Common Security Protocols for Wireless Networks: A Comparative Analysis

Muhammad Ehsan Rana[1,*], Mohamed Abdulla[2] and Kuruvikulam Chandrasekaran Arun[3]

[1,2,3] *Asia Pacific University of Technology & Innovation, 57000, Bukit Jalil, Kuala Lumpur, Malaysia*
[*] *Corresponding author. Email: muhd_ehsanrana@apu.edu.my*

ABSTRACT
In computer networks, security is one of the most important aspects of protecting the network from various attacks. Especially in wireless networks, security can prevent unauthorized data access and save systems from potential threats. The security protocols in the wireless networks help to achieve the security process. Many protocols are designed to accomplish wireless security, which includes Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA) and WiFi Protected Access 2 (WPA2). This research paper discusses on the prominent wireless security protocols, that is, Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA) and WiFi Protected Access (WPA2) by providing a comparative analysis in terms of strengths and weaknesses of each protocol. In addition to that, the paper assesses each protocol in terms of authentication and encryption mechanisms and recommends the best wireless security protocol for a corporate network, which helps the network from unauthorized attacks.

Keywords: *Wireless Security Protocols, Wired Equivalent Protocol (WEP), WiFi Protected Access (WPA), WiFi Protected Access 2 (WPA2).*

1. INTRODUCTION

The wireless network is the most common type of network in which computers and network equipment are connected without using cables for exchanging information. The wireless network uses high-frequency radio waves to connect deceives, 2.4 GHz and 5GHz are the two prominent frequency bands used in the 802.11 Wireless LAN. This type of network will be the best networking solution for small firms.

The core component of the wireless network are routers, access points, and wireless-based computers. Unlike the wired network, the wireless network will be able to provide networking services to nearby devices, as the wireless network range is limited compared to the wired network. Wireless networks are classified into ad-hoc and infrastructure-based networks. All the wireless nodes are connected to an Access point or centralized unit in Ad-hock or peer-to-peer network. All the computers/nodes will be able to communicate directly and share the data. However, in order to communicate efficiently, the number of nodes should be limited [36-39].

On the other hand, a single access point will facilitate all the wireless nodes to communicate and share the data and resources. This type of network will be suitable for small and medium-size business as they do not need enormous effort to set up the entire network using wired media. Wireless networks are highly exposed to security threats, as the data is broadcast using a wireless medium. Both internal and external threats are more in the wireless network, as anyone who breaks the wireless security will be able to access the network. Rogue Access Point is one of the common security threats to this type of network. This access point is not legitimate, allowing others (outside of the business) to access the business resources without authorization from the network administrator. This type of access point is mostly set for sharing Internet services with nearby people without the knowledge of network administrators. Denial of Service is also one of the common security threats to wireless networks. A large number of requests are sent to the access point at once, which will slow down or stop the service of the network equipment [32-35] [40-43]. This paper focuses on the security protocols of wireless networks, describing the security protocols and the effectiveness of these protocols.

2. SECURITY PROTOCOLS

In this section, researchers have discussed the common security protocols. i.e. WEP, WPA and WPA2 for wireless networks.

2.1 WEP (Wired Equivalent Protocol)

WEP (Wired Equivalent Protocol) is a wireless security protocol introduced and ratified by the IEEE. Both IEEE 802.11 and IEEE 802.11i standards contain a description of this protocol, while IEEE 802.11i introduced a more advanced security mechanism to this protocol with the help of existing security measures [1]. The core reason for introducing this protocol is to provide encryption for data broadcast by the networking devices [2].

2.1.1. History

Ron Rivest first developed this protocol in the year 1987. However, it was implemented in 1997 by IEEE and labelled as IEEE 802.11 protocol [3]. Until 2005, this protocol was the most widely used protocol for businesses and individuals. Most of the networking components have a default configuration with this protocol. Since 2001, several weaknesses were identified in this protocol by cryptanalysts, which introduced a new protocol to provide security with the wireless network [4].

In 2005, the FBI demonstrated the weakness of this protocol by cracking the encrypted key in less than 3 minutes [2], [5]. After that, IEEE has declared that WEP is an obsolete protocol and WPA and WPA2 gets more popular in wireless security. As for the safety of the users, most of the devices will show a warning message when the user tries to use this protocol's service. However, this protocol is still in use, where security is not a significant concern.

2.1.2. Authentication

According to [6], IEEE 802.11 defines Open System and Shared Key WEP authentication. In open system authentication, the network will not have any security mechanism to prevent unauthorized access. In other words, anyone will be able to join the network without restrictions. Figure 1 shows WEP authentication process.

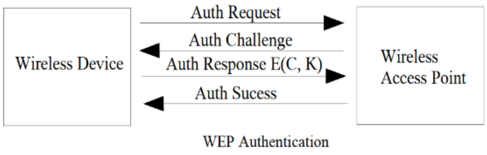

Figure 1 WEP Authentication [7].

By scanning the wireless signals, the wireless computer/nodes will be able to find the wireless access point by identifying the SSID of the wireless access point. The SSID is the broadcast name of the access point. At first, the wireless computer/node will send an authentication request following that the access point will send a random 128-bit text to the wireless device.

The wireless device will encrypt the random text by using a pre-configured key on the device. The encrypted text will be sent to the access point. Then the access point will decrypt the text, using its pre-configured. It will compare the original text and the decrypted text, and if it matches, access will be granted to the witless device. Then the access point will send permission granted replay message to the wireless device [6], [7].

2.1.3. Encryption - Rivest Cipher 4

The encryption algorithm used in this protocol is RC4 (Rivest Cipher 4) stream cipher. According to [2], this is a stream cipher cryptographic engine that enables encrypting the network traffic. Stream cipher RC4 was used to achieve the confidentiality of the data packets, while the CRC-32 checksum is used for the integrity of the data [3]. Using these two encryption algorithms, data is well protected during transmission. Due to the advancement of the technologies, the encryption algorithm used in this protocol provides a lack of security to the network and the data. In order to overcome this problem, the Temporal Key Integrity Protocol was introduced, which provides a wrapper to the WEP protocol.

2.1.4. Key

According to [1], a single key is shared between all the networking devices, which is referred to as Root Key (Rk). In most cases, a single key will be used. However, in exceptional cases, more than four keys will be used. 40-bit keys are used in the standard version of this protocol. The advanced version uses a 104-bit key, while some vendors implement this protocol in their devices having a 232-bit key to strengthen the encryption.

2.1.5. Strengths

It is a well-known fact that the impact of security protocol for transmitting the data over the wireless network is tremendous. Attackers have to make some effort in order to break the encryption of WEP. Not every user will be able to hack the wireless network and access the resource to the data will be protected to a certain level.

2.1.6. Weaknesses

There is a high degree of data manipulation and data loss in WEP as a shared key can be easily decoded by capturing the data. The integrity of the data cannot be guaranteed. In addition to that, key management is also an issue, as it does not maintain a proper key table leading to use the same key for a more extended period [8]. Poor key management exposed to a high threat to WEP networks. Apart from the key management, the size of the key is small, which provides a lack of security to the data packets. The 40-bit key is not enough to provide adequate security to the network [9]. The small size key opens the WEP networks for the attackers to implement brute force attack.

Moreover, the same initialization vector is being used in this protocol, enabling the attacker to decrypt without using the encryption key. The challenge-response scheme used in a shared key is a significant issue in the authentication process of WEP. There is no protection against packet forgery, while data packets can be forged using third-party applications and injected into the network [10].

2.1.7. Attacks / Treats

The most common attack for WEP is Keorek Chopchop Attack, where the attacker tries to decrypt the last bytes of plaintext using a 128-bit packet over the network. In this attack, the attacker modifies the captured data packet with his values and sends it back to the wireless access point [11]. If the attacker's guess is correct, the wireless access point will accept the data packet. This attack is highly possible, as there is a high possibility of guessing the last byte of the encrypted data encrypted in the data transmission. Another type of common attack is Bittu's Fragmentation attack. This type of attack is usually known as a fragmentation attack, where the attacker tries to find the key stream length after having the key stream [10].

2.2 WiFi Protected Access (WPA)

The WiFi Protected Access (WPA) is the wireless security protocol introduced by Alliance to overcome the security loopholes faced in the WEP protocol. This protocol was introduced in 2003, and still, this protocol is used in many devices to secure the witless network. This protocol is a subset of 802.11i, and it is designed to provide security to all versions of 802.11 devices, including 802.11a, 802.11b, and 802.11g. WPA uses the basic principle of WEP however, it rectifies its security problems by providing improvements in security problems of authentication and data integrity.

2.2.1. History

As security analysts have found weaknesses in the WEP protocol, there is a high demand for an improved protocol. WAP is not a new protocol as it is an enhancement for WEP protocol. WiFi Alliance developed WAP in 2003 by adding a security layer to the WEP protocol. WiFi Alliance is a non-profit international association established to carry out research work related to network securities. The flaws in WEP protocol resulted in introducing a new protocol by Alliance in 2003 [12]. In 2004, WEP protocol was declared an outdated security protocol for wireless networks, and it was replaced by WPA, which is more reliable and has a more robust algorithm. So the significant change in this protocol is a message integrity check to verify the data packets between the client and the wireless access point [13].

2.2.2. Authentication

Different authentication process is used for two versions of WPA protocol. For WPA Personal, PSK authentication has been used. On the other hand, EAP authentication is used for WPA Enterprise [14]. RADIUS is used to secure extensive networks by securing centralized management through access control. As there is no centralized authentication server in small offices (SOHO), the Pre-shared key is used to provide security to the network, enabling the users to get access by providing a password or a key [15]. Extensible Authentication Protocol (EAP) is the protocol used by the client during the authentication process. The authentication components in this protocol are the Client, Access Point (AP) and Network Access Server (NAS). The three-entity model was initially designed to use Point-to-Point Protocol (PPP) connections in a modem and Local Area Networks [16].

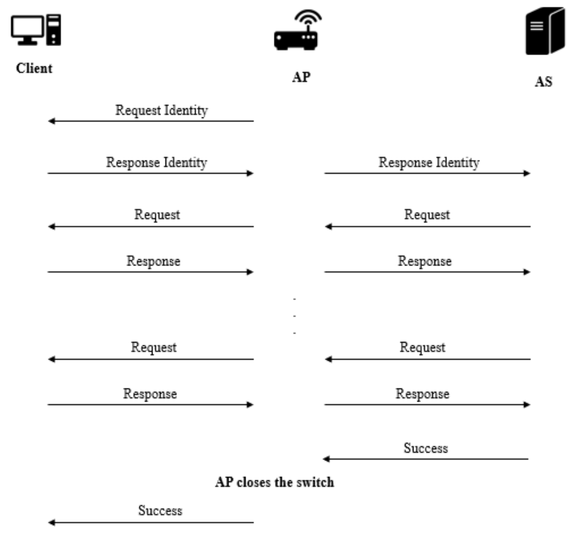

Figure 2 WPA Authentication uses NAS

In this model, the client obtains access to the network through the network access server in the network. When the client tries to connect to the access point, the request will be forwarded to the network access server by the access point. NAS initially blocks access to the client, and after verifying the client's authentication, the NAS will decide to grant permission or not. NAS act as a broker between the client and the access point [17]. Figure 2 shows WPA Authentication uses NAS.

2.2.3. Encryption - Temporal Key Integrity Protocol

TKIP algorithm acts as a wrapper to the old WEP algorithm, providing more security to the WEP without modifying the WEP security flaws. According to [6], TKIP is a cipher suite, an enhancement to the WEP protocol on pre - RSNA hardware. Through Temporal Key Hash (TKH) function, WEP integrated devices will be more secured over the wireless network communication. Due to the introduction of CCMP, the TKIP was considered a short-term solution, as CCMP is more advanced in providing security to the WEP [18]. Also, after the introduction of CCMP, the complicated calculation slowed down the entire network. There was an increase in the data packet size, which makes the network more inefficient [19]. Different keys are provided to do encryption in specified intervals. For every ten thousand data packets, temporal keys are changed. Due to this key mechanism, WPA networks are challenging to crack [20]. According to [13], TKIP uses per packet key system through a dynamic key mechanism and provides more security to the network. Advanced Encryption Standard (AES) is also used as an optional security enhancement for this protocol. After encryption keys are generated, a security verification will be done by configuring TKIP.

2.2.4. Key

In WPA, keys are generated on the authentication server, and these keys are validated and certified. Pre-shared key (WPA – PSK), usually known as WPA Personal, was used in this protocol. WPA-PSK uses a 128-bit encryption key, which will be insufficient to break down. According to [21], TKIP allows creating 280 trillion possible keys for a data packet, leading to offer a high-security key to the client.

2.2.5. Strengths

This protocol prevents forgeries by using the cryptographic Message Integrity Code (MIC). MIC is used to detect the error in data packets. The data packet may have an error due to the alteration of data packets or errors in data transfer. Using the Message Integrity Code, the wireless network will be secured from the man in the middle attack and DoS attacks. In addition to that, replay attacks are removed using a new Initialization Vector (IV). Moreover, the key relaying mechanism is used to provide a new and fresh key for data encryption, enabling the attackers to make it difficult to break the network [22].

2.2.6. Weaknesses

The Pairwise Master Key (PMK) implementation is weak as there is a loophole in Passphrase Choice in WPA Interface. Also, this security protocol is very much exposed to brute force attacks. The attacker will try every possible permutation to generate keys and decrypt the encrypted message. Attackers use file header and other data to compare and validate key in the process of cracking the key. Moreover, the Placement of MIC is considered as another issue. With the combination of a brute force attack, MIC can be used to validate the data in the decrypted message [23]. There is a high-security weakness when the security protocol is changed through firmware updates from WEP to WPA, as the weakness of WEP will still exist in WPA at a certain level [13].

2.2.7. Attacks / Treats

The introduction of Beck and Tews' attack, several weaknesses of TKIP was exposed, enabling the attacker to find an easier path to decrypt ARP and facilitates DoS attack on the network. Ohigashi-Morii Attack is another possible attack to WPA networks. This is an improvement of Beck and Tews' attack as time is reduced from 15 minutes to 1 minute to inject a fake data packet to the network. This attack is exposed to all models of the WPA protocol.

In addition to that, Michael Attacks and Hole196 vulnerabilities are also possible on this protocol. Hole196 vulnerabilities are a type of man-in-middle attack, where the attacker tries to manipulate the ARP request and updating ARP tables of other users. Moreover, a Dictionary attack is also a common attack on this protocol, where the attacker tries to obtain the security key by using different words from the dictionary file. The dictionary is a large text file with many different words with different characters [24].

2.3 Wi-Fi Protected Access 2 (WPA2)

Wi-Fi Protected Access 2 (WPA2) of IEEE 802.11i standard is developed in 2004 as an enhancement for WPA. Both encryption 802.1X/EAP authentication and PSK authentication is used in this protocol. The most significant change in this protocol is using the Advanced Encryption Standard (AES) for encryption. AES enables an adequate security level by ensuring that the current technologies are insufficient to break a WPA2 network.

2.3.1. History

WPA2 was introduced in June 2004 with the introduction of IEEE standard 802.11i. As WPA was introduced as a temporary solution for WEP devices, this protocol was introduced as a permanent /great lasting solution for wireless networking devices. Significant changes were introduced in this protocol, especially in the authentication process. Due to TKIP's weakness in the Message Integrity Check, a more secure algorithm was introduced into WPA2, i.e. CCMP (Counter Mode/CBC-MAC Protocol) [25]. AES encryption was created in October 2000 by, National Institute of Standards and Technology as a replacement for the RC4 algorithm. WPA2 is considered the most reliable wireless security protocol [27].

2.3.2. Authentication

WPA2 uses the same authentication mechanism used in WPA. The two types of key management systems are the authentication server and the pre-shared key. The pre-shared keys are mostly used in home and small business, where an authentication server is not needed. For Small Office Home Office (SOHO) environment, it will be not sufficient to establish an authentication server due to its complexity and cost. IEEE 802.11i protocol provides enough security to pre-shared key generation and usage [4].

Whereas, in a large organization, authentication servers are used. 802.1x key generation protocols are used to create matching Pairwise Master Keys (PMK). On both sides, i.e. Supplicants and the server sides. Whenever the client tries to connect to the access point four types of 128-bit temporal keys are generated. These keys are data encryption key, a data integrity key, EAPOL-key encryption, and EAPOL-key integrity key [28].

2.3.3. Encryption

WPA2 uses Advanced Encryption Standard (AES) algorithm for encryption and decryption, addressing both data privacy and integrity in the network. AES's symmetric-key algorithm enables the use of the same key for encryption and decryption [29]. AES is considered the strongest block cipher as it uses a minimum 128-bit key and text blocks that make the algorithm secure. AES chipper is mostly combined with robust and sophisticated cryptographic algorithm, i.e. Counter Mode Cipher Block Chaining Message Authentication Code Protocol, known merely as CMM mode Protocol. Here, Counter Mode AES is used for encryption, while CBC-MAC is used for authentication and integrity of the data [27].

2.3.4. Key

In this protocol, Pairwise Transient Key (PTK) is used to generate keys, allowing to have more secure keys of 128 bit to 256-bit keys. Only the authorized entities will know the generated key, so it enables to provide security to the data packets [30].

2.3.5. Strengths

The introduction of WPA2 provides enough security to the network users as it uses AES encryption to protect the data. Moreover, CMMP encryption provides encryption to the data packet header too, enabling the data and data packet to be well protected in this protocol. The well-known strength of this protocol is the length of the initialization vector (IV). 48-bits are allocated to overcome the weakness of using 24-bit used in previous protocols. Since brute force attacks, due to the complexity in the pre-shared key, are unpredictable and time-consuming, and disk usage may arise. PMK caching and pre-authentication support reduce the roaming time in streaming applications like video streaming and VoIP. The roaming time is reduced from 1 second to 1/10 second, which is a significant improvement in this protocol. PMK caching support enables wireless users to move from one access point to another without the need to re-authenticate on previously connected access points. Pre-authentication support enables the client to be authentic to the access point before moving to that access point, and the users will not realize the process happens, as it is a very fast and quick process [23].

2.3.6. Weaknesses

Until now, significant weakness is not discovered in WPA2; however, minor weaknesses exist in this protocol. The greatest weakness in WPA2 is the implementation of PSK. The strength of PTK relies on the strength of the PSK. According to [29], the second message of 4 way handshake in the authentication process of this protocol exposes to the dictionary and brute force attack. Moreover, there is a high processing power in this protocol. High ended hardware devices are needed to provide security to the network.

2.3.7. Attacks / Treats

The most common attack for WPA2 is DoS attacks, like RF jamming and data flooding, as none of the Wi-Fi security protocols prevents these types of attacks. These attacks operate on Layer 2 of the network, so the physical layer will not be able to prevent these attacks. Due to continuous requests sent to the access point, the access point will not respond to all the requests [31].

In addition to that the implementation of management frames enables the attacker to discover the topology used in the network. The attacker will be able to find the locations of the access point, which enables them to attack more quickly. Moreover, the use of Control Frames in the network opens DoS attacks from hackers [30].

While implementing re-authentication, there is a possibility of MAC address spoofing in this protocol, as there is a weakness in the implementation of the re-authentication protocol. The attacker is to make successful attacks when the user navigates from one access point to another access point.

3. CONCLUSION

In this paper, the three security protocols used in wireless networks are assessed, and each security protocol's strengths and weaknesses are identified. Through the information presented in this paper, network administrators and security specialists will be able to determine the most suitable wireless protocol for the wireless network that caters for their business needs. WPA2 protocol is the best protocol for Wi-Fi security, as this protocol provides several advantages over other protocols. One of the key reasons to choose the WPA2 protocol is that it uses AES encryption, a reliable encryption algorithm and is approved and recognized worldwide.

REFERENCES

[1] E. Tews, “Attacks on the WEP protocol,” IACR Cryptology ePrint Archive, 2007.

[2] M. Juwaini, R. Alsaqour, M. Abdelhaq, and O. Alsukour, “A review on WEP wireless security protocol,” Journal of Theoretical and Applied Information Technology, vol. 40, no. 1, pp. 39–43, 2012.

[3] N. Sun, “A Study of Wireless Network Security,” Governors State University, 2010.

[4] M. Abreha, “History and implementation of IEEE 802 security architecture,” IEEE Standards Education E-Magazine, 2016.

[5] G. Lehembre, "WiFi security – WEP, WPA and WPA2," Hakin9, 2005.

[6] M. Izhar, M. Shahid, and V. R. Singh, “Enhanced Security Evaluation and Analysis of Wireless Network based on MAC Protocol,” International Journal of Scientific and Research Publication, vol. 3, no. 11, pp. 1–4, 2013.

[7] S. Vibhuti, “IEEE 802. 11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability,” San Jose State University, CA, USA, 2005.

[8] D. B. N. Arif Sari, “Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism,” International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), vol. 3, no. 3, pp. 79–94, 2012.

[9] A. L. Vani B Associate Professor, “A Survey of Denial of Service Attacks and it’s Countermeasures on Wireless Network,” International Journal on Computer Science and Engineering, vol. 02, no. 05, pp. 1563–1571, 2010.

[10] 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.

[11] A. Sari, “Security issues in RFID Middleware Systems: Proposed EPC implementation for network layer attacks,” Transactions on Networks and Communications, vol. 2, no. 5, Oct. 2014.

[12] M. P. S and S. Pavithran, “Advanced Attack Against Wireless Networks Wep, Wpa / Wpa2-Personal and Wpa / Wpa2- Enterprise,” International Journal of Scientific & Technology Research, vol. 4, no. 08, pp. 147–152, 2015.

[13] S. Rawal, “How Wireless Security Can Be Compromised,” International Journal of Computer Science Trends and Technology (IJCST), vol. 4, no. 1, pp. 1–4, 2016.

[14] A. B. Gali and A. B. A. Mustafa, “A Comparative Study between WEP, WPA and WPA2 Security Algorithms,” International Journal of Science and Research (IJSR), vol. 4, no. 5, pp. 2390–2391, 2015.

[15] S. Malgaonkar, "Research on WiFi Security Protocols," International Journal of Computer Applications, vol. 164, no. 3, pp. 30–36, 2017.

[16] K. Baek, S. W. Smith, and D. Kotz, “A Survey of WPA and 802. 11i RSN Authentication Protocols,” Dartmouth College Computer Science, 2004.

[17] U. Kumar and S. Gambhir, “Analysis and Literature Review of IEEE 802.1x (Authentication) Protocols,” International Journal of Future Generation Communication and Networking, vol. 7, no. 4, pp. 25–34, 2014.

[18] J. Huang, W. Susilo, and J. Seberry, “Observations on the Message Integrity Code in IEEE 802. 11 Wireless LANs,” University of Wollongong, 2004.

[19] M. R. Doomun and K. M. S. Soyjaudah, “Modified Temporal Key Integrity Protocol for Efficient Wireless Network Security.,” in SECRYPT 2007 - International Conference on Security and Cryptography, 2007, pp. 151–156.

[20] A. I. Angela, “Evaluation of Enhanced Security Solutions in 802.11-Based Networks,” International Journal of Network Security & Its Applications (IJNSA), vol. 6, no. 4, pp. 29–42, 2014.

[21] F. H. Katz, “WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?” in 2010 4th Annual

Computer Security Conference (CSC 2010), 2010, pp. 1–4.

[22] M. Mohi, E. Adam, A. Gasim, and E. Abdallah, "WiFi Security," International Journal of Advances in Engineering and Management (IJAEM), vol. 2, no. 2, pp. 143–149, 2015.

[23] M. S. Prastavana, S.P. and Praveen, "Wireless Security Using WiFi Protected Access 2 (WPA2)," International Journal of Scientific Engineering and Applied Science (IJSEAS)-ISSN, vol. 2, no. 1, pp. 374–382, 2016.

[24] M. Caneill and J. Gilis, "Attacks against the WiFi protocols WEP and WPA," Journal, 2010.

[25] A. H. Adnan et al., "A comparative study of WLAN security protocols: WPA, WPA2," in Proceedings of 2015 3rd International Conference on Advances in Electrical Engineering, ICAEE 2015, 2016, pp. 165–169.

[26] M. Vanhoef Imec-Distrinet, "WiFuzz: detecting and exploiting logical flaws in the WiFi cryptographic handshake WiFuzz: detecting and exploiting logical flaws in the WiFi handshake," imec-DistriNet, 2018.

[27] S. Alblwi, K. Shujaee, and C. Atlanta, "A Survey on Wireless Security Protocol WPA2," in International Conference on Security and Management - SAM17, 2017, pp. 12–17.

[28] G. M. Pérez, S. M. Thampi, R. Ko, and L. Shu, "A Survey on WiFi Protocols:WPA and WPA2," Springer-, Berlin, 2014.

[29] M. M. Armin Akte, A.K.M. Nazmus Sakib, Fariha Tasmin Jaigirdar, "Security Improvement of WPA 2 (WiFi Protected Access 2), "International Journal of Engineering Science and Technology (IJEST) Security, vol. 3, no. 1, pp. 723–729, 2011.

[30] E. B. Barker and A. Roginsky, "Recommendation for Cryptographic Key Generation," NIST Special Publication 800-133, 2012.

[31] P. Arana, "Benefits and Vulnerabilities of WiFi Protected Access 2 (WPA2)," Global Journal of Computer Science and Technology, vol. 612, pp. 1–6, 2006.

[32] Kiran, P., Parameshachari, B.D., Yashwanth, J. and Bharath, K.N., 2021. Offline Signature Recognition Using Image Processing Techniques and Back Propagation Neuron Network System. SN Computer Science, 2(3), pp.1-8.

[33] Jagannathan, P., Rajkumar, S., Frnda, J., Divakarachari, P.B. and Subramani, P., 2021. Moving Vehicle Detection and Classification Using Gaussian Mixture Model and Ensemble Deep Learning Technique. Wireless Communications and Mobile Computing, 2021.

[34] Vadivel, S., Konda, S., Balmuri, K.R., Stateczny, A. and Parameshachari, B.D., 2021. Dynamic Route Discovery Using Modified Grasshopper Optimization Algorithm in Wireless Ad-Hoc Visible Light Communication Network. Electronics, 10(10), p.1176.

[35] Nguyen, T., Liu, B.H., Nguyen, N., Dumba, B. and Chou, J.T., 2021. Smart Grid Vulnerability and Defense Analysis Under Cascading Failure Attacks. IEEE Transactions on Power Delivery.

[36] Nguyen, N.T., Liu, B.H., Pham, V.T. and Luo, Y.S., 2016. On maximizing the lifetime for data aggregation in wireless sensor networks using virtual data aggregation trees. Computer Networks, 105, pp.99-110.

[37] Nguyen, N.T. and Liu, B.H., 2018. The mobile sensor deployment problem and the target coverage problem in mobile wireless sensor networks are NP-hard. IEEE Systems Journal, 13(2), pp.1312-1315.

[38] Prabu, S., Velan, B., Jayasudha, F.V., Visu, P. and Janarthanan, K., 2020. Mobile technologies for contact tracing and prevention of COVID-19 positive cases: a cross-sectional study. International Journal of Pervasive Computing and Communications.

[39] Arun, M., Baraneetharan, E., Kanchana, A. and Prabu, S., 2020. Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors. International Journal of Pervasive Computing and Communications.

[40] K. Yu, Z. Guo, Y. Shen, W. Wang, J. C. Lin, T. Sato, "Secure Artificial Intelligence of Things for Implicit Group Recommendations", IEEE Internet of Things Journal, 2021, doi: 10.1109/JIOT.2021.3079574.

[41] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, F. A. Khan, "Securing Critical Infrastructures: Deep Learning-based Threat Detection in the IIoT", IEEE Communications Magazine, 2021.

[42] L. Tan, K. Yu, F. Ming, X. Cheng, G. Srivastava, "Secure and Resilient Artificial Intelligence of Things: a HoneyNet Approach for Threat Detection and Situational Awareness", IEEE Consumer Electronics Magazine, 2021, doi: 10.1109/MCE.2021.3081874.

[43] L. Tan, N. Shi, K. Yu, M. Aloqaily, Y. Jararweh, "A Blockchain-Empowered Access Control Framework for Smart Devices in Green Internet of Things", ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1-20, 2021,https://doi.org/10.1145/3433542.