FRI-ONLINE-1-CCT2-10

AN OVERVIEW OF THE RECENT STANDARDS AND SECURITY TECHNOLOGIES FOR WIRELESS LOCAL AREA NETWORKS[22]

Eng. Petar Stoilov, PhD Student
Department of Telecommunications,
University of Ruse "Angel Kanchev"
Tel.: +359 88 797 9174
E-mail: pstoilov@uni-ruse.bg

Abstract: *This paper reviews the emerging and the most recently adopted standards for wireless connectivity, as well as the evolution of the standards for providing security in the wireless local area networks. Different parameters, characteristics and specifications of the WiFi 4, WiFi 5 and WiFi 6 are investigated, compared and presented in the first chapter of the paper. A review on the methods for providing confidentiality and integrity in the wireless local area networks is also presented in the later part of the paper.*

Keywords: *IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax, wireless local area standards, WEP, WPA, WPA2, WPA3, WPS, wireless security standards*

INTRODUCTION

With the digital transformation of our society, the need to develop new information and communication technologies is imperative. The modern day applications rely on technologies that require higher bandwidths to answer the need for faster transmission and processing of the information. With the development of virtual and augmented reality products, cloud-based working spaces, new streaming technologies, and higher-resolution media, the need for advanced connectivity and mobility is as tangible and notable as never before. At the same time, the number of cybercrimes continues to grow with an unprecedented rate, which calls for the development of novel solutions and standards for confidentiality, integrity and accessibility of the data. To answer these issues, a new generation of standards for connectivity and security was developed and introduced in the wireless local area networks.

EXPOSITION

History and evolution of IEEE 802.11 Wireless standards

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) has certified the original 802.11 Legacy standard, which later became known simply as Wi-Fi.

In 1999, the wireless local area communications were introduced to the general public as a *"nice to have"* with the IEEE 802.11a and IEEE 802.11b ratifications. These standards provided speeds of up to 54 Mbps and 11Mbps respectively. These speeds were more than enough for the time period, as there were no Wi-Fi capable handheld mobile phones at that time and only few computers and laptops were capable of using the technology.

By 2003, however, some mobile devices that utilized Wi-Fi were coming out and portable laptops were becoming more standard for both business and personal use. That is when 802.11g was ratified – delivering up to 54 Mbps in the 2.4 GHz range. As we move closer to the present day, in 2007, the birth of the smartphone really came about and along with it came the ratification of the IEEE 802.11n. The "n" standard brought faster processing speeds of up to 450 Mbps for Wi-Fi and it supported both 2.4 GHz and 5 GHz enabled devices.

The evolution of the Wi-Fi standards is presented in Fig. 1.

[22] The paper is presented on 13 November 2020 with original title: AN OVERVIEW OF THE RECENT STANDARDS AND SECURITY TECHNOLOGIES FOR WIRELESS LOCAL AREA NETWORKS

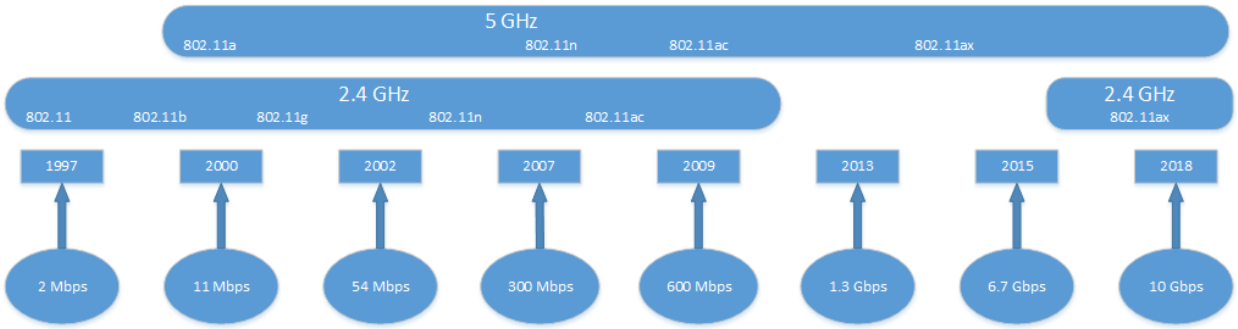

Fig. 1. The evolution of the Wi-Fi standards from 1997 until the present time

Comparison between the IEEE 802.11n (Wi-Fi 4), IEEE 802.11ac (Wi-Fi 5) and IEEE 802.11ax (Wi-Fi 6) standards

The IEEE 802.11n standard, under its full name IEEE 802.11n-2009, is a wireless networking standard that was published in 2009. The standard is also referred to as Wi-Fi 4. It allows the use of two radio frequency bands, 2.4 GHz and 5 GHz, and can provide data transfer speeds of up to 600 Mbps. IEEE 802.11n was also the first wireless standard that offered support for multiple-input-multiple-output (MIMO). This technology allows the use of multiple antennas for transmission of more data by combining independent data streams (Selvam T. et. al. 2009). Modern wireless routers use the Wi-Fi 4 standard on the 2.4 GHz band. Wi-Fi 4 is used to connect older devices to the network or smart home devices like smart plugs, smart bulbs, sensors, etc.

The IEEE 802.11ac is a wireless networking standard that was published in the late 2013. It is also known as Wi-Fi 5. The IEEE 802.11ac is the most common wireless standard today, as most routers sold during the last few years are 802.11ac compatible (Bejarano O, et. al, 2013). This standard, just like the 802.11n before it, supports multi-user MIMO (MU-MIMO), but it can offer maximum data transfer speeds of up to 2.3 Gbps. The 802.11ac standard works only on the 5 GHz frequency band, but most of the wireless routers that support it also offer support for the 802.11n standard on the 2.4 GHz frequency band. 802.11ac devices are split into two categories, called 802.11ac Wave 1 and Wave 2. The products that are sold as part of the 802.11ac Wave 1 were introduced to the market in 2013, while the ones from Wave 2 were introduced in 2016. Wave 2 presents an improved version of the standard and all 802.11ac Wave 2 wireless routers have higher throughputs and add support for MU-MIMO. While the Wave 1 routers can provide speeds of up to 1.3 Gbps, the ones in Wave 2 can deliver speeds of up to 2.3 Gbps (Hoefel, 2019).

The 802.11ax or IEEE 802.11ax is a wireless networking standard. 802.11ax is also referred to as Wi-Fi 6 and is also known as High-Efficiency Wireless (HEW). It was designed to work in the same 2.4 GHz and 5 GHz frequency bands as the standards that was mentioned so far. The standard is also planned to work with additional frequency bands between 1 and 7 GHz, when they become available (Khorov, E. et. al, 2013). The 802.11ax wireless networking standard aims to improve the average data transfer speeds by up to four times more than the 802.11ac standard. It offers significantly improved speeds, especially in crowded places such as train stations, airports, coffee shops or restaurants. Wireless routers and mesh Wi-Fi systems that are Wi-Fi 6 compatible have already shown up on the market and the standard is slowly replacing its predecessor.

Benefits of Wi-Fi 6 over previous generations of wireless connectivity

Wi-Fi 6 not only improves the current features for wireless connectivity, but also adds new features such as:

- Lower battery consumption for the devices that support Wi-Fi 6 connectivity;
- Higher data speeds with a peak of up to 10 gigabits per second;
- Increased capacity with reduced latency to support more users and devices;
- High levels of efficiency in saturated frequency spectrum;
- Increased efficiency and lower latency with orthogonal frequency access multiple access (OFDMA).

Wi-Fi 6's most significant technological advantage comes from the introduction of the Orthogonal Frequency Division Multiple Access modulation (OFDMA). This technology is the multi-user version of the Orthogonal Frequency Division Multiplexing (OFDM) that was used in the earlier Wi-Fi networks (Fig. 2). With the OFDMA, the channel is divided between multiple users that can simultaneously exchange data with the access point using smaller sub-channels.

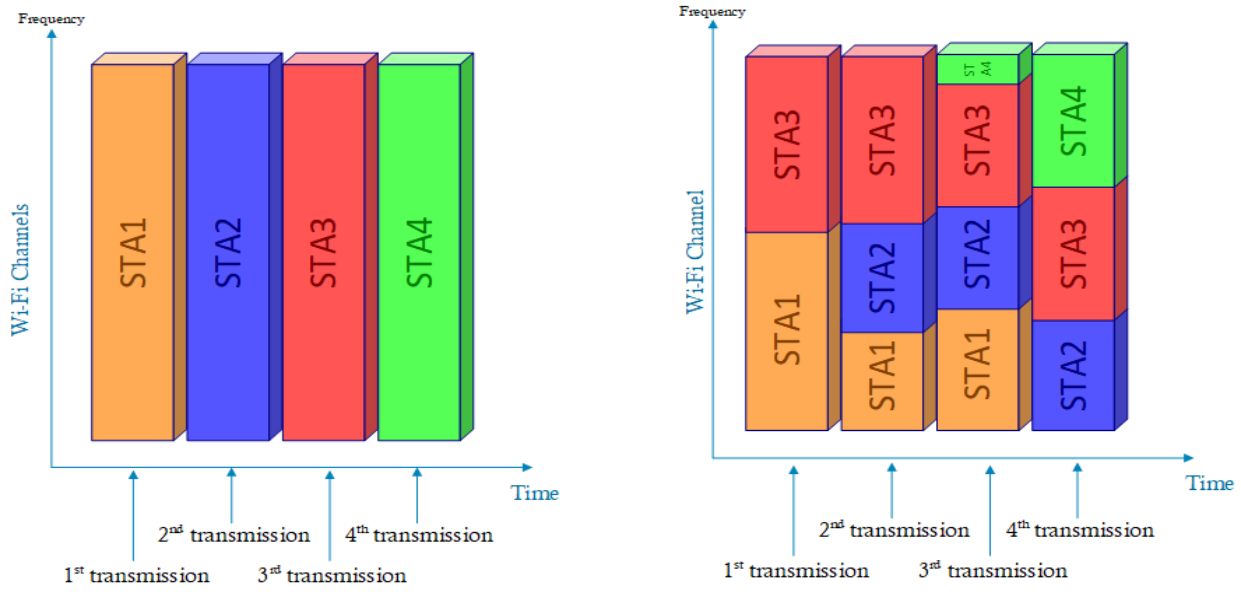

Fig. 2. Graphical representation of the sub-channel use in OFDMA (right) and OFDM (left)

Wi-Fi 6 relies on OFDMA technology to achieve greater capacity and lower latency in environments with high device density. However, with multiple devices sharing the spectrum and transmitting simultaneously, one bad actor can ruin the transmission for all other devices in the network. With OFDMA, the access point plays a central role, acting as the network distributor.

Table 1 provides further comparison between the parameters of the recent Wi-Fi standards.

Table 1. Comparison between the Wi-Fi 4, Wi-Fi 5 and Wi-Fi 6 standards

Parameters	802.11n	802.11ac	802.11ax
Channel bandwitdh (MHz)	20, 40	20, 40, 80, 80+80, 160	20, 40, 80, 80+80, 160
Subcarrier (KHz)	312.5	312.5	78.125
Symbol time (µs)	3.2	3.2	12.8
Cyclic prefix (µs)	0.8	0.8, 0.4	0.8, 1.6, 3.2
MU-MIMO	-	Downlink	Uplink and downlink
Modulation	OFDM	OFDM	OFDM, OFDMA
Data subcarrier modulation	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
Coding	BCC (Mandatory) LDPC (Optional)	BCC (Mandatory) LDPC (Optional)	BCC (Mandatory) LDPC (Mandatory)

In the downlink direction, the transmission from the access point (DL-OFDMA) bundles together data destined for multiple stations on their respective sub-channels. The client station devices tune their radios to receive their respective data on their assigned sub-channel (Bokhari, S.M., 2019).

In the uplink direction (UL-OFDMA), the traffic is transmitted from the client stations to the access point. The process described above is reversed: as multiple stations transmit simultaneously on their respective pre-assigned sub-channels, the access point is in charge of coordinating simultaneous transmissions from the client stations. This synchronization is done by the transmission of a trigger frame. In response to the trigger frame, the client stations have to tune their timing, frequency and power to participate in the upcoming transmission.

History of recent security technologies for wireless local area networks

Wired Equivalent Privacy (WEP)

When in 1997 Wi-Fi was introduced, it quickly turned out that the standard lack adequate security. To solve this issue, the Wi-Fi Alliance developed the Wired Equivalent Privacy or WEP, which became the primary security mechanism for the IEEE 802.11 networks.

Two processes are applied to the plaintext data when WEP is used. One of them encrypts the plaintext, while the other protects the data from being modified by unauthorized parties. The 40-bit secret key is connected with a 24-bit Initialization Vector (IV) resulting in a 64-bit total key size. The resulting key is forwarded to a RC4 stream cipher that outputs a pseudorandom key sequence. The resulting sequence is used to encrypt the data. The result is an encrypted stream of bytes, equal in length to the number of data bytes that are to be transmitted in the expanded data plus four bytes. This is because the key sequence is used to protect the 32-bit Integrity Check Value (ICV), as well as the data. Figure 3 below illustrates how the WEP mechanism functions.

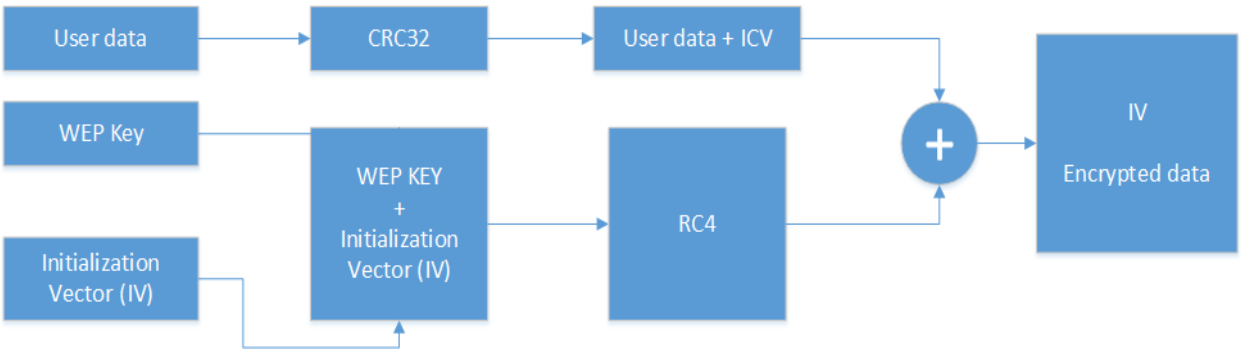

Fig. 3. The general functionality workflow of the WEP encryption mechanism

Wi-Fi Protected Access (WPA)

To improve the functions of WEP, Wi-Fi Protected Access or WPA was created in 2003. This temporary enhancement still has relatively poor security, but is easier to configure. WPA uses Temporal Key Integrity Protocol (TKIP) for more secure encryption than WEP offered.

As the Wi-Fi Alliance made this transition to a more advanced protocol, they had to keep some of the same elements of WEP, so older devices would still be compatible. Unfortunately, this means vulnerabilities, such as the Wi-Fi Protected Setup feature, which can be hacked relatively easily, are still present in the updated version of WPA.

WPA is implemented as part of the 802.11i standard and importantly, it is based on the same hardware as WEP, so only a firmware upgrade is required to improve the security aspect. This eliminated the two main shortcomings in WEP. Encryption is still based on RC4, as it is hardware-embedded and cannot be updated, but the IV is extended to 48 bits (Fig. 4).

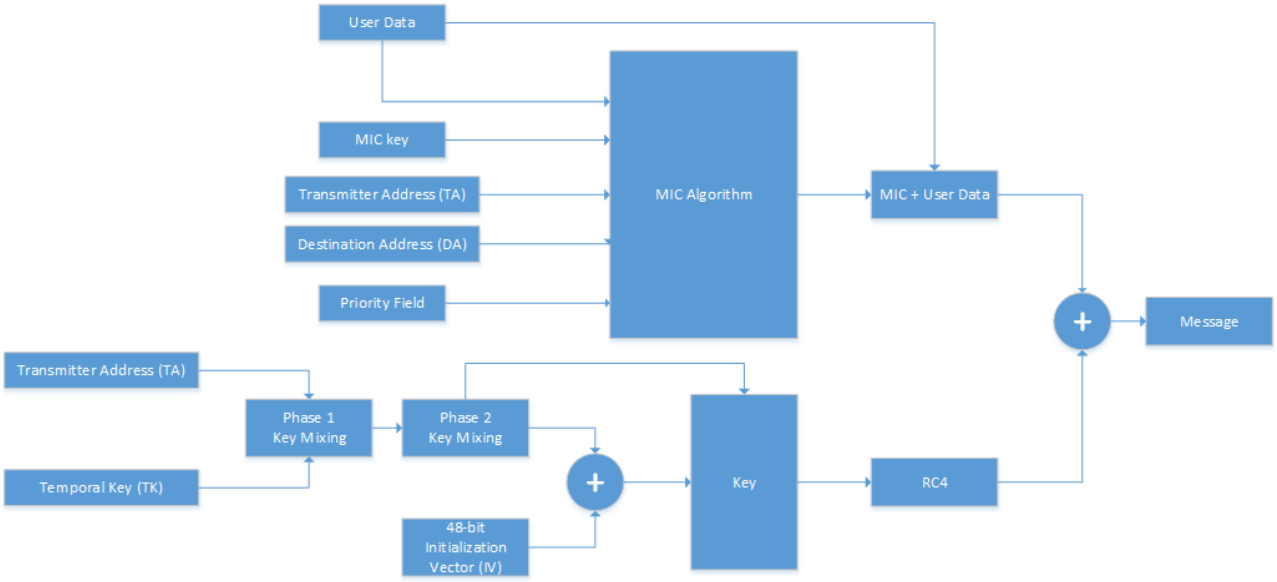

Fig. 4. Block diagram of the WPA security mechanism

Wi-Fi Protected Access II (WPA2)

WPA2 is an updated version of WPA that uses the Advanced Encryption Standard (AES) encryption and long passwords to create a secured network. WPA2 has personal and enterprise options, making it ideal for home users and businesses. However, it needs a significant amount of processing power, so if you have an old device, it may be slow or not work at all.

WPA2 performs all mandatory functions of the 802.11i standard. It provides a significant improvement, in terms of security, compared to WEP and WPA. The most important architectural change is the data encryption algorithm - in WPA2, the Chaining Message Authentication Code Protocol (CCMP) uses the Advanced Encryption Standard (AES). WPA2 differs from WPA in the way the encrypted message and its integrity are calculated. In WPA2, encryption and integrity checking are performed within one logical block – CCM (Fig. 5).

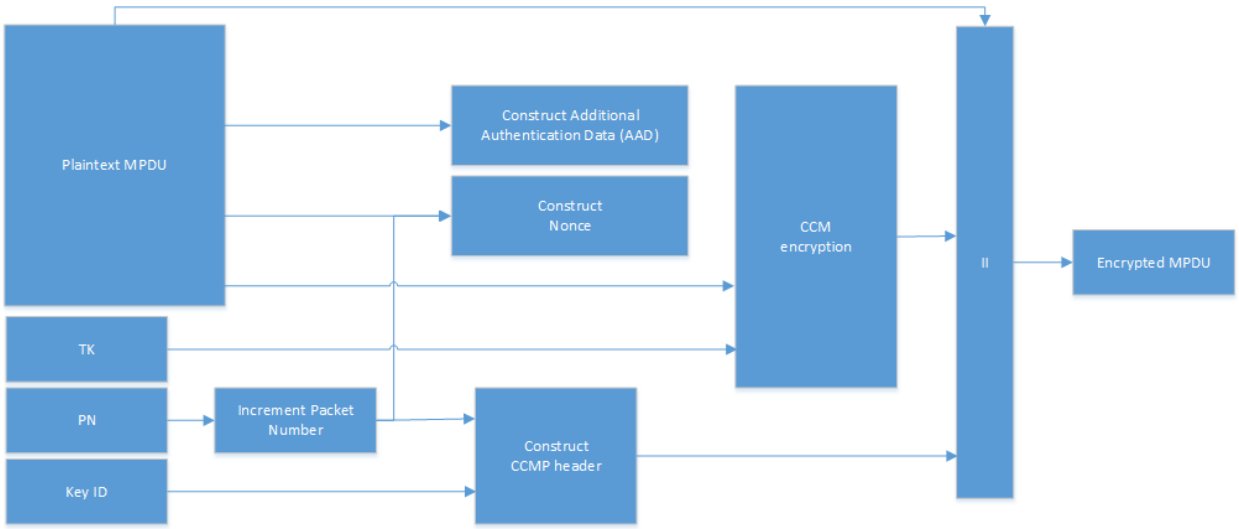

Fig. 5. The WPA 2 operations block diagram

Common attacks on WPA and WPA2

WPS Attacks

Wi-Fi Protected Setup (WPS) allows users to configure a wireless network without typing in the passphrase. Instead, users can configure devices by pressing buttons or by entering a short

personal identification number (PIN). User can configure a new wireless device by pressing a button on the WAP and on the wireless device. It will automatically configure the device within about 30 seconds with no other actions needed. These buttons can be physical buttons on the devices, or virtual buttons that the user clicks via an application or web page. When using the PIN method, users first identify the eight-digit PIN on the WAP and then enter the PIN on the new wireless device (Redondi, A. E. et. al, 2018).

WPS is susceptible to brute force attacks. A WPS brute force attack keeps trying different PINs until it succeeds. Reaver is an open source tool freely available that allows attackers to discover the PIN within 10 hours, and often much quicker. Once it discovers the PIN, it can then discover the passphrase in both WPA and WPA2 wireless networks (Friess, K, 2018).

Hole196 Attacks

"Hole 196" vulnerability can lead to a potentially fatal insider attack, where an insider can bypass the WPA2 private key encryption and authentication to scan the authorized devices for vulnerabilities, install malware on these and steal personal or confidential corporate information from the devices. Although specifically mentioned for WPA2, the vulnerability applies to the WPA version also, irrespective of the authentication method used (Hurley, C. et al, 2007).

Exploiting the 'Hole 196' vulnerability is simple and easy. Hence, the vulnerability can lead to practical insider attacks when compared with the WPA TKIP vulnerability, which was largely of theoretical interest and difficult to exploit for launching any practical attacks.

KRACK Attacks

KRACK ("Key Reinstallation Attack") is a replay attack on the Wi-Fi Protected Access protocol that secures Wi-Fi connections. It was discovered in 2016 by the Belgian researchers Mathy Vanhoef and Frank Piessens of the University of Leuven. Vanhoef's research group published details of the attack in October 2017 (Vanhoef M. & F. Piessens, 2017). By repeatedly resetting the nonce transmitted in the third step of the WPA2 handshake, an attacker can gradually match encrypted packets seen before and learn the full keychain used to encrypt the traffic. The attack targets the four-way handshake used to establish a nonce (a kind of "shared secret") in the WPA2 protocol. The standard for WPA2 anticipates occasional Wi-Fi disconnections and allows reconnection using the same value for the third handshake. Because the standard does not require a different key to be used in this type of reconnection, which could be needed at any time, a replay attack is possible. An attacker can repeatedly re-send the third handshake of another device's communication to manipulate or reset the WPA2 encryption key. Each reset causes data to be encrypted using the same values, so blocks with the same content can be seen and matched, working backwards to identify parts of the keychain, which were used to encrypt that block of data. Repeated resets gradually expose more of the keychain until eventually the whole key is known, and the attacker can read the target's entire traffic on that connection.

Wi-Fi Protected Access III (WPA3)

Wi-Fi WPA3 delivers the necessary capabilities to meet the requirements of different networks from home networks to corporate environments. After WPA and WPA2 attacks, WPA3 devices are delivering two key benefits: Cryptographic consistency which the susceptibility of networks to a successful attack by mandating policies around the use of Advanced Encryption Standard (AES) with legacy protocols and network resiliency deliver a level of protection against eavesdropping. The consistent use of that improves the resiliency of mission-critical networks

WPA3-Personal

WPA3-Personal replaces the Pre-Shared Key (PSK) used in WPA2-Personal with Simultaneous Authentication of Equals (SAE), delivering stronger password-based authentication.

WPA3-Personal uses passwords for authentication by proving knowledge of the password and not for key derivation (Caso, G, et al, 2018), providing users with stronger security protections, like:

- Offline dictionary attack resistance
- Key recovery resistance
- Natural password use
- Simple work flow continuity

WPA3-Personal is based on Simultaneous Authentication of Equals (SAE), defined in the IEEE 802.11-2016 Standard. The Wi-Fi Alliance WPA3 Specification defines additional requirements for devices operating in SAE modes. SAE is a key exchange protocol that authenticates two peers using only a password, resulting in a shared secret between the two peers that can be used for secret communication while exchanging data over a public network. It provides a secure alternative to using certificates or when a centralized authority is not available. One of the key benefits of WPA3 is improved consistency in the application of cryptography. WPA3-Personal Transition Mode provides backwards interoperability with WPA2-Personal, while other legacy protocols are disallowed in this mode (Cisco Annual Internet Report, 2019).

WPA3-Enterprise

WPA3-Enterprise does not fundamentally change or replace the protocols defined in WPA2-Enterprise (Kohlios, C. et. al, 2018). Instead, WPA3-Enterprise defines and enforces policies to deliver greater consistency in the application of those protocols to ensure desired security. For sensitive security environments, WPA3-Enterprise offers an optional 192-bit security mode that specifies the configuration of each cryptographic component, such that the overall security of the network is consistent. This not only delivers the desired security level, but also makes provisioning easier. The approach is based on the concept that cryptographic primitives have a work factor necessary for successful attack and an attacker will target the weakest component in a system.

To achieve a consistent level of system security it is necessary to ensure that the work factor for each cryptographic primitive meets or exceeds a selected level. For example, it does no good to derive a 256-bit AES key from a shared secret resulting from a Diffie-Hellman group with a work factor of 2^{80}. The WPA3-Enterprise 192-bit security mode uses 256-bit Galois/Counter Mode Protocol (GCMP), widely written as GCMP-256, to provide authenticated encryption, 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384) for key derivation and key confirmation, and Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve for key establishment and authentication. While GCMP-192 would deliver the appropriate equivalent strength, GCMP-256 was selected based on its broader adoption (Rahane, S. et. al, 2018).

In general WPA3 is build up on WPA2, but brings a lots of improvements:

- Encryption is based on 256-bits protocol Galois / Counter Mode (GCMP-256)
- Key derivation uses 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (SHA)
- Key management uses Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve и Elliptic Curve Digital Signature Algorithm (ECDSA)

Data integrity is based on 256-bit Broadcast / Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256).

Detailed comparison between WEP, WPA, WPA2 and WPA3 is presented in the next figure (Fig. 6).

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like Privacy in wireless	Based on 802.11i Without requirement For new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/ Multicast Integrity Protocol Galois Message Authentication Code
Key Management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

Fig. 6. Comparison between the WEP, WPA, WPA2 and WPA3 wireless security mechanism

CONCLUSION

The Wi-Fi standards have evolved significantly to meet the ever-increasing demands of users for faster and more reliable connectivity. The modern generations of Wi-Fi standards, Wi-Fi 4, Wi-Fi 5 and Wi-Fi 6, are characterized by many innovations and partially meet the user demands. The development of multimedia services and the introduction of newer types of content requires the development of the next generations of wireless standards for connectivity in the local area networks, which means that we are far from the moment when we will see the last standards of the IEEE 802.11 family. By 2023, 66% of TVs in the world will support Ultra High Definition, compared to just 33% in 2018. The trends in the wireless networks are growing at a tremendous rate and by 2020, there will be about 11.6 billion devices that generate 1.7 megabits of information every second from each user.

Based on the provided information, it can be easily stated that WEP should always be avoided. The devices with old hardware must be updated with the latest available firmware. The next generation of Wi-Fi connectivity requires robust tools and practices to maintain user data privacy and security. The Wi-Fi Alliance has continued its track record of constantly evolving the Wi-Fi Protected Access family of technologies to provide the latest security changes. Through use of standards-based mechanisms, consistent application of protocols, and security interface tools that are easy to use, network owners can better protect user data and promote adoption of security best practices. Still every network environment is different. The Wi-Fi Alliance recognizes the need for robust solutions that meet the security requirements of a variety of devices and networks.

Via WPA3, the Wi-Fi Alliance brings new capabilities that support the way the world works and lives today. Providing for secure on-boarding of every type of device and enabling user data protection for personal and data sensitive Wi-Fi network environments, it increases the Wi-Fi user experience, as well as dependence on Wi-Fi. WPA3 builds upon trusted WPA2 success to bring a new level of security for personal and enterprise environments with strong security protocols. Focus on cryptographic consistency, strong password-based authentication, and 192-bit security ushers the market into the next age of connectivity with confidence.

ACKNOWLEDGMENT

This paper is supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Ministry of Education and Science of Bulgaria.

The work presented in this paper is completed as partial fulfilment of Project 2020 - FEEA - 03 “Design and Development of a Multifunctional Robot for Implementation and Evaluation of Autonomous Navigation Algorithms”, financed under the Scientific and Research Fund of the University of Ruse "Angel Kanchev".

REFERENCES

Hoefel, R.P.F. (2019). Applications of Multi-User Technologies on IEEE 802.11ac (Wi-Fi 5), 802.11ax (Wi-Fi 6) and 802.11be (Extremely High Throughput) Amendments, IEEE Latin-American Conference on Communications, Salvador, Bahia, Brazil

Cisco Annual Internet Report (2018–2023) White Paper, 2019, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Bokhari, S.M., (2019), Introduction and Architecture of Wi-Fi 6 (802.11ax).

Selvam, T. & Srikanth, S. (2009) Performance study of IEEE 802.11n WLANs, First International Communication Systems and Networks and Workshops. Bangalore. pp. 1-6. DOI: 10.1109/COMSNETS.2009.4808917.

Vanhoef M. & F. Piessens. (2017). Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS).

Bejarano, O., Knightly, E., Park, M. (2013). IEEE 802.11ac: from channelization to multi-user MIMO. IEEE Comm. Magazine Vol. 51(10), pp.84–90 doi:10.1109/MCOM.2013.6619570

Khorov, E., Kiryanov, A., Lyakhov, A. & Bianchi., G. (2019). A Tutorial on IEEE 802.11ax High Efficiency WLANs'. IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 197-216. doi: 10.1109/COMST.2018.2871099.

Kohlios, C. & Hayajneh, T. (2018). A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. Electronics. Vol. 7 (11).284, DOI: 10.3390/electronics7110284.

Rahane, S., Ulekar, S., Vatti, R., Meshram T., & Male, S. (2018). Comparison of Wireless Network Performance Analysis Tools. 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), Coimbatore, pp.1-4, DOI: 10.1109/ICCTCT.2018.8550997.

Caso, G., Le, M., De Nardis, L. & Di Benedetto, M.-G. (2018). Performance Comparison of WiFi and UWB Fingerprinting Indoor Positioning Systems. Technologies 2018.6.14.

Hurley, C., Rogers, R., Thornton, F. & Baker, B. (2007), Wardriving and wireless penetration testing, Syngress, 2007.

Redondi, A. E. & Cesana, M. (2018). Building up knowledge through passive Wi-Fi probes, Computer Communications, vol. 117, pp. 1–12, 2018.

Friess, K. (2018). Multichannel-sniffing-system for real-world analysing of Wi-Fi-packets. Tenth International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, pp. 358–364.