ISSN 2303-4521
**Periodicals of Engineering and Natural Sciences** *Original Research*
Vol. 9, No. 4, December 2021, pp.1093-1101

# Analyzing Attacking methods on Wi-Fi wireless networks pertaining (WEP, WPA-WPA2) security protocols

**Doaa Talib Zaidan**
Laser and Optoelectronics Engineering, Department, Kut University College, Iraq

## ABSTRACT

The technology of wireless network systems has eased the possibility to communicate utilising the electromagnetic waves which leads to eliminating the major barriers in portable communications. Wireless networks have a vital role in the current era that all devices; rangingfrom local modems to organizational equipment, are using various coding approaches to exchange data on the network. However, since the wireless networks utilise the air, as the communication medium, that results to confront more vulnerabilities. If an attacker penetratesa wireless network, he/she would be capable to attack users connected to the network. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and WPA2 are the common security protocols that play the most significant role in local and organizational wireless communication. Accordingly, this study analysed the attacking methods in WEP, WPA, and WPA2 coding protocols. The main objective of the current study is to identify the security vulnerabilities related to these three protocols and define optimal solutions to improve the security of wireless networks against the attackers. The findings presented in this study wouldsupport users to maintain security of their home wireless networks as well as employees to secure the organizational network.

**Keywords**: Wi-Fi networks, network security, WEP, WPA, WPA2.

***Corresponding Author:***

Doaa Talib Zaidan
Laser and Optoelectronics Engineering Department
Kut University College, Iraq
E-mail: Doaa.almosawi@alkutcollege.edu.iq

## 1. Introduction

A wireless network is a computer network that allows different devices to communicate with each other without being connected through a physical communication medium such as a network cable [1]. Modern wireless networks typically rely on radio communications that operate in frequencies beyond the infrared in the electromagnetic spectrum.

With the development of wireless communications in various applications such as the Internet of Things, smart devices, and increasing Wireless Fidelity (Wi-Fi) access points in different areas, security concerns cannot be ignored [2, 3]. The modern technology used for wireless networks is Wi-Fi, which is associated with longer distance and more stable transmission than other technologies such as Bluetooth, Radio Frequency Identification (RFID) and Infrared Radiation (IR). Wi-Fi communication is very common because of its ease of use and high speed. To provide security for Wi-Fi communications, WIFI Protected Access (WPA) and WPA2 security protocols are now the most common protocols used for that purpose [1, 4]. WPA and WPA2 were developed by the Association of Electrical and Electronics Engineers (IEEE). However, in these protocols (WPA & WPA2) only data is protected, and attackers have the opportunity to infiltrate sensitive information exchanged on the network.

In recent years, Wi-Fi wireless network security issues has been a field of continuous research that with the development of wireless network systems, secure and reliable communication is of particular importance [5-7]. The importance of this area is the security of wireless systems has a vital role to prevent illegal access or damage

to the system and data by attackers. Because wireless networks are open and borderless in nature, wireless network security remains a serious and challenging issue. The question here is, how secure are these protocols? This article is organized into sections as follows. Section 2 highlights the Wi-Fi security protocols. This section also classifies the types of attacks in wireless networks. Section 3 explains the research method employed in this study. While Section 4 examines the attacking methods in Wi-fi networks pertaining Wired Equivalent Privacy (WEP) and WPA-WPA2 protocols. Section 5 present suggested techniques to improve the security of wireless equipment against the attackers. Lastly, Section 6 concludes this study.

## 2. Background

### 2.1. WI-FI security protocols

In the 90s, when the use of wireless networks became widespread, protocols were introduced to maintain networks security over the years. These protocols are intended for managing the security of users' devices connected to the wireless network [8]. Table 1 shows the key specifications of the common three security protocols used in Wi-Fi networks.

Table 1. Key specifications of WEP, WPA, WPA2 security protocols

| | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| **Year of presentation** | 1999 | 2003 | 2004 |
| **Key length** | 40 bits | 128 bits | 128, 192, 256 bits |
| **Key type** | Fixed | Dynamic | Dynamic |
| **Central Key Manager** | Does not have | Radius | Radius |
| **Authentication** | WEP security key | 802.1X (EAP) | 802.1X (EAP) |
| **Cryptographic pattern** | RC4 | TKIP with RC4 encryption | CCMP with AES encryption |
| **Device compatibility** | 802.11a/b/g | 802.11a/b/g | 802.11a/b/g |

The three security protocols presented in Table 1 are further described as follows.

- WEP protocol. Introduced in 1999, WEP protocol is the first version of the IEEE 802.11family of wireless network security protocols. Two years after its introduction, this protocol was broken due to its key length and poor structure and cryptographicalgorithm.
- WPA protocol. Introduced to solve the problems of the previous protocols, namely WEP. This protocol is equipped with stronger Temporal Key Integrity Protocol (TKIP)encryption and its key length is 128 bits.
- WPA2 protocol. Replaced WPA protocol in 2004. This protocol was equipped with Counter Mode Cipher Block Chaining (CCMP) with Advanced Encryption Standard (AES) algorithm.

### 2.2. Attacks in wireless networks

Wireless networks are vulnerable to attackers due to their hard to prevent illegal access to them. Wireless networks use electromagnetic waves precisely like radios or televisions. In fact, wireless communication is almost like two-way radio communication in which wireless signals can be easily reflected and scattered [9-11]. Thus, allowing potential attackers to access wireless communications. In this respect, the sole advantage wireless networks have is that attackers should be in physical proximity to the wireless network, which could limit the pool of potential attackers [1].

Wireless networks are subject to two categories of attacks that are related to their security. The two categories are passive and active attacks [2, 12-13]. In passive attacks, the attacker captures the signals; but it does not change the content of the source signal. This category of attacks attempt to learn information captured from the system. Passive Attacks can be simple eavesdropping or traffic analysis. On the other hand, in active attack, attacker can send signals also; the attacker changes the information that comes from the source or origin. Thereby, in active attacks, attacker attempts to modify system resources and/or effect their operations.
Figure 1 illustrates the attacking methods in wireless networks classified under the active and passive attacks. While further demonstration for attacking methods pertaining to Wi-Fi networks is presented in Section 4.

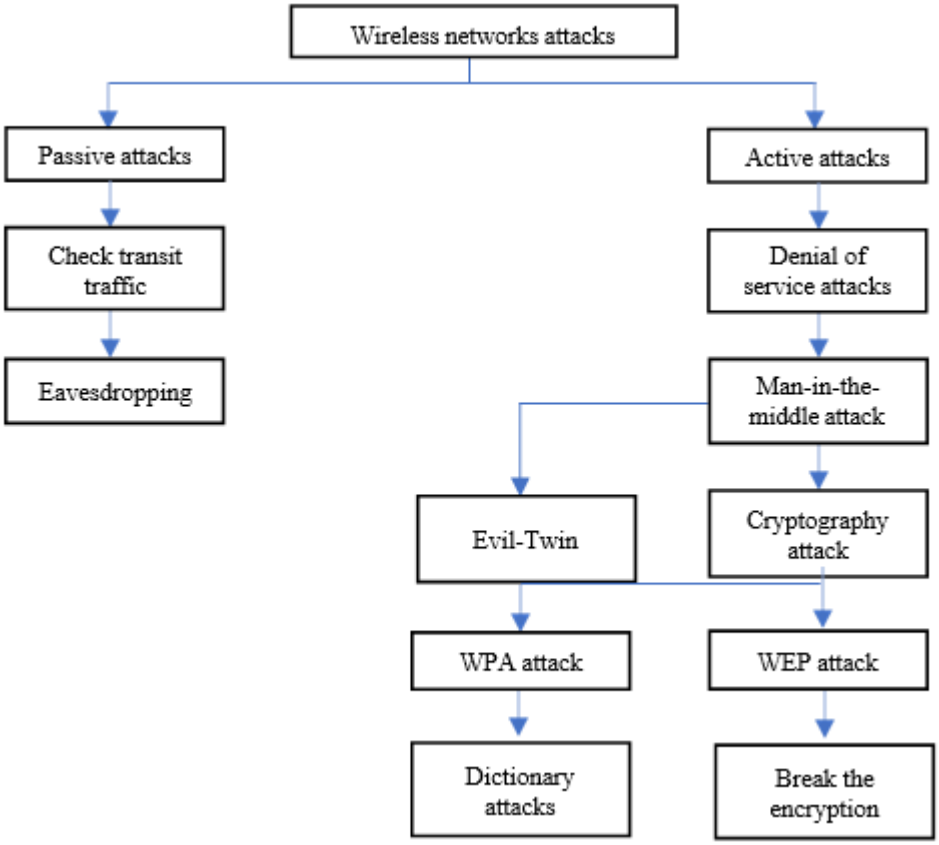


Figure 1. Categorization of attacking methods in wireless networks.

## 3. Method

The method employed for this article involved searching of various databases. Search queries were performed using SpringerLink, IEEE Explore, ACM Digital Library, Science Direct, Web of Science, and Taylor and Francis databases. Much broader search was made on the SCOPUS database, in order to extract relevant literature not covered in the aforementioned databases.

Authors conducted an in-depth analysis of the extracted literature to (1) fully investigate the attacking methods in WEP, WPA, and WPA2 coding protocols, and (2) to identify their common security vulnerabilities and define optimal solutions for the identified vulnerabilities. To perform the analysis, we utilized Microsoft Excel Spreadsheets as a tool to manage the information gathered from the extracted literature. Figure 2 is further showing the research method followed in this study.

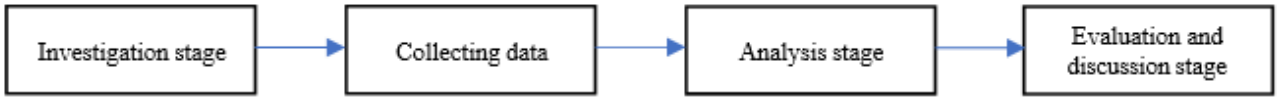


Figure 2. Research method

## 4. Results and discussion

### 4.1. Attacking methods on Wi-Fi networks

As the waves of wireless network systems are transmitted in the air; Wi-Fi networks become exposed and vulnerable to attackers [5, 7]. Attackers can infiltrate and eavesdrop on exchanged information as long as this information is within range of radio waves. One of the important features of this type of intrusion is that attackers can execute it with only a laptop and a remote wireless network card without physical identification [5, 14]. In this section, we analysed attacking methods on Wi-Fi networks pertaining to the common security protocols (i.e., WEP and WPA-WPA2). Whereas in Section 4.2 we defined the techniques suggested to improve the security of wireless equipment.

#### 4.1.1. Attacking methods on WEP protocol

WEP security protocol was presented in 1997 and officially adopted in 1999 in an effort to provide a sophisticated level of protection for Wi-Fi networks [7, 15]. In further details, WEP was intended to be used in wireless communications with a level of security and privacy similar to that of wired communication. However, two years after the official publication of the protocol, many critical weaknesses have been identified in WEP protocol [16]. Those weaknesses limit their effective user to provide the anticipated security and privacy levels for Wi-Fi networks. We have identified critical security vulnerabilities pertaining WEP security protocol. These security vulnerabilities are as follows.

1. Poor Encryption. Recorded network traffic has shown that the shared key used by WEP can be easily analysed and decrypted by attackers, which can lead to data manipulation and loss of integrity.
2. Lack of key management. The WEP protocol does not have the key management feature to manage different keys in its key table, but the same key is used for a long period.
3. Short key size. The standard WEP key size is only a forty-bit key. This allows the WEP password to be quickly guessed by a dictionary attack.
4. Authentication Problems. Depending on the challenge and response scheme used to authenticate the key, a Man-in-the-Middle (MITM) attack can take place in WEP. This type of attack is an attempt to gain access to confidential information, which leads to the misinformation of sensitive information and, possibly, can lead to the loss of information.
5. Packet forgery. There is no protection against packet counterfeiting in WEP. Data packets can be forged and injected into the network using a third-party program, which can lead to data manipulation and loss of data integrity.
6. Denial-of-Service (DoS) Attacks. These attacks involve sending large data packets to a server, thereby preventing users from accessing the network.

At the present time, the use of this old protocol has significantly decreased. Due to its limited security encryption, WEP-based networks could be infiltrated in a quick time with the tools available in Linux.

#### 4.1.2. Attacking methods on WPA-WPA2 protocol

##### 4.1.2.1. WPA handshake attack

It is one of the first successful methods in attacking wireless networks [18, 19]. In this method, the attacker scans the surrounding networks and selects a network to attack. Attacked must consider that the target network is close enough to him/her in order to carry out a successful attack [18-20]. After selecting victim network, attacker could easily connect to the network in order to obtain WPA four-stage handshake connection.

To solve weakness of the WPA protocol, WPA2 protocol uses a powerful encryption algorithm called AES, which is very difficult to break; nonetheless it is not impossible [21, 22]. The weakness of WPA2 is that the encrypted password is common to what is known on four- step process. In more details, when a user connects to a network, that network performs the 4- way handshake to negotiate a fresh encryption key. Network installs the “fresh encryption key” once it received message 3 of the 4-way handshake. Once the key is installed, it is utilised to encrypt data frames using an encryption protocol. This key reinstallation could happen spontaneously if the last message of a handshake process is missed because of background noise [6, 23]. Thus, a re-transmission

of the previous message is needed. When this retransmitted message is processed, keys may be reinstalled, causing a nonce reuse similar to a real attack. This retransmitting process could be forced by an attacker who managed to perform a MITM attack. WPA handshake attack comprised of three stages as follow [16, 24].

1. Select the access point for the attack. In this step, all the access points are scanned with standard tools in the Linux operating system. After scanning access points, attacker selects a network that is physically close and at least one device is connected to it. The next step is attempting to get the Handshake.
2. Get a handshake. Attacker makes possible effort to achieve a four-step handshake between the access point and the connected device. Once the handshake is achieved, password of the victim network is possible to be obtained. This is a type of DoS attacks performed through radio waves that interrupts the connection between the access point and the client in the victim network. The only way attacker can get the WPA handshake is to do a multi-second DoS attack to disconnect access point and the client and get the handshake after reconnecting.
3. Break WPA handshake to get password. After getting the Handshake, attacker has to do a dictionary attack against the network. The structure of this attack is such that each dictionary contains a number of predicted words of password, which is scanned to check all the words in the dictionary with the main key in the handshake. If the password is found in the dictionary, then the attack is concluded to be successful.

#### 4.1.2.2. Pairwise master key identifier (PMKID) attack

Password cracking for WPA networks has remained virtually the same for years, until 2018 when security experts discovered a new approach to hack into WPA-based networks [25- 27]. In this technique, attacking WPA networks requires fewer steps and information than the previous methods, and also has the advantage of targeting access points to which no one is connected.

This new attack against Pairwise Master Key (PMK) utilises “Hashcat” to crack WPA passwords allowing attackers to crack WPA networks have weaker passwords with more ease [2, 6, 28]. An attacker can utilise this new technique to communicate directly with a vulnerable access point, instead of trying to establish two-way communication with Wi-Fi devices to test the password. A single Extensible Authentication Protocol over Local Area Network (EAPOL) frame can be used to get the information needed to attempt an attack. However, as in previous methods of attacking WPA, attacker must be in the vicinity of the network he/she wants to attack. It should be noted that not every network is vulnerable to this attack; PMKID is an optional package added by some equipment manufacturers, thereby a comprehensive success with this technique should not expected. Getting PMKID depends on whether the manufacturer of the target access point has included this field in the package and the password (defined by user) is easy to guess by dictionaries. Figure 3 shows a screen that presents hacking password with PMKID attack in Linux operating system.

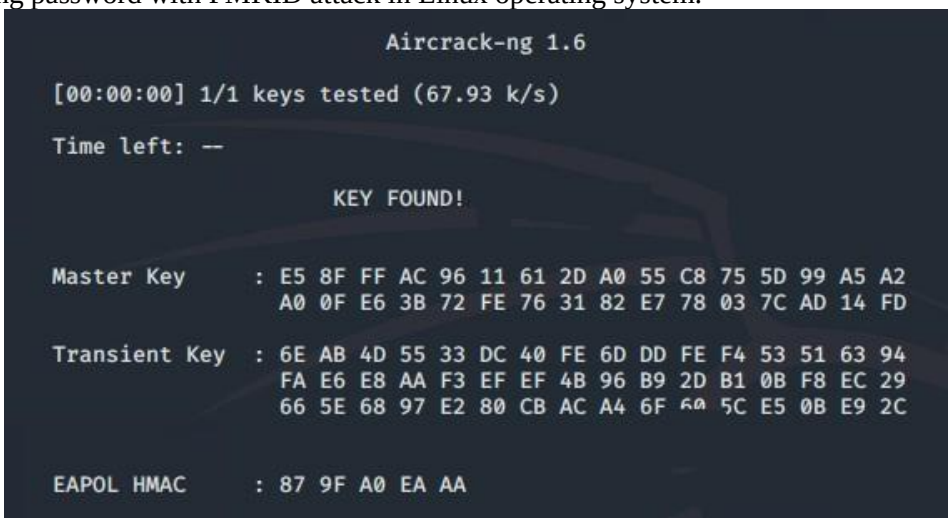


Figure 3. Screen presents hacking password with PMKID attack

#### 4.1.2.3. Evil-Twin attack

Although existing Wi-Fi security protocols are primarily focused on network protection, the protection concerns on the user side have been relatively neglected. Attacks such as Evil-Twin, in which an attacker fakes an access point, are still possible [29, 30].

In Evil-Twin approach, attacker steals Wi-Fi passwords while creating a fraudulent access point that seems to be legitimate to user [1, 11-13]. But that fraudulent access point is set up to eavesdrop on Wi-Fi network. Through this approach, an attacker can obtain end-users' personal information without users' knowledge.
In the fake network created by attacker, the victim user enters the password to access the unencrypted fake network on the phishing page that is being redirected to the victim. However, there are many differences between the phishing screen and the router home screen; a professional user may notice this attack, but it is effective against people who have not been trained in suspicious network behaviour. Once the victim has been connected to fraudulent access point, attacker can take further steps to identify victim's activities on the network. In this context, attacker can use software such as Ettercap 2 to perform a MITM attack. As the victim user is connected to fraudulent access point, attackers have almost a full access to the user's transit traffic and can analyse information transmitted through the network. Figure 4 illustrates the steps of the Evil-Twin attack on Wi-Fi networks.

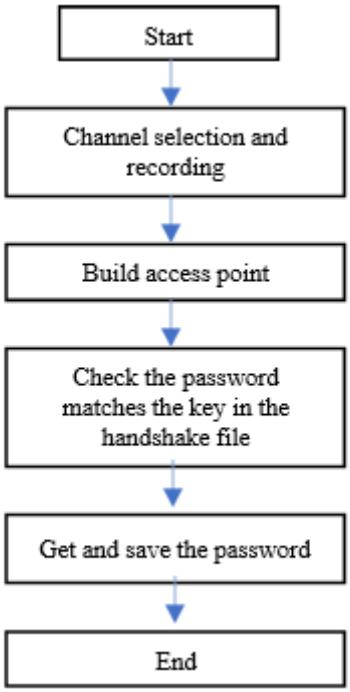


Figure 4. The steps of the evil-twin attack

### 4.2. Improve the security of wireless equipment

In this part of the research, we present five possible techniques to improve the security of Wi-Fi wireless networks against potential attacking attacks. These techniques are as follows.

1. Hiding network SSID. Hiding SSID aims to prevent user's wireless network name from spreading around. It is natural that if the network's name appears in the "list of available networks" to those around user, that would trigger attackers' motivation to penetrate those available networks.
2. Choosing strong password. Never use simple passwords or those relevant to user or his/her family. Using 123456 or user pet's name as Wi-Fi network password is like locking the door and placing the keys under the flowerpot next to the door. Attackers are smart enough to predict user's possible passwords. It is suggested to use a combination of letters, numbers, symbols and special characters in order to create a strong password.
3. Router shutdown. Turning Wi-Fi router off during long hours of non-use has several advantages. Initially, when the device is off, there are no waves in the environment that might be exposed to attackers allowing them to penetrate wireless networks. Additionally, turning Wi-Fi router off this will reduce the cost of electricity consumption and increase the life of router electronic components.
4. Using secure encryption. Strong encryption will prevent the attacker from infiltrating. Use the WPA2 protocol to improve Wi-Fi network security, and if this version is not supported, use the first version.

5. Wireless device update. Older software has a number of vulnerabilities that could be exploited by attackers to gain access to Wi-Fi network. Worse, most of the old software are obsolete and does not include technical support to users; developers may no longer release security patches for new holes. Users are suggested to be sure that their wireless devices are up to date with the latest version of software. Table 2 concludes our comparison between WEP and WPA-WPA2 security protocols.
6. Using narrow band filters are advantageous in enhancing the networking security as they reduce band interferences or restrict the operational bands based on wireless network requirements [31-34].

Table 2. Comparison between WEP and WPA-WPA2 security protocols

| | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| **Vulnerability** | Vulnerable against: DoS attacks, Bittau's fragmentation, and Chopchop. | Vulnerable against: Dos attacks, WPA-PSK, Chopchop, and Ohigashi-Morii. | Vulnerable against: DoS attacks. |
| **Replay attacks protection** | Not protected. | Protected by implements sequence counter. | Protected by implementation of 48-bit datagram/packet. |
| **Deployment complexity** | Easy deployment. | Easy deployment. | WPA-2 demands complicated setup. |
| **Hardware compatibility** | Possible to deploy on existing hardware. | Possible to deploy on existing as well as previous hardware. | Old Network Interface Cards (NIC) are not supported; 2006 and newer. |

## 5. Conclusions

Wireless networking is one of the most popular technologies worldwide. However, few users are aware of the security state and the intrusion of their Wi-Fi wireless network. Ordinary users often buy only one Wi-Fi router modem and set it up to default settings, without taking any further security considerations. This security ignorance could potentially be dangerous in exposing Wi-Fi networks to attackers. In this article, we analyse theoretical and practical studies on wireless network security with an in-depth investigation of various attacking methods on Wi-Fi wireless networks and the weaknesses of their security protocols. In this regard, we concluded that WPA-WPA2 protocols are found to be the best in terms of resisting attacks comparing to WEP. While we found all protocols vulnerable to be breaking when week passwords are used. However, experts suggest that if wireless card and router support WPA2, then WPA2 is the protocol that should be used to setting up wireless network. Experts' suggestion is in line with our findings.

## References

[1] M. R. Neamah, H. A. Thuwaib, and B. I. Farhan, "An analyzing process on wireless protection criteria focusing on (WPA) within computer network security", Periodicals of Engineering and Natural Sciences (PEN), vol.9, no.1, pp. 242-252, 2021.

[2] S. Ntontis, A. Khan, and J. Abdirahman, "Alternative ways of transferring data wirelessly: A comparison of wireless data transfer with goal of practical implementation at Hitachi ABB Ludvika", 2021.

[3] A. Terkawi, and N. Innab, "Major impacts of key reinstallation attack on Internet of Things system." 2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, 2018.

[4] R. Guo, "Survey on Wi-Fi infrastructure attacks", International Journal of Wireless and Mobile Computing vol.16, no.2, pp.97-101, 2019.
[5] A. Sari, and M. Karay, "Comparative analysis of wireless security protocols: WEP vs WPA", International Journal of Communications, Network and System Sciences, vol.8, no.12, p.483, 2015.
[6] H. I. Bulbul, I. Batmaz, and M. Ozel, "Wireless network security: Comparison of WEP (wired equivalent privacy) mechanism, WPA (Wi-Fi protected access) and RSN (robust security network) security protocols", Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, 2008.
[7] F. Fikriyadi, R. Ritzkal, and B. A. Prakosa, "Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method", Jurnal Mantik, vol.4, no.3, pp.1658-1662, 2020.
[8] Y. Wang, D. Liu, and M. Li, "A survey on hierarchical modulation for high-definition video transmission based on IEEE 802.11 n", 2010 IEEE 12th International Conference on Communication Technology. IEEE, 2010.
[9] R. R. Asaad, "Penetration Testing: Wireless Network Attacks Method on Kali Linux OS." Academic Journal of Nawroz University, vol.10, no.1, pp.7-12, 2021.
[10] Dimitrova, Vesna, and Stefan Pavlov. "A Note on a Successful WEP Attack." (2020).
[11] C. C. T. Teyou, and P. Zhang, "Solving downgrade and dos attack due to the four ways handshake vulnerabilities (WIFI)", International Journal of Engineering and Management Research (IJEMR), vol.8, no.4, pp.1-10, 2018.
[12] B. Rahnama, A. Sari and R. Makvandi, Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial Data Interconnect, 2013 International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), pp.579-582, 2013.
[13] M. Alioto, and S. Taneja. "Enabling ubiquitous hardware security via energy-efficient primitives and systems", 2019 IEEE Custom Integrated Circuits Conference (CICC), 2019.
[14] U. Banerjee, C. Juvekar, A. Wright, A.P. Chandrakasan, "An energy-efficient reconfigurable DTLS cryptographic engine for End-to-End security in IoT applications", In Solid-State Circuits Conference-(ISSCC), pp. 42-44, 2018.
[15] N. Pimple, et al, "Wireless security—an approach towards secured Wi-Fi connectivity", 6th international conference on advanced computing and communication systems (ICACCS). IEEE, 2020.
[16] Z. Liu, J. Großschädl, Z. Hu, K. Järvinen, H. Wang, I. Verbauwhede, "Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things", IEEE Transactions on Computers, vol.66, no.5, pp.773-785, 2017.
[17] S. Raza, L. Seitz, D. Sitenkov, G. Selander, S3K: scalable security with symmetric keys— DTLS key establishment for the Internet of things, IEEE Transactions on Automation Science and Engineering, vol.13, no.3, pp.1270-80, 2016.
[18] J. Li, et al., "A fast and scalable authentication scheme in IoT for smart living", Future Generation Computer Systems, vol.117, pp.125-137, 2021.
[19] M. Vink, E. Poll, and A. Verbiest, "A Comprehensive Taxonomy of Wi-Fi Attacks", MSc Thesis, Radboud University Nijmegen, 2020.
[20] K. Mahmood, S.A. Chaudhry, H. Naqvi, T. Shon, H.F. Ahmad, " A lightweight message authentication scheme for Smart Grid communications in power sector", IEEE Transactions on Smart grid, vol. 2, no. 4, pp.675-685, 2011.
[21] S. Frankel, B. Eydt, L. Owens and K. Scarfone, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, National Institute of Standards and Technology, NIST 800-97, 2007.

[22] S. Sciancalepore, Capossele A, Piro G, Boggia G, Bianchi G. Key management protocol with implicit certificates for IoT systems. In Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, pp. 37- 42, 2015.
[23] M. Mohammedi, et al. "Energy-aware key management and access control for the internet of things", World Wide Web, pp.1-32, 2021.
[24] M. Stute, et al., "Disrupting Continuity of Apple's Wireless Ecosystem Security: New Tracking, DoS, and MitM Attacks on iOS and macOS Through Bluetooth Low Energy, {AWDL}, and Wi-Fi." 30th {USENIX} Security Symposium ({USENIX} Security 21), 2021.
[25] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, W. Hu, Talos: Encrypted query processing for the internet of things. In Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, pp. 197-210, 2015.
[26] A. Sari and B. Necat, Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. International Journal of Ad Hoc, Sensor & Ubiquitous Computing, vol.3, pp.79-94, 2012.
[27] K.N. Prasetyo, Y. Purwanto, D. Darlis, an implementation of data encryption for Internet of Things using blowfish algorithm on FPGA, International Conference on Information and Communication Technology pp. 75-79, 2014.
[28] A. Sharma, T. Bhatia, and A. Katyar, "Wireless Security–An Introduction to Wireless Security Protocols and their Security Flaws", Annals of the Romanian Society for Cell Biology, vol.25, no.6, pp.11805-11812, 2021.
[29] I. ul Haq, and A. Kh. Tamim, "Penetration frameworks and development issues in secure mobile application development: A Systematic Literature Review", IEEE Access, vol. 9, pp. 87806–87825, 2021.
[30] Ş. Okul, and M. A. Aydın, "Security Attacks on IoT", International Conference on Computer Science and Engineering (UBMK), IEEE, 2017.
[31] Y. S. Mezaal and J. K. Ali, "Investigation of dual-mode microstrip bandpass filter based on SIR technique," *PLoS One*, vol. 11, no. 10, p. e0164916, 2016.
[32] Y. S. Mezaal, H. T. Eyyuboglu, and J. K. Ali, "Wide Bandpass and Narrow Bandstop Microstrip Filters based on Hilbert fractal geometry: design and simulation results," *PLoS One*, vol. 9, no. 12, p. e115412, 2014.
[33] Y. S. Mezaal and A. S. Al-Zayed, "Design of microstrip bandpass filters based on stair-step patch resonator," *Int. J. Electron.*, vol. 106, no. 3, pp. 477–490, 2019.
[34] Y. S. Mezaal, H. T. Eyyuboglu, and J. K. Ali, "A novel design of two loosely coupled bandpass filters based on Hilbert-zz resonator with higher harmonic suppression," in *2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT)*, 2013.