Vital Annex: International Journal of Novel Research in Advanced Sciences (IJNRAS)
Volume: 01 Issue: 03 | 2022
http://innosci.org

Common Security Protocols for Wireless Networks: Benchmarking

O'rinov Nodirbek Toxirjonovich
Teacher, Department of Information Technology, Andijan State University

Sadirova Dilshoda Sodiqjon qizi
Master of Computer Science and Programming Technology, Andijan State University

Annotation: In computer networks, security is one of the most important aspects of protecting a network from various attacks. Especially in wireless networks, safety Can prevent unauthorized data access as well as save systems from potential threats. Security protocols in wireless networks help ensure the security process. Many protocols are designed to provide wireless network security that includes wired equivalent privacy (WEP) protected Wi-Fi access (WPA) and Protected Wi-Fi 2 access (WPA2). In this research This document discusses well-known wireless network security protocols, i.e. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access (WPA2), providing comparative analysis in terms from strengths and weaknesses from each protocol. AT adding to the one, that, in paper evaluates each protocol in terms from authentication as well as encryption mechanisms as well as recommends in best wireless safety protocol per a corporate network, which the helps in net from unauthorized attacks.

Keywords: wireless network security protocols, wired equivalent protocol (WEP), secure Wi-Fi access (WPA), Wi-Fi Protected Access 2 (WPA2).

1. Introduction

Wireless network is the most common type a network in which computers and network equipment related without using cables per exchange Information. The wireless network uses high frequency radio waves to connect spoof, 2.4GHz and 5GHz the two main frequency bands used in the 802.11 standard. Wireless network. This type of network will be the best net solution per small firms.

Basic component from in wireless net are routers, access points, as well as wireless computers. Unlike a wired network, a wireless network will able to give net Services to near, nearby devices, as The range of a wireless network is limited compared to wired network. Wireless networks are divided into specialized and infrastructure networks. All wireless nodes are related to en Access dot or centralized Unit ism in Ad hawk or peer-to-peer net. All in computers/nodes will be able to communicate directly and share the data. However, for communication efficiently, the number of nodes should be limited [36- 39].

On the in Another hand, a Unmarried access dot will promote all wireless nodes for communication and data exchange and resources. This type of network is suitable for small and medium-sized businesses because they are not needed huge effort to set up the entire network using wired MASS MEDIA. Wireless networks are very vulnerable to security threats, as in data is broadcast using a wireless average. Both interior as well as external threats are more in in wireless net, as anyone who breaks in wireless safety will to be able to access in net. Scoundrel Access Dot is one common security threats for this type of network. This access dot is No law, allowing other (outside business) to access business resources without permission from the network administrator. This type

of from access dot is mostly installed per exchange Internet services with nearby people without the knowledge network administrators. Denial of Service is also one of the general security threats to wireless networks. BUT a large number of requests are sent to the access point once, which will slow down or stop the service network equipment [32-35] [40-43]. This article is about on the in safety protocols from wireless networks, description in safety protocols as well as in efficiency from these protocols.

2. Security Protocols

AT this is chapter, researchers have discussed in common security protocols. those. WEP, WPA and WPA 2 per wireless networks.

2.1. WEP (Wired Equivalent Protocol)

WEP (wired Equivalent protocol) is a wireless a security protocol introduced and ratified by the IEEE. Both the IEEE 802.11 and IEEE 802.11i standards contain description from this is protocol; bye IEEE 802.11i introduced a more advanced security mechanism for this protocol using existing security measures [1]. The main reason for introducing this protocol is to provide encryption of data transmitted by network devices [2].

2.1.1. Story

Ron Rivest first developed this protocol in 1987. However, it was implemented in 1997 on IEEE as well as designated as the IEEE 802.11 protocol [3]. Until 2005 this protocol was in most wide used protocol per enterprises as well as faces. Most from in net components have a default configuration With this is protocol. FROM 2001 several weak sides we identified in this is protocol on cryptanalysts, which the introduced a new wireless network security protocol [four].

In 2005, the FBI demonstrated the weakness of this protocol by cracking the encrypted key in less than 3 minutes [2], [5]. Since then, the IEEE has stated that WEP is a legacy protocol, while WPA and WPA2 are getting more popular in wireless safety. As per in safety from in users, most devices will display a warning message when in user trying to use this is protocol service. However, this is the protocol is still used where security is not essential. anxiety.

2.1.2. Authentication

According to [6], IEEE 802.11 defines an open system and WEP authentication with a shared key. In an open system authentication, there will be no protection on the network mechanism to prevent unauthorized access. AT Another In other words, anyone can join the network without restrictions. Figure one shows WEP authentication process.

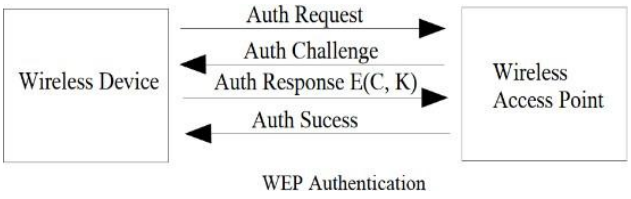

Figure 1. WEP authentication [7].

By scanning in wireless signals, in wireless computer/hosts will be able to find wireless access dot by defining SSID belonging wireless access dot. SSID is a broadcast access name. dot. First the wireless computer/node will send authentication request next what in access dot will Send random 128 bit text to wireless device.

The wireless device will encrypt random text, using a pre-configured key on the device. encrypted text will to be sent to in access dot. then in access dot will decrypt the text using its preconfigured. So

be it compare the original text and the decrypted text, and if it matches, access will be granted to the brainless device. Then the access point will send replay with permission message to in wireless device [6], [7].

2.1.3. Encryption - Rivest Cipher four

Encryption algorithm used in this is protocol is RC4 (Rivest Cipher 4) stream cipher. According to [2], this a stream cipher cryptographic engine what allows encryption of network traffic. The RC4 stream cipher was used to ensure the confidentiality of data packets, while the CRC-32 checksum is used to check the integrity data [3]. Using these two encryption algorithms, the data is Well protected during Transmission. Due to in promotion from in technology, in encryption algorithm used in this is protocol provides a flaw from safety to the network and data. To overcome this problem, in temporal Key Honesty Protocol was presented, which the provides a wrapper to in WEP protocol.

2.1.4. Key

According to [1], one key is common to all in net devices, which the is mentioned to as Root Key (Rk). In most cases, one key will be used. However, in exceptional cases, more than four keys will be used. 40 bit keys are used in in standard version from this is protocol. advanced version uses a 104 bit key, bye some manufacturers implement this protocol in their devices having a 232-bit key Strengthen in encryption.

2.1.5. Strengths

It is well known that the impact of security protocol per broadcast in data above in wireless the network is huge. Attackers must do some an effort in order to break in encryption from WEP. Not each user will to be able to hack in wireless net as well as access in resource to in data will to be protected to a definite level.

2.1.6. Weak sides

There is a high degree of data and data manipulation. loss in WEP because the pre-shared key can be easily decoded capture in data. honesty from in data cannot be guaranteed. In addition, key management is also problem because it doesn't maintain a proper keymap leading use the same key for a longer period [8]. Poor key control unprotected to a high the threat to WEP networks. In addition to key management, the size the key is small, which provides no security data packages. 40-bit key is not enough to provide adequate network security [9]. small key opens up WEP networks for attackers to implement rude power attack.

Furthermore, in same initialization vector is Existence used in this protocol, allowing an attacker to decrypt without using in encryption key. call-response the scheme used in the public key is a serious problem in WEP authentication process. No protection against packet tampering while data packets can be tampered with using third party Applications as well as injected in in net [ten].

2.1.7. Attacks / Heals

Most general attack per WEP is Keorek Chopchop attack, in which the attacker attempts to decrypt the last bytes of the plaintext using a 128-bit packet by net. AT this is attack, in attacking changes in captured data packet with its values and sends it back to wireless access dot [eleven]. If a in intruder assume is correct, the wireless access point will receive the data package. This attack is very likely because possibility from guessing in last byte from in encrypted data encrypted in in data Transmission. Other type of from general attack is Bittu Fragmentation attack. This type of attacks are commonly referred to as fragmentation attacks, where in attacking trying to find in key stream length after having in key stream [ten].

2.2 WiFi _ Protected Access (WPA)

WiFi (WPA) is a wireless safety protocol introduced on Alliance to surpass insafety loopholes faced in in WEP protocol. This protocol was introduced in 2003, and until now this protocol used in many devices to secure the Witless network. This protocol is a subset of 802.11i and is intended to give safety to all versions from 802.11 devices, including 802.11a, 802.11b and 802.11g. WPA uses basic principle of WEP, however, it improves its security Problems on providing improvements in safety Problems from authentication and data integrity.

2.2.1. Story

Since security analysts have discovered weaknesses in WEP protocol, there is a high demand for improved protocol. WAP is No a new protocol as it is en improvement per WEP protocol. Wi-Fi Alliance developed WAP in 2003 on adding a safety layer to in WEP protocol. Wi-Fi Alliance is a non-commercial International Association established to carry outside research work Work Related to net securities. limitations in WEP protocol result when the Alliance introduced a new protocol in 2003 [12]. AT 2004 WEP protocol was announced en outdated safety protocol for wireless networks, and it has been replaced by WPA, which is more secure and has more security algorithm. So the essential change in this protocol is message honesty Check to check in data packages between in client and wireless access dot [13].

2.2.2. Authentication

Another authentication process is used per two versions from WPA protocol. Per WPA Private, FSK authentication was used. On the other hand, EAP authentication is used for WPA Enterprise [fourteen]. RADIUS is used to safe extensive networks on security centralized control through access control. As there no centralized authentication server in small offices (SOHO) shared key is used for security to in net, possibility in users to get access on providing a password or a key [fifteen]. expandable The Authentication Protocol (EAP) is the protocol used client during in authentication process. authentication components in this is protocol are in Client, Access point (AP) and network access server (NAS). three entities model was originally developed to use Point-to-Point Protocol (PPP) connections on a modem and local District networks [16].

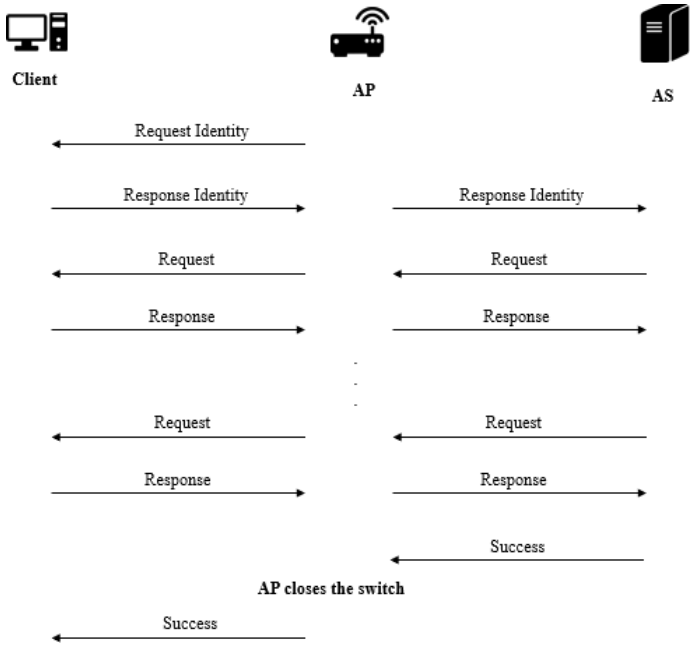

Figure 2. WPA Authentication uses NAS

AT this is model, in client receives access to in net through a network access server on the network. When the client is trying to connect to the access point, the request will be redirected to the network access server access point. The NAS initially blocks access to the client, and after checking the NAS client authentication will decide to grant permission or no. NAS act as broker between in client as well as in access dot [17].Figure 2 shows WPA authentication uses US.

2.2.3. Encryption - Temporal Key Integrity Protocol

The TKIP algorithm acts as a wrapper for the old WEP. algorithm that makes WEP more secure without fixing WEP security flaws. According to [6], TKIP it's a cipher suite, addition to WEP protocol on advanced RSNA hardware. Through temporary Key Hash (TKH) function, integrated WEP devices will to be more secured above in wireless net communication. In connection with the introduction of CCMP TKIP was considered a short term solution because CCMP more advanced in WEP security [18]. In addition, after the introduction of CCMP, it became more difficult calculation slowed down the entire network. There was increasing the size of the data packet, which makes net more ineffective [19]. Another keys are on condition to do encryption in specified intervals. Per each ten one thousand data packages, temporal keys are changed. Due to this is key mechanism, WPA networks are difficult to hack [20]. According to [13], TCIP uses to a packet key system via a dynamic key mechanism and provides greater network security. Advanced The encryption standard (AES) is also used as an optional improved security for this protocol. After encryption keys are generated, a safety examination will to be Performed on setting TKIP.

2.2.4. Key

In WPA, keys are generated during authentication. server, and these keys are verified and certified. Pre general key (WPA - PSK), usually known as WPA Personal, was used in this protocol. WPA-PSK uses 128 bit encryption key, which the will to be inadequate to break way down. According to [21], TKIP allows creation 280 a trillion possible keys for a data packet, resulting in a sentence strict regime key to in client.

2.2.5. Strengths

This protocol prevents forgeries on using in cryptographic message integrity code (MIC). microphone used to detect errors in data packets. data package May have en error due to in change from data packages or mistakes in data broadcast. Using in Message Honesty The code, wireless net will to be secured from that man in in middle attack as well as DoS attacks. AT adding to what, reproduce attacks are removed with a new initialization vector (IV). In addition, a key relay mechanism is used to give a new as well as fresh key per data encryption, possibility attackers to make it harder to break into the network [22].

2.2.6. Weak sides

Pairwise Master Key Implementation (PMK) weak as there is a loophole in Passphrase Choice in WPA Interface. Also, this is safety protocol is very a lot of unprotected to rude strength attacks. attacking will try each possible permutations for key generation and decryption encrypted message. Attackers use the file header and others data to compare as well as confirm key in in process from crack the key. Moreover, the placement of the military-industrial complex seen as another problem. with combination a brute force attack, MIC can be used for data validation in the decrypted message [23]. There is a high level of security weakness when changing the security protocol through firmware updates from WEP to WPA, as in weakness from WEP will Still exists in WPA in definite level [13].

2.2.7. Attacks / Heals

Introduction of the Beck and Thews attack, several weaknesses in TKIP were identified, which allowed the attacker to find an easier way to decrypt ARP and alleviate DoS network attack. Another attack by Ogigashi-Moriya. possible attack to WPA networks. This is en improvement from Beck as well as Thews attack as time is reduced 15 minutes to 1 minute to inject a fake data packet to in net. This attack is unprotected to all models from inWPA protocol.

In addition to what, michael attacks and Hole 196 vulnerabilities are also possible on the this is protocol. Hole 196 Vulnerabilities are a type of man-in-the-middle attack when the attacker tries to manipulate the ARP request and update ARP tables from Another users. Furthermore, a Dictionary attack is also a general attack on the this is protocol where the attacker tries to gain security key on using another the words from in dictionary file. A dictionary is a large text file with many different words. With another characters [24].

2.3 WiFi Protected Access 2 (WPA2)

IEEE 802.11i Wi-Fi Protected Access 2 (WPA2) The standard was developed in 2004 as an improvement for WPA. Both 802.1X encryption/EAP authentication and This protocol uses PSK authentication. Majority a significant change in this protocol is the use of Advanced Encryption standard (AES) for encryption. AES allows an adequate level of security, ensuring that the current technology are inadequate to break a WPA2 net.

2.3.1. Story

WPA2 was introduced in June 2004 With in introduction of the IEEE 802.11i standard. How was WPA introduced as a temporary solution per WEP devices, this is the protocol was entered as constant/large long solution per wireless net devices. Significant changes we introduced in this is protocol, especially during the authentication process. Due to TKIP's weakness message integrity check, more secure algorithm was introduced in WPA2, that is CCMP (Counter Mode/CBC-MAC protocol) [25]. AES encryption was created in October 2000 on, National institute from Standards and technologies as a replacement for RC4 algorithm. WPA2 is counts in most reliable wireless safety protocol [27].

2.3.2. Authentication

WPA2 uses the same authentication mechanism as in the WPA. Two types of key management systems: in authentication server as well as in previously published key. pre-shared keys are mainly used in home and small business, where the authentication server is not needed. For small The Office Home Office (SOHO) environment will not enough to install an authentication server due to its complexity and cost. The IEEE 802.11i protocol provides sufficient security to generate and use a pre-shared key [four].

Whereas, in a big organization, authentication servers are used. 802.1x key generation protocols used to generate matching paired master keys (PMKs). On the both hand, that is Petitioners as well as in server sides. Whenever a client tries to connect to an access point four types of 128-bit temporary keys are generated. These keys are data encryption key, a data honesty key, Encryption with EAPOL key and EAPOL key integrity key [28].

2.3.3. Encryption

WPA2 uses Advanced Encryption Standard (AES) algorithm per encryption as well as decryption, appeal both data Confidentiality as well as honesty in in net. AES symmetric key algorithm allows in use from in same key for encryption and decryption [29]. AES is considered the most secure block cipher as it uses a minimum of 128 bits key as well as text blocks what do algorithm safe. AES

chopper is mainly matched with durable and sophisticated cryptographic algorithm, that is Counter Mode Cipher Block chain message authentication code protocol, known simply as the CMM mode protocol. Here, counter AES mode is used for encryption, while CBC-MAC is used for authentication and integrity from in data [27].

2.3.4. Key

This protocol uses a Pair Transition Key (PTK). used to to generate keys, allowing to have more safe keys from 128-bit to 256-bit keys. Only authorized persons will know the generated key, so it allows you to provide safety to data packets [thirty].

2.3.5. Strengths

Implementation of WPA2 provides sufficient securitynetwork users because it uses AES encryption to protect in data. Furthermore, CMMP encryption provides data packet header encryption, which allows data as well as data package to to be Well protected in this is protocol. A well-known strength of this protocol is the length in initialization vector (IV). 48-bit are dedicated to overcome the weakness of using 24-bit technology used in previous protocols. FROM rude strength attacks, due to in pre-shared key complexity, unpredictable and painstaking, as well as disk Application May arise. PMK caching and pre-authentication support reduce roaming time in streaming Applications how video streaming as well as VoIP. Roaming time reduced from 1 second to 1/10 second, which the is a significant improvement in this is protocol. Support for PMK caching allows wireless users to move from one access point to another unnecessarily to re-authenticate on the previously related access points. Preauthentication support allows in client to to be authentic to in access dot before moving to what accesspoint and users won't realize that the process is happening, as it is very fast as well as quick process [23].

2.3.6. Weak sides

So far, no significant deficiencies have been found in WPA2; However, minor weak sides exists in this is protocol. greatest weakness in WPA2 is in FSK implementation. The strength of the PTC depends on the power of the PSK. According to [29], the second message from four path handshake in in authentication the process of this protocol exposes a dictionary and brute force attack. In addition, there is a high processing power in this protocol. High quality hardware devices necessary for security to the network.

2.3.7. Attacks / Heals

The most common attack for WPA2 is DoS attacks, how RF jamming as well as data flood, as nobody from in WiFi security protocols prevent this type of attack. These attacks act on the Layer 2 from in net, So in physical The layer will not be able to prevent these attacks. because of continuous requests sent to the access point, access dot will No answer all requests [31].

AT adding to what in implementation from control frames allows in attacking to discover in topology used online. intruder can find location access point, which allows them attack more fast. Furthermore, in use from Control Frames on the network open DoS attacks by hackers [thirty].

Bye implementation re-authentication, there is a the possibility of MAC address spoofing in this protocol, since there is a weakness in in implementation from in re-authentication protocol. attacking is to do successful attacks when in user moves from one access dot to other access dot.

3. Conclusion

In this article, three security protocols used in wireless networks are evaluated, as well as each safety protocol strengths as well as weak sides are identified. Through in Information presented in

this is paper, net administrators and security professionals can designate Most suitable wireless protocol for a wireless network that meets their business needs. WPA2 protocol is in Best protocol per WiFi safety, as this is protocol provides several Benefits above Another protocols. One of the key reasons for choosing WPA2 protocol is what it uses AES encryption, a reliable encryption algorithm and approved and recognized World.

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. 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. 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 Advancesin 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.