucial sets of management frames for creating terminal connections in Wi-Fi networks [6]. Both of these management frame types support unicast and multicast techniques, and they are never encrypted during transmission over a conventional Wi-Fi network. [11], [15]. This implies that all users on the network will be forced to disconnect if an attacker is in any Wi-Fi group and broadcasts de-association requests or de-authentication request messages continuously. This will cause a denial of service for the entire network and instantly paralyze traffic. Vanhoef (2017) revealed the WPA2 key reinstallation attack (KRACK) vulnerability, which is another issue brought to light by Wi-Fi networking that uses the WPA2 encryption scheme. The 4-way handshake stage of WPA2 networking is when key reinstallation attacks take place. During the 4-way handshake, the WPA2 pairwise temporal key (PTK) can be negotiated by both parties using a pre-shared key or a pairwise master key (PMK) that is derived from a certificate. Typically, the session key In the third step of the 4-way handshake, encryption is created and installed on both parties' devices [15]. To put it another way, the basic idea behind KRACK's attack is that a phony terminal will repeatedly send replies that haven't received the third handshake message in the third stage of the 4-way handshake. This will result in the PTK in the 4-way handshake being continuously recalculated and reinstalled into the counter. The counter will have an opportunity to return to the all-zero state as the number of reinstallations rises [11]. At this point, the data transmission using the encryption will be almost transparent, and the PTK produced by the counter will become the all-zero key. It is therefore unable to escape the passive situation. where, despite WPA2's subsequent encryption mechanism, the encrypted data is exactly equal to the plaintext. Following the disclosure


ISSN: 2961-6611

of the KRACK vulnerability, the US Department of Homeland Security also published and validated the security threats associated with KRACK, rendering the WPA2 encryption technique insecure [16].

### *D. WPA3 security protocol*

The Wi-Fi Alliance introduced WPA3, a new generation of Wi-Fi security scheme, in 2018 in response to the previously unheard-of sheer volume of Wi-Fi application scenarios. WPA3 was developed to defend users' privacy and communication security against evolving cyberthreats and attacks in the wide range of Wi-Fi application fields. The first Wi-Fi protocol to use the asymmetric key method for wireless communication was WPA3 technology. WPA3 technology is anticipated to accompany the next phase of wireless communication based on Wi-Fi technology, relying on the most cutting-edge cryptography technology and the growing computing power globally [11].

The encryption scheme using symmetric keys as the cryptographic system was gradually exhibiting signs of fatigue as a result of the unprecedented prosperity brought about by the rapid development of computer network technology, digital social media, electronic commercials, online business, and other applications. For instance, in order to guarantee secure communication between n users, the network equipment must manage $C(n,2)=n(n-1)/2$ keys, which is practically unaffordable for contemporary Wi-Fi or WLAN data communication. Key management has become a major burden due to the explosion of network users [16]. Furthermore, e-commerce applications require confidential communication between unknown network users, and key distribution is typically carried out using an asymmetric key system under the default sharing mechanism [6], which is unable to satisfy the previously stated novel security requirements.

Every node in the network that needs to communicate will use a pair of keys for encryption or decryption, according to the asymmetric key principle. Every communication node keeps its own private key, while the network management center or key management center publishes the public key. During the session encryption stage, the public key encrypts and transmits the message, while the recipient's private key decrypts it [16]. As the name suggests, an asymmetric key is one that is used for both message encryption and decryption. Elliptic curve cryptography is a representation of the asymmetric key group generation technique used in the SAE point-to-point communication key exchange system used in WPA3 encryption. The elliptic curve equation can precisely produce a sufficiently large asymmetric key set to meet the requirements of encryption for point-to-point communication [6], [11], [16].

## V.A COMPARISON AND CONTRAST OF THE SUGGESTED METHODS

The Wi-Fi security protocols WPA and WPA2 are both comparatively sophisticated. Users of 802.11i can select between the two encryption methods because WPA employs the TKIP protocol, while WPA2 introduces the CCMP protocol based on this. One could consider the WPA protocol to be an improved version of the WEP protocol [11]. The rationale is that, although more rigorous advancements in key length and encryption techniques have significantly increased the ability to fend off attacks and cracking, the RC4 algorithm remains the most crucial TKIP algorithm. The implementation of CCMP, which uses AES as its primary algorithm, is crucial to the WPA2 protocol. The RC4's drawbacks are successfully addressed by the AES algorithm. algorithm and enhances the security potential. In contrast, WPA2 can only be used after the hardware has been replaced; therefore, it cannot be used on WEP devices unless the software has been upgraded. 802.11i was created with TKIP compliances in order to better achieve hardware compatibility between the WPA and WPA2 protocols [6], [11], [16].

The CCMP cipher block chaining message protocol is a recognized encryption technique in WPA2. Its primary algorithm is an AES encryption algorithm that employs a 128-bit key and a 128-bit data block for encryption operations, setting it apart from WEP and TKIP's RC4 algorithm. This cipher block chaining message protocol is processor-related and has higher hardware requirements. Therefore, outdated devices are capable of supporting WEP and TKIP encryption, but not CCMP/AES [11]. In contrast to the WPA/WPA2 protocol, the WPA3 protocol's encryption scheme not only mitigates the security threats in earlier Wi-Fi network communications, but it also makes possible a more efficient management frame protection mechanism for management frames, known as the protected management frame (PMF). The worth is to offer better encryption methods for point-to-point wireless device communications and future large Wi-Fi networking equipment [6], [11], [16]. Additionally, the key management bottleneck issue has been resolved. The digital signature feature of the public key encryption scheme used by the WPA3 protocol can efficiently trace the encryption operation of each node for an increasing number of new Internet applications of e-commerce. This will have a significant impact on future applications based on Wi-Fi communication mode [11], [16]. Table I summaries this comparison depends on various aspects.

## IV. VULNERABILITIES IN WPA3

WPA3's Simultaneous Authentication of Equals (SAE) has a transition mode to make it compatible with WPA2 users. But according to the 2020 IEEE Symposium on Security and Privacy, a hacker can use the previously used WPA2 security attack


ISSN: 2961-6611

techniques, like KRACK and PMKID, to recover the network password in this mode [2]. A downgrade attack is the term used to describe the attack flow. By forcing the hardware that contains WPA3 to use only WPA2 and to disable the countermeasure for PMKID and KRACKs, the adversary exposes the state to security risks [2].

There is a vulnerability against attacks that take advantage of the high overhead of the Dragonfly-handshake used in WPA3, in addition to downgrade attacks that use SAE compatibility. The hash-to-curve function used by the Dragon Fly Handshake has a high above. An attacker could pose as a user and send a commit frame by taking advantage of such a high overhead. Then, they could purposefully slow down the access point's response time with subsequent attacks to carry out a denial-of-service attack. Right now, Dragon Blood is thought to be the most difficult task. The most recent security protocol, WPA3, has a problem that needs to be fixed as soon as possible in order to prevent WPA3 from becoming more widely used.

TABLE I: SYNOPSIS OF WEP, WPA, WPA2, AND WPA3 COMPARISON AND CONTRAST

| Aspects | WEP | WPA | WPA2 | WPA3 |
|---|---|---|---|---|
| Release Year | 1997 | 2003 | 2004 | 2018 |
| Security Level | Extremely low | Relatively low | Relatively high | Extremely high |
| Core Encryption | RC4 | TKIP with RC3 | AES-CCMP | AES-CCMP & AES-GCMP |
| Key Size | 64-bit & 128-bit | 128-bit | 128-bit | 128-bit & 256-bit |
| Authentication | WEP open & shared | WPA-PSK & 802.1X with EAP | WPA-PSK & 802.1X with EAP | AES-CCMP & AES-GCMP |
| Integrity | CRC-32 | 64-bit MIC | CCMP with AES | SHA-2 |
| Pre-Shared Key | PSK | PSK | PSK | SAE |
| Key Management | None | 4-way handshake | 4-way handshake | Elliptic curve cryptography methods. |
| Vulnerability | Brute-force attack, including dictionary attack, vulnerabilities | Brute-force attack, including dictionary attack, vulnerabilities | Brute-force attack, including dictionary attack, vulnerabilities / key reinstallation attack vulnerabilities | No significantly fatal vulnerabilities |

## *IIV*. Conclusion

Since wireless networks are spreading more quickly than any other technology in the world, it is important that they be properly secured to avoid sensitive information being exploited. We provided a concise synopsis of them in this paper, emphasizing the three primary security protocols: WEP, WPA, and WPA2. We talked about and demonstrated the general, step-by-step process for breaking WEP. The paper also discussed the current issues with the WPA3 protocol, which are slowing its adoption rate because no workaround has been found and hardware for WPA3-capable devices is costly. This component is seen as a major limitation since research cannot be carried out collaboratively in a single network. The necessity for enhanced wireless security and the widespread believe that WPA/WPA2 security protocols are hard for an outsider to breach these days, but our paper showed that if a wireless network is not properly configured and secured, it can be the target of successful hacking attempts.

## REFRENCES

**[1]** D. Buil-Gil, F. Mir´o-Llinares, A. Moneva, S. Kemp, N. D´ıaz-Casta˜no, “Cybercrime and shifts in opportunities during covid-19: a preliminary analysis in the uk,” European Societies, pp. 1–13, 2020.


ISSN: 2961-6611

**[2]** M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd," in 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020, pp. 517–533.

**[3]** V. Jones and H. Sampath, "Emerging technologies for wlan," IEEE Communications Magazine, vol. 53, no. 3, pp. 141–149, 2015.

**[4]** D. Bhaskar and B. Mallick, "Performance evaluation of mac protocol for ieee 802. 11, 802. 11ext. wlan and ieee 802.

**[5]** S. Banerji and R. S. Chowdhury, "On ieee 802.11: Wireless lan technology," International Journal of Mobile Network Communications Telematics, vol. 3, no. 4, p. 45ˆa64,Aug2013.[Online].Available: http://dx.doi.org/10.5121/ijmnct. 2013.3405.

**[6]** S. Malgaonkar, R. Patil, A. Rai, and A. Singh, "Research on wi-fi security protocols," International Journal of Computer Applications, vol. 164, no. 3, pp. 30–36, Apr 2017. [Online]. Available: http://www.ijcaonline.org/archives/ volume164/number3/27465-2017913601

**[7]** D. Coleman, CWSP: certified wireless security professional study guide CWSP-205, second edition ed. Indianapolis, IN: John Wiley and Sons, 2017, oCLC: on1005831581.

**[8]** M. Waliullah and D. Gan, "Wireless lan security threats vulnerabilities," International Journal of Advanced Computer Science and Applications, vol. 5, no.1,2014.[Online].Available: http://dx.doi.org/10.14569/IJACSA.2014.050125

**[9]** A. Sari and M. Karay, "Comparative Analysis of Wireless Security Protocols: WEP vs WPA," International Journal of Communications, Network and System Sciences, vol. 08,no. 12, pp. 483–491, 2015. [Online].Available:http://www.scirp.org/journal/doi.aspx?DOI=10.4236/ijcns.2015.812043.

**[10]** SANS Institute Reading Room site "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards".

**[11]** http://www.aircrack-ng.org/

**[12]** A. Sari, M. Karay et al., "Comparative analysis of wireless security protocols: Wep vs wpa," International Journal of Communications, Network and System Sciences, vol. 8, no. 12, p. 483, 2015.

**[13]** M. Prastavana and S. Praveen, "Wireless security using wi-fi protected access 2 (wpa2)," International Journal of Scientific Engineering and Applied Science (IJSEAS), vol. 2, pp. 374– 382, 2016.

**[14]** M. Rana, M. Abdulla, and D. Arun, "Common security protocols for wireless networks: A comparative analysis,"International Journal of Psychosocial Rehabilitation, vol. 24,pp. 3887–3896, 04 2020.

**[15]** S. Malgaonkar, R. Patil, A. Rai, and A. Singh, "Research on wi-fi security protocols," International Journal of Computer Applications, vol. 164, no. 3, pp. 30–36, 2017.

**[16]** V. Poddar and H. Choudhary, "A comparitive analysis of wireless security protocols (wep and wpa2)," Int. J. Ad Hoc Netw. Syst, vol. 4, no. 3, pp. 1–7, 2014.


ISSN: 2961-6611