ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 1, February 2022, pp.632-644

Enhanced IoT Wi-Fi protocol standard's security using secure remote password

Hiba A. Tarish
Civil Engineering Department, University of Technology, Baghdad-Iraq

ABSTRACT

In the Internet of Things (IoT) environment, a network of devices is connected to exchange information to perform a specific task. Wi-Fi technology plays a significant role in IoT based applications. Most of the Wi-Fi-based IoT devices are manufactured without proper security protocols. Consequently, the low-security model makes the IoT devices vulnerable to intermediate attacks. The attacker can quickly target a vulnerable IoT device and breaches that vulnerable device's connected network devices. So, this research suggests a password protection based security solution to enhance Wi-Fi-based IoT network security. This password protection approach utilizes the secure remote password protocol (SRPP) in Wi-Fi network protocols to avoid brute force attack and dictionary attack in Wi-Fi-based IoT applications. The performance of the IoT security solution is implemented and evaluated in the GNS3 simulator. The simulation analysis report shows that the suggested password protection approach supports scalability, integrity and data protection against intermediate attacks.

Keywords: Brute force attack, Dictionary attack, Intermediate attacks, IoT security solutions, secure remote password protocol, Wi-Fi network protocols,

Corresponding Author:

Hiba A. Tarish
Civil Engineering Department
University of Technology
Baghdad-Iraq
Email: Hiba.A.Tarish@uotechnology.edu.iq

1. Introduction

The Internet of Things (IoT) [1] provides interactive network enabling services without using a keyboard or screen's interaction. A network of objects or appliances, and people are connected through the internet to provide interactive services. The technology utilizes the internet's power to automatically collect information [2] from the device and perform data analysis to make intelligent decisions based on the application requirement.

The IoT technologies are utilized in many application services such as smart home monitoring [3, 4], environment monitoring [5, 6], industrial equipment automation, health monitoring[7], inventory management etc. The IoT network enables many interactive services such as machine to machine, human to machine, and machine to human interactions. Generally, the IoT network services are enabled by protocol standards [8, 9]. The adapted protocol services define the interaction between sensor devices, gateways, access points, applications and users. Manufactures introduces many protocols based on the customer's primary needs.

The standard protocol helps to avoid data or connection fragmentation and to reduce security risks. Some of the popular IoT protocol services are constrained application protocol (CoAP) [10], message queuing telemetry transport (MQTT) [11, 12], Wi-Fi [13], ZigBee [14], Bluetooth, Extensible Messaging and Presence Protocol (XMPP)[15], Data Distribution services(DDS), Advanced Message queuing protocols (AMQP)[16], etc.

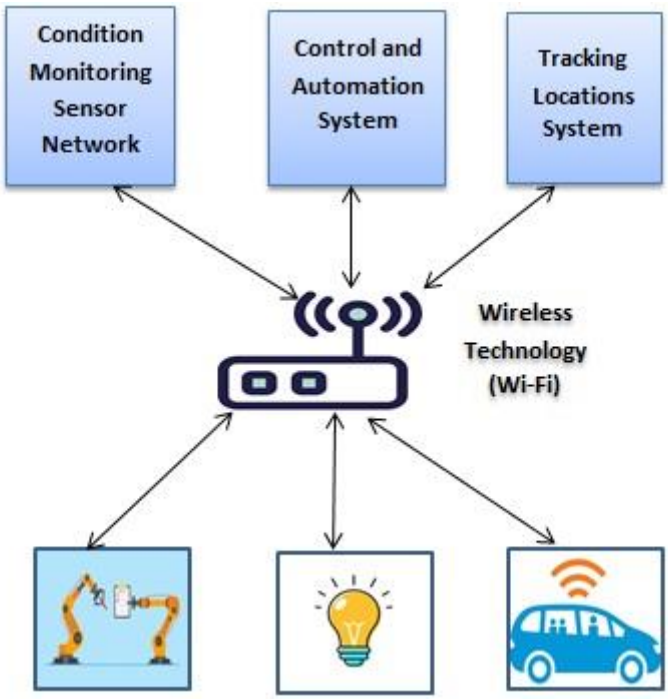


Figure 1. Wi-Fi technology-based IoT applications

Figure 1 shows some popular IoT applications utilizing Wi-Fi technologies to perform automation at low cost and short-range. Among these IoT protocols, Wi-Fi technology [17] is trendy among the customers for its short-range and low-cost interactive services. Due to this technology's popularity, manufacturers rush to build IoT Wi-Fi device without specifying any good standard protocol-based security services. The low protocol models make the IoT device vulnerable to intermediate attacks [18]. Therefore, in this research, a secure password-based security model reduces the security risks in Wi-Fi network standard-based IoT applications. It combines the Wi-Fi standard's basic features and SRP protocol's secret key encryption generation and verification to enhance password protection against dictionary attacks and brute force attacks. The protocol security extension helps to find out feasible IoT configurations for Wi-Fi network. The feasible IoT configurations are identifies by analyzing the simulated parameter's outcomes. Moreover, this research is suggesting suitable node's configuration parameter for IoT smart home application to establish secure communications. The rest of the research is organized as section 2 discusses the related works on IoT security, and section 3 discusses the security issues in Wi-Fi-based IoT. Section 4 discusses the Wi-Fi module's and SRP protocol-based security extensions, and section 5 discusses the simulations results and their discussions. Section 6 discusses the conclusion of the IoT security-based research findings.

2. Related works

This section discusses the various authors' research experience on IoT network's security. It helps to identify the research gaps and strengths and weaknesses of advanced security systems of IoT protocol environments.
This research [19] analyzed the wireless network's security issues and identified end to end security services as challenging tasks. Enhanced wireless network security is introduced to achieve this challenging task named Eclipse curve cryptography (ECC). This approach encrypts the data in a 164-bit platform, and to breach the network, 1024 bit platform is defined. This research [20] combined machine learning and artificial intelligence to detect attacks in the wireless network. It's analyzing each IoT device's behaviour, which is connected with a wireless network environment to detect insecure devices. In this, the insecure devices are identified using sensor devices' abnormal traffic behaviour using the intelligent technique. This study [21], Introduced a machine learning approach to detect vulnerable subnet detection approach. In this, the Support vector machine method is used to detect abnormal traffic behaviours of each device. The density-based clustering method clusters the infected devices and their subnet devices using random behaviour of even sequence. The evaluation results show that the binary classifier and density clustering-based attackers behaviours and infected node detection have a maximum 94.8 % precision rate in attack detection. The security of IoT mobility nodes is evaluated [22] using three existing mobility models. In this analysis, a graphical model is utilized to detect the potential

attacker's path detections in mobility changing devices such as mobile phone, smart TV etc. The detection process is explained with two use cases. In [23], tree-based fabrication attack detection and defence strategies are developed for Wi-Fi network-based IoT devices. Initially, it performs entity and message fabrications. It then identifies spoofing in entity spoofing, and packet reply and pocket foraging are conducted in message fabrication. In the final stage, IDS is defined to detect the spoofing, authentication is performed for all the packets to detect replay attack, and data freshness is implemented to discard old packets. Generally, the encryption and decryption approaches are utilized to protect the data from attackers; on the other hand, this study [24] introduced attack based password retrieval and decryption technique for L2TP/IP Sec Protocol layer. This research [25] evaluated the performance of the security extension of IoT communication protocol. Based on each extension's simulation analysis report, this research suggested that the CoAP with DTLT approach as a reliable security extension for smart grid application's environment. This study [26] introduced a Zigbee protocol security model to reduce the reply attack in Zigbee-related IoT applications. The performance of this security model is analyzed using various IoT end devices for all the Zigbee topologies. This research [27] reviewed the functionalities, limitations, and specifications of the IoT MAC layer's protocols and applications. This review is performed for the short-range wired and wireless protocols and long-range wired and wireless protocols. This study [28] designed a nested attributed meta-graph architecture-based security approach to protect vulnerable IoT devices against attacks. This architecture performs the supervisory control and Data accusation (SCADA) techniques to establish secure data transmission in public networks for IoT protocols.
This in-depth study [29] analyzed the functionalities and vulnerabilities of various network security protocols. It covers the various security protocol model's authentication techniques, public-key cryptography techniques, key agreement techniques etc. This study [30] recommended an easily adaptable and manageable software and hardware-based security verification approach. It verifies each level of organizational operation's security at the design phase. The operating system's security features are enabled to detect unauthorized security access in the software model. The hardware model ensures the data protection of both sides of IoT devices during the data transmission. This research [31] designed an end to end security model for organizational plans. It helps organizations to plan strategies and disclosures. In this, the data gathering approach analyze and measure the overall security of IoT organizations. This study [32] analyzed the security attacks for each layer of IoT reference models. It also suggested a four-layered IoT reference model layers based security approach. It contains the perception layer, edge computing layer, network and cloud layers. This research [33] analyzed the vulnerabilities of a password protecting protocol. This protocol not storing the secret keys directly in server, it stores the key in encrypted password form. It is specially designed to reduce dictionary attacks. Some of the researches are utilizing machine learning and artificial network approaches to ensure IoT applications' security. Some researches utilize hardware and software-based solutions to ensure IoT security. Few research types are focused on establishing security in protocol levels by establishing security extension policies. All approaches are focused on ensuring data protection from cyber-attacks. Due to the availability of automated software attackers such as brute force attacks and dictionary, attackers can quickly enter even into the protected environment by targeting one or a few systems in a connected environment. In this situation, the existing system's data protection policies failed to protect the devices from attackers. In this research, an encrypted password approach is incorporated to provide security for wireless network-based IoT applications. It applies cryptographic policies for the password to protect from attackers. In this case, attackers can't guess the encrypted passwords even if they try to access the device's information to take control.

3. Security issues in Wi-Fi-based IoT

Fluhrer, Mantin and Shamir (FSM) attack is also known as FMS [34] attack. It permits the hackers to recover the encoded key in an RC4's. It is using a key scheduling algorithm to reconstruct the encoded large number of the frame. It requires a large number of the frame to succeed.

Korek and ChopChop attack can able to decode the wired equivalent privacy data packets without knowing the key. It does not retrieve the key; however, it can able to expose the actual text. It requires a minimum of one data packets to decode the entire packets data.

The Internet Protocol (IP) datagram fragmentation is one of the DoS attacks [35]. All the packets transmitted over the Wi-Fi standards use a common header so the attacker can guess the first 8 bytes of data quickly. The rest of the parts are extracted from the Initialization Vector (IV). It has several forms of attacks, such as user

datagram protocol and Internet Control Message Protocol (ICMP) fragment attack and Transport Control Protocol (TCP) fragment attack.

Pyshkin Tews Weinmann (PTW) attack [36] is an improved form of FSM attack. It decreases the requirement of the initialization vector count to retrieve the WEP key. It can retrieve 104 bit of the WEP key with more than a 50% success rate. It guesses the wireless traffic on the same channel as the target frames. However, it requires a large amount of time to collect the necessary frame information. So, re-inserts frames in the response path to create traffic to retrieve the frame information more quickly.

In Google reply attack, attackers can retrieve all the log streams by merely setting the Google search engine as default. Generally, this type of attackers may send mail to the target system or ID and notify them to reset the password. The hackers can retrieve partial information about the logs.

The Michael algorithm is generally used to create hash functions. But the Michael attack is performing the de-hashing. In this, hackers can insert code in data packets.

In Ohigashi-Morii attack, the time taken to inject a malicious packet in-network is decreased. The time taken to perform the packet injection is reduced from 15 minutes to 1 minute.

The Hole 196 vulnerability attack allows the known user in the same network to access other's resources using the WPA 2 and wireless network. The IEEE standard 802.11 contains the documentation for these vulnerability attacks.

In the Brute force attack [37], the attackers submit a set of possible password's combinations, log information, encryption key, and hidden web page to determine the matching password combinations to access the information. Generally, a set of the automated bot is utilized to perform this attack. The attacks are performed in various form such as Simple brute force, Dictionary attack, hybrid brute force, revere brute force, and credential stuffing. The simple BF approach is to guess the simple form of password or PIN. The hackers try possible password combinations on the targeted system to enter the profile in a dictionary attack. The hybrid approach combines the dictionary and other brute force method to form a combo of password combinations. In credential stuffing, the hybrid approach predicted password combo of one site is utilized to breach many websites. The password guessing process is performed using automated tools. It uses several techniques to obtain the matches, such as dictionary mode, weak password prediction, decoding the password from the encoded passwords stored location, and trying all the possible character combinations.

Dictionary attack is one of the BF attacks. It gains access by guessing the possible set of the password and tying the previously saved passwords. It guesses and tries the possible password or passphrases for thousands and millions of times to determine the matches to gain access. The sequential attack is mostly used to reveal the password. Some attackers' uses complete dictionary of words and its combinations of alphabets, numeric and special characters to found the matches. The research is focused on reducing brute force and dictionary attack based issues in Wi-Fi standard modules. The subsequent section discusses the security extension techniques of Wi-Fi standards, which discusses the specifications of Wi-Fi standards, SRP protocol's encrypted secret key generation and authentication process, and a use case is explaining how the SRP Protocol avoids brute force and dictionary attack in Wi-Fi-based IoT application.

4. Enhanced Wi-Fi network's security using secure remote password protocol (SRPP)

This section discusses the Specification features of Wi-Fi standards and describes the SRPP's encryption and secret key exchange strategies. Then it demonstrates how the SRP protocol is enhancing the security of Wi-Fi modules in IoT applications using two use cases, such as brute force and dictionary attacks.

Table 1. Abbreviation table

Abbreviations	Description
WLAN	Wireless Local Area Network
CoAP	Constrained Application Protocol
MAC	Media Access Control
Wi-Fi	Wireless Fidelity
ISM	Industrial, Scientific and medical (applications of radiofrequency energy)
OFDM	Orthogonal frequency division multiplexing

DSSS	Direct sequence spread spectrum.
CSMA/CA	Carrier sense multiple access with collision avoidance
LLC	Logical link control
TDLS	Tunnelled direct link setup
NDP	Null Data packets
RAW	Restricted Access Window
PS mode	Power saving mode
TWT	Target wave time
SST	Sub-channel selective transmission
MIMO	Multi-Input Multi-Output
MU-MIMO	Multi-User –MIMO
FHSS	Frequency-hopping spread spectrum
CCK	Complimentary Code Keying
SRP	Secure Remote Password Protocol
BPSK & QPSK	Binary Phase Shift Keying & Quadrates Phase Shift Keying
M-QAM	M-ary Quadrature amplitude modulation

4.1. Wi-Fi Protocol standards

It is one of the IoT short-range communication protocols widely used by customers in many IoT applications. It is a simple wireless networking technology standardized by IEEE for WLAN. Generally, the trouble-free high-speed data transmission feature of this Wi-Fi protocol is the main reason for choosing it to establish communications in many IoT applications. It is one of the IEEE 802.11 standard's families. It provides in-build brand band coverage. It provides the airway concept to establish a connection between wireless IoT clients or Wireless IoT clients and base stations.

Table 2. Basic Wi-Fi IEEE standards

	802.11b	**802.11a**	**802.11g**
Frequency band	2.4 GHz ISM	5 GHz U-NII	2.4 GHz ISM
Channel bandwidth	25 MHz	20 MHz	20 MHz
Duplexing	Half	Half	Half
Maximum Signal Data rate	11 Mbps	54 Mbps	54 Mbps

Table 2 contains the basic 802.11 protocol standard's specification details. The Wi-Fi protocols contains several IEEE standard versions such as Wi-Fi 1(802.11), Wi-Fi 2(802.11b), Wi-Fi 3(802.11a), Wi-Fi 3E(802.11g), Wi-Fi 4 (802.11n), Wi-Fi 5(802.11ac), Wi-Fi 6(802.11ax), Wi-Fi 6E(802.11ax), etc. Among this three first four version are unbranded services.

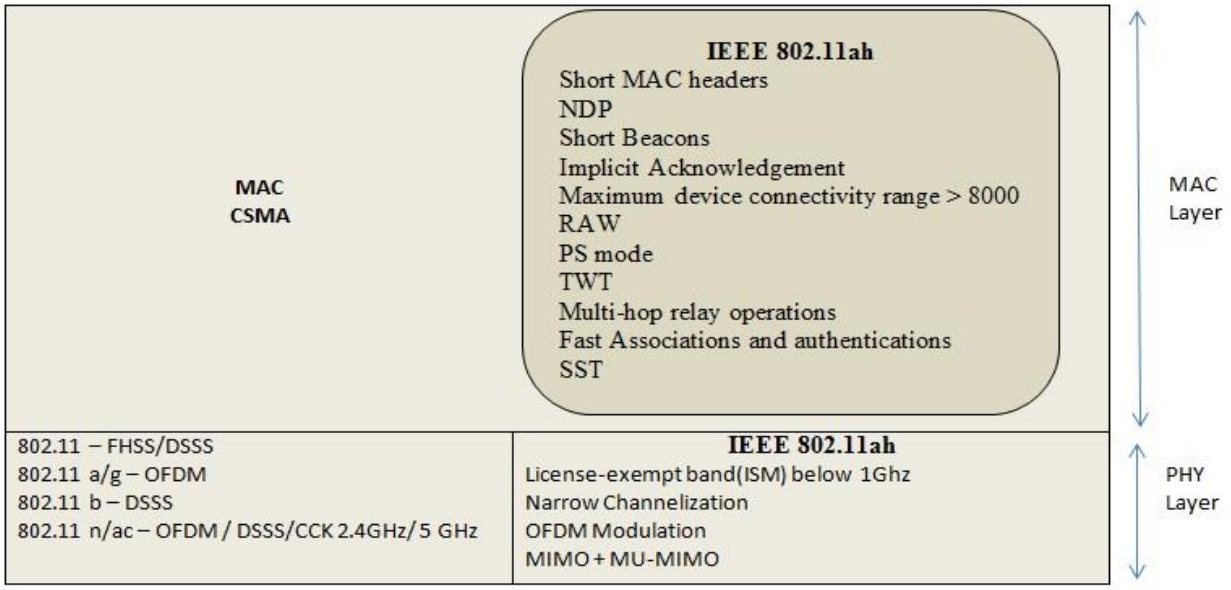


Figure 2. IEEE 802.11 standards Wi-Fi technology

Figure 2 [30] describes the standards of the IEEE 802.11 protocols; it follows OSI reference mode's Physical (PHY) and MAC layers. These standards are designed to establish communications between peer to peer devices. The layer supports frequency bands from 2.4 GHz to 5GHz with OFDM and DSSS. It adapted the multiple beams forming technology to enhance the data transmission rate from 2 Mbps (802.11) to 600 Mbps (802.11n). The median of access supported by this standard is CSMA/CA. The IEEE standard 802.11 has several attractive features: security and power-saving mechanisms, Acknowledgement in MAC layer level, roaming support, inter-frame gaps and exponential back-off, fragmentations, and resemble support, synchronization. The standards use a best-effort delivery mechanism to LLC. Consequently, data transmission is not guaranteed. Therefore, the MAC layer is employed for these standards to manage the data relay in the ISO layer's high-level protocols. In the MAC layer, NDP is carrying a null data payload of a wireless client. It contains RAW and PS mode. The RAW is restricting authorized access to other wireless client's information. The TWT permits an AP to manage the Wi-Fi network activity to reduce the medium contention between Stations (STA's); it also allows to set the minimum required amount of time the station is awake to PS mode. The access point (AP) /a station / by both is determining the capacity of SST. It supports many (multi-hop) relay operations such as a fixed relay, mobile relay etc. In PHY layer, the base station or AP using MIMO/ MU-MIMO/ FHSS technology; it uses multiple transceivers for each cell sector. The IEEE 802.11 n/ac supports CCK. In infrastructure mode, all the communications are performed through base stations. The communications within the network are established using additional airwaves. In ad hoc and Wi-Fi direct mode, it can establish communications between two computers without using any intermediate access points. In TDLS, two devices on the same network can communicate directly without access point support. The modulation types supported by the Wi-Fi standards are BPSK, QPSK, COFDM, CCK, M-QAM. The IEEE standard 802.11h supports the dynamic frequency selection transmits power control method. This standard supports a 32-bit cyclic redundancy check (CRC) to provide data protection. It establishes connections to cell nodes maximum of >2007. It uses 14 radio frequency channels to produce data signals. The Specifications and the functionalities of some of the Wi-Fi standards are discussed in these sections. The Wi-Fi technology is trendy among the customers and IoT developers for its attractive features, discussed in this section. Consequently, the manufactures rush to build IoT Wi-Fi device without specifying any good security policies. The low-security protocol adoption makes the Wi-Fi-based IoT device vulnerable to intermediate attacks. This research suggests a secure secret keying to reduce the security risks in Wi-Fi network standard-based IoT applications. The subsequent section discusses the functionalities of the SRP protocol.

4.2. Secure remote password (SRP) protocol

This protocol is used to form a known secret session key ssK and password PS for IoT Client Device and IoT Application server node. In this, the password or key matching is performed in prime group Y_r. The notation q represents a sizeable prime integer. The notation i represents the generator of prime numbers. The SRP uses the hash function $hash$. In this, any session password key z is $\in Y_r$. The prime group Y_r is denoted as $i^z \bmod r$. Initially, the IoT device must register its password to the Application server. The server saves the value (s, u) indexed by the IoT device. The notation s indicates the encryption, and the derivative $z = hash(s, PS)$ is the encrypted hash value of the IoT device's password. The non-sensitive verifier is represented as $u = i^z$, which is derived from the password PS. The PS does not reveal the x or PS. This process is performed in two stages, such as Key establishment and Key verification. The step-by-step key establishment and verification process for IoT client device and IoT application server is explained as flows,

I. IoT Device and it's application server form session key ssK.

1. IoT Device sends its identity to the server.
2. The server receives IoT Device's identity and searching for IoT Device's encrypt s and saved verifier $u = i^z$, and the z is contained $z = hash(s, PS)$. The server sends IoT Device's encrypt s to IoT Device.
3. IoT Device receives s, calculates and sends i^c to server.
4. The server receives i^c and generates a random secret nonce d and random scrambling parameters. The server calculates and sends $u + i^d$ to IoT Device, together with u.
5. Both server and client devices compute the session key ssK as the hash of a common value, which both server and client devices compute differently. IoT Device computes $ssK = hash((u + i^d) - i^z)^{c+uz}$ and Server computes $ssK = h(i^c i^{uz})^d$.

II. Alias and Server verifies the session key

6. IoT Device computes $N_1 = hash(i^c, u + i^d, ssK)$ and sends N_1 to Server. The server verifies the received value by re-computing$N_1 = hash(i^c, u + i^d, SSK)$.
7. The server computes $N_2 = hash(i^c, N_1, ssK)$ and sends it to IoT Device. IoT Device verifies the received values by re-computing $N_2 = hash(i^c, N_1, SSK)$
8. If these two-verification process is to succeed, then the session key ssK is verified.

The low-cost Wi-Fi-based wireless network is using inadequate password protection and key exchange policies to provide security. It makes the Wi-Fi-based IoT application vulnerable to Dictionary attacks and Brute force attacks. Therefore, in this research, the Wi-Fi module's secret key password protection is enhanced using a secure remote password protocol. This protocol encrypts the shared secret key with a maximum number of prime groups. Suppose the attackers try to guess the secret key by combining number; also, the automated attacker's bot can't know the actual count of the secret key. The possible attacks and the key protection schemes are explained using the use case in the subsequent section.

4.3. Dictionary attacks and brute force attacks in Wi-Fi module based IoT smart home environment

This section explains the two possible attacks in IoT application in Wi-Fi modules. This research is focused on enhancing the secret key protections against brute force and dictionary attacks. The attacks and the key protection process has been described using the IoT based smart home-based use case.

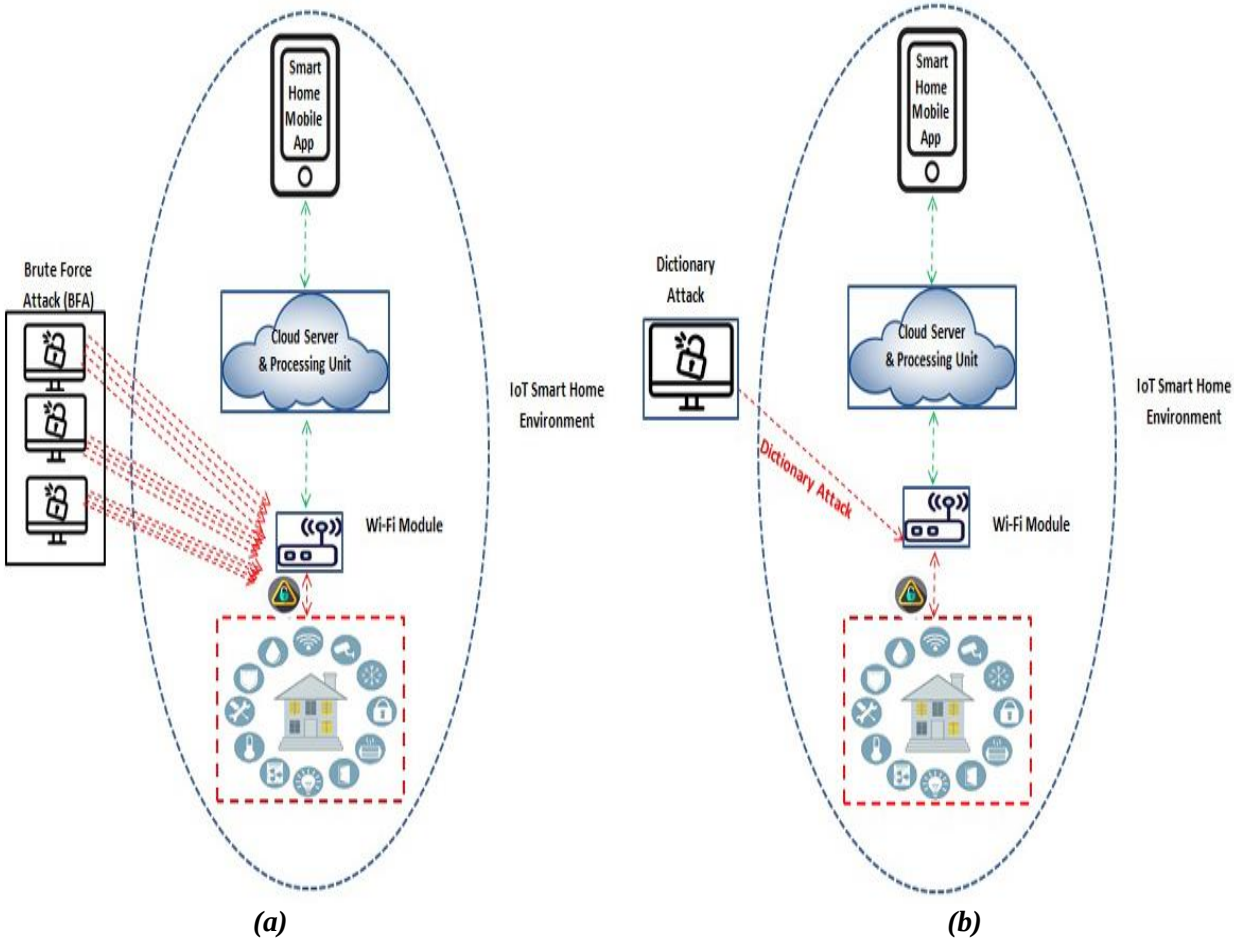


Figure 3. Wi-Fi Module based Smart home environment (a) Brute force attack (b) Dictionary attack

Figure 3 a) illustrates the brute force attack in a Wi-Fi-based IoT smart automation application environment. In this, each infected device submitting a possible password by guessing combinations. This illegal password submissions process is mostly performed using automated bots until the correct password matches. Figure 3 b) illustrates the Dictionary attack in a Wi-Fi-based IoT smart automation application environment. This attack

is also a kind of brute force attack, but it attempts to defeat the protocol's cryptographic techniques by guessing the possible combinations.

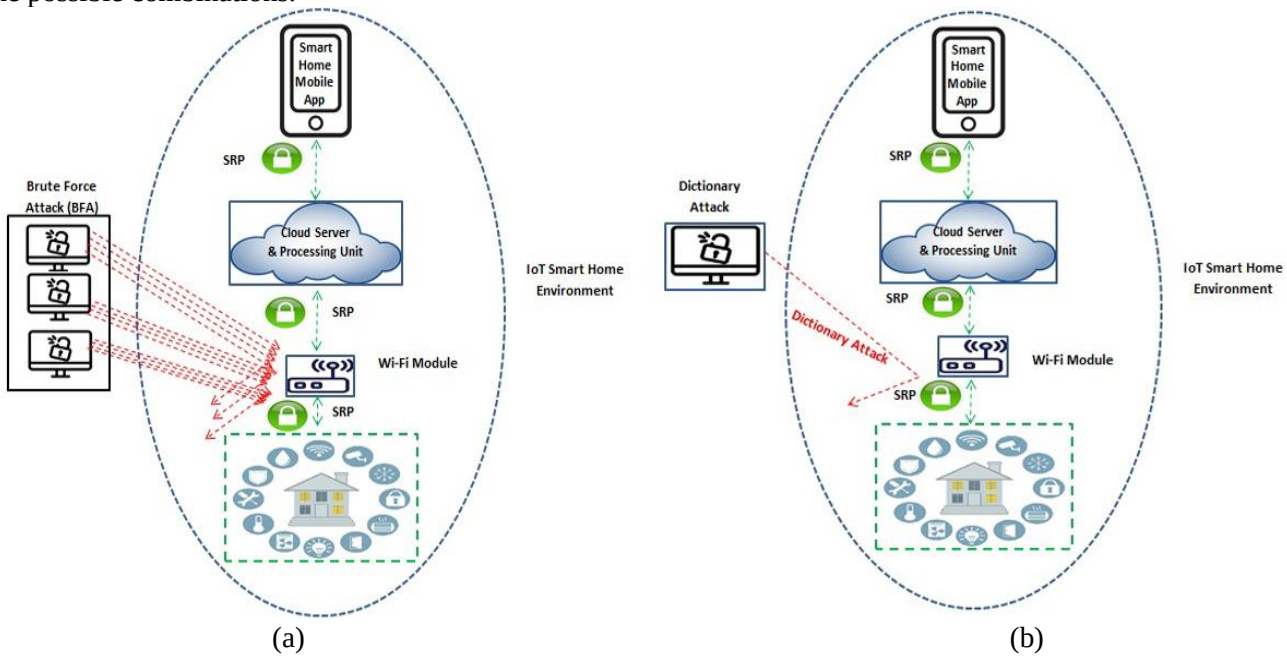


Figure 4. Wi-Fi Module based Smart home environment (a) Protected from Brute force attack using SRP Protocol, (b) Protected from Dictionary attack using SRP Protocol

Figure 4 a) illustrates the brute force attack and SRP protocols based enhanced security in Wi-Fi-based IoT smart automation application environment. In this, each infected device submitting a possible password by guessing combinations. However, SRP protocol is utilized a large number of encrypted prime number group series to encrypt the secret keys. Therefore, suppose the attackers try to guess the secret key password combinations also they can't guess the exact combinations of the actual secret key password. Figure 4 b) illustrates the Dictionary attack in a Wi-Fi-based IoT smart automation application environment. Suppose the dictionary attacker attempts to defeat the cryptographic techniques by guessing the password. Also, they can't get the exact combination of the existing password to decrypt the secret key. The SRP protocol establishes the secret key and password protection for all three layers of the IoT smart home environment. The subsequent section discusses the simulation results and analysis of the Wi-Fi protocol's enhanced security using SRPP.

5. Results and discussions

This section discusses the performance analysis of the enhanced Wi-Fi module's security. This protocol setup is implemented and tested with network performance monitoring metrics using the GNS3 tool. The enhanced Wi-Fi module's security is simulated using 50 data packets, 12 simulated IoT nodes, and 10 MB of comprehensive data. The enhanced Wi-Fi security performance is evaluated with the IoT security model's evaluation metrics such as packet overhead, integrity, network latency, and scalability. Lots of researches are introduced a security mechanism to enhance the Wi-Fi network's security. However, the Eclipse curve cryptography (ECC) approach [15] and the tree-based authentication (TA) approach [19] are provides better security against intermediate attacks for Wi-Fi network's IoT applications. Therefore, these two approaches are chosen to compare the Secure Remote Password protocol enhanced Wi-Fi security modules.

5.1. Latency analysis

The latency rate comparison is performed for Wi-Fi module with SRPP, Wi-Fi module with ECC, and Wi-Fi module with AP approaches are illustrated in figure 5. The latency is analyzed by increasing the number of tasks and utilized response times. It comparison graph shows that the Wi-Fi module with SRP protocol takes less response time (59(ms) to 598(ms)) to perform the secret key creation ($ssK = hash((u + i^d) - i^z)^{c+uz}$), $ssK = h(i^c i^{uz})^d$ and authentication tasks and packet transmission using large prime groups. It proves that the secret key generation process in SRPP protocol obtains a very less latency rate than comparison approaches.

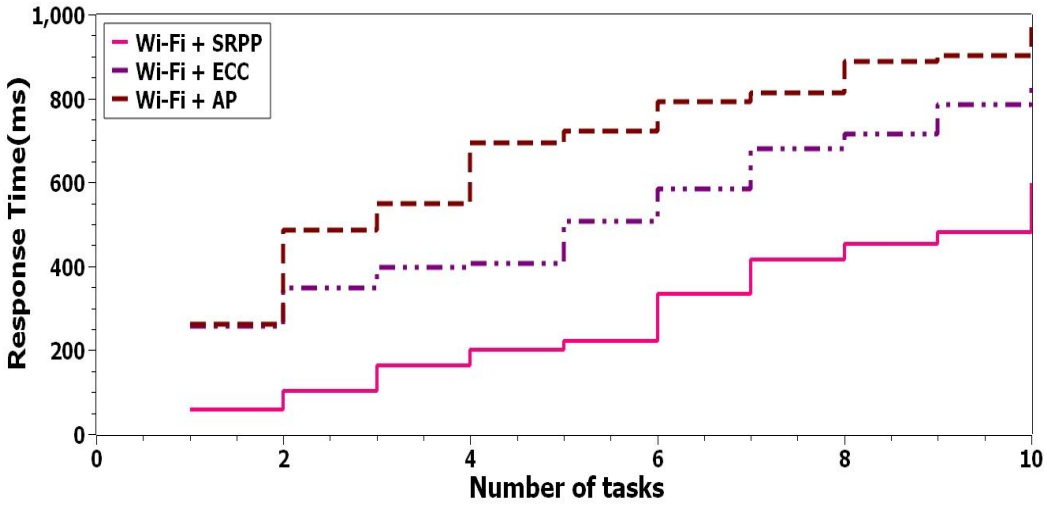


Figure 5. The latency rate comparison

5.2. Scalability analysis

The scalability rate comparison is accomplished for Wi-Fi module with SRPP, Wi-Fi module with ECC, and Wi-Fi module with AP approaches are illustrated in figure 6. The scalability is estimated by the number of nodes and each node's overall task completion time. It comparison graph shows that the Wi-Fi module with SRP protocol takes less overall response time (512(ms) to 6175(ms)) than comparison methods to complete all the secret key encryption and key authentication process for all the nodes.

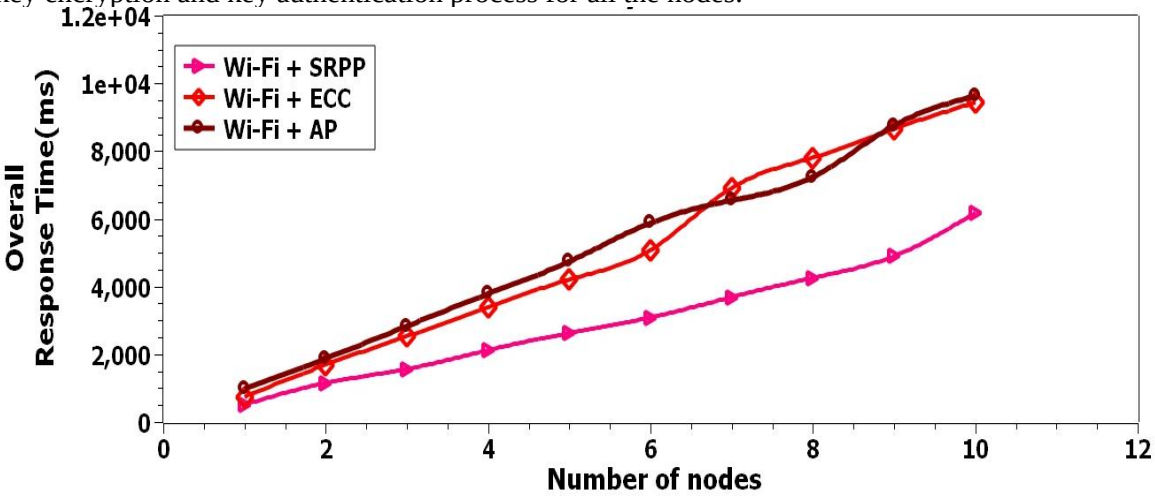
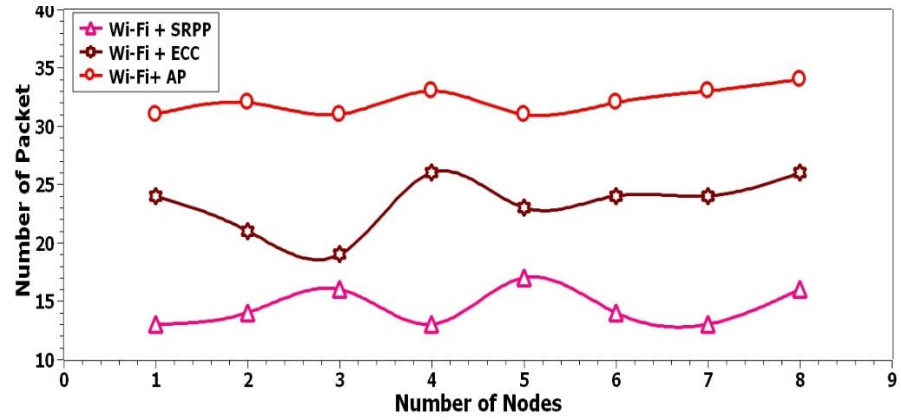


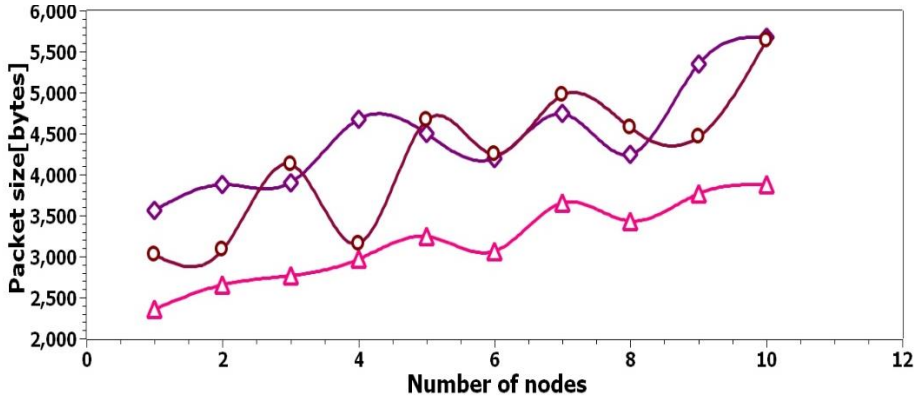
Figure 6. Scalability rate comparison

5.3. Packet overhead analysis

The Packet overhead's analysis comparison is accomplished for Wi-Fi module with SRPP, Wi-Fi module with ECC, and Wi-Fi module with AP approaches are illustrated in figure 7 (a) and (b). In Figure 7 (a), the packet overhead is analyzed by observing the utilization of a number of the packet for each node's tasks during the key generation and key verification ($N_2 = hash(i^c, N_1, SSK)$). The comparison graph shows that the Wi-Fi module with SRP protocol takes fewer packets (13 packets to16 packets) to complete the encrypted key generation and secret key authentication process for all the nodes. In Figure 7 (b), the packet overhead is analyzed by observing the packet size increases for each node's tasks during the key generation ($ssK = hash((u + i^d) - i^z)^{c+uz}$), ($ssK = h(i^c i^{uz})^d$) and key verification. The comparison graph shows that the Wi-Fi module with SRP protocol utilized fewer data packets (2357 bytes to 3876 bytes) to complete the encrypted key generation and secret key authentication process for all the nodes.



(a)



(b)

Figure 7. Packet overhead a) Overall packet count b) Overall data packet size

5.4. Integrity analysis

The Integrity analysis comparison is accomplished for Wi-Fi module with SRPP, Wi-Fi module with ECC, and Wi-Fi module with AP approaches are shown in figure 8. It clearly shows that the Wi-Fi module with the SRPP approach obtains less response time (75 ms to 139 ms) for up to 50 data packets. It proves that the Wi-Fi module with the SRPP approach gives equal priority to perform encrypted key generation and secret key verification for both IoT client node (Sensor device) and Application Server node. The overall simulation analysis graphs in this sections proves that the Secure Remote Password Protocol in Wi-Fi module achieved reliable integrity rate, scalable rate, latency rate and packet overhead than Eclipse curve cryptography (ECC) and tree structure approach based security to perform encrypted secret key generation and authentication for both client (IoT device) and server (IoT application server).

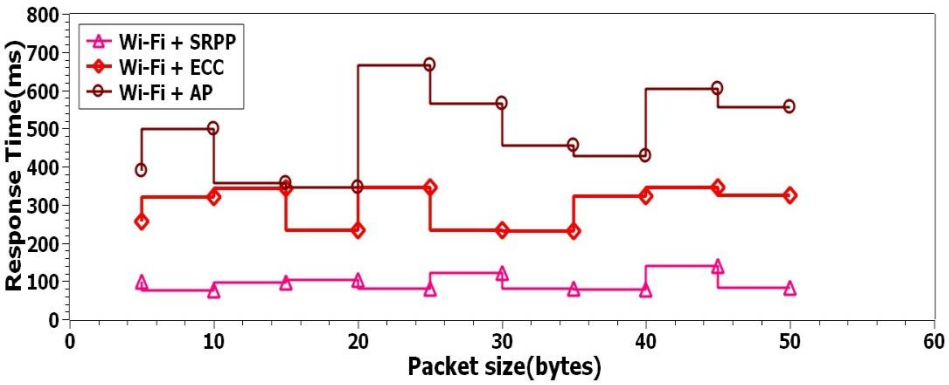


Figure 8. Integrity rate comparison graph

6. Conclusion

The Wi-Fi module's node specification with the security protocol extension process is implemented to evaluate the performance. The simulation results and performance analysis are discussed in the previous section. The latency analysis is observed that the Wi-Fi module with the SRPP approach is to attain a good response time (59 ms to 598 ms). The scalability analysis is observed that the Wi-Fi module with SRPP approach is attain encouraging overall response time (512(ms) to 6175(ms)) to complete 10 node's tasks (encrypted key generation and authentication). The Packet overhead analysis proves that the Wi-Fi module with the SRPP approach takes fewer packets (13 packets to16 packets) and less overall data packet size (2357 bytes to 3876 bytes), the encrypted key generation and secret key authentication process for all the nodes. The integrity analysis report proves that the Wi-Fi module with the SRPP approach takes less response time (75 ms to 139 ms) to perform encrypted key generation and key verification for IoT client node (Sensor device) and application server node. Therefore, the overall simulation results analysis report is proven that the SRPP based Wi-Fi module outperforms in terms of integrity, scalable, latency and packet overhead rate than comparison approaches. Thus, the research suggests that the SRPP based Wi-Fi module approach is suitable for extending the Wi-Fi module's security against brute force and dictionary attack in an IoT-based smart home environment. Moreover, the research is extended to establish multiple authentication strategies to strengthen Wi-Fi standards security by combining two authentication strategies.

References

[1] A. Khanna and S. Kaur, "Internet of Things (IoT), applications and challenges: A comprehensive review," *Wireless Personal Communications*, vol. 114, pp. 1687-1762, 2020.

[2] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato, "A survey on network methodologies for real-time analytics of massive IoT data and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1457-1477, 2017.

[3] Q. I. Sarhan, "Systematic survey on smart home safety and security systems using the arduino platform," *IEEE Access*, vol. 8, pp. 128362-128384, 2020.

[4] H. T. Salim, and N. A. Jasim, "Design and Implementation of Smart City Applications Based on the Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 13, pp. 4-15, 2021.

[5] M. Abbasi, M. H. Yaghmaee, and F. Rahnama, "Internet of Things in agriculture: A survey," in *2019 3rd International Conference on Internet of Things and Applications (IoT)*, 2019, pp. 1-12: IEEE.

[6] O. H. Yahya, H. T. ALRikabi, R. a. M. Al_airaji, and M. Faezipour, "Using Internet of Things Application for Disposing of Solid Waste," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 13, pp. 4-18, 2020.

[7] C. F. Pasluosta, H. Gassner, J. Winkler, J. Klucken, and B. M. Eskofier, "An emerging era in the management of Parkinson's disease: wearable technologies and the internet of things," *IEEE journal of biomedical and health informatics*, vol. 19, no. 6, pp. 1873-1881, 2015.

[8] A. D. Pathaka and J. V. Tembhurne, "Internet of Things: a survey on IoT protocols," in *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, 2018, pp. 26-27.

[9] H. Alrikabi, and H. Tauma, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, pp. 144-157, 2021.

[10] M. N. Rizal, "Data transmission in machine to machine communication protocols for internet of things application: a review," in *2019 International Conference on Information and Communications Technology (ICOIACT)*, 2019, pp. 899-904: IEEE.

[11] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1-29, 2019.

[12] O. H. Yahya, H. Alrikabi, and I. Aljazaery, "Reducing the Data Rate in Internet of Things Applications by Using Wireless Sensor Network," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 16, no. 03, pp. 107-116, 2020.

[13] I. U. Din, M. Guizani, S. Hassan, B.-S. Kim, M. K. Khan, M. Atiquzzaman, and S. H. Ahmed, "The Internet of Things: A review of enabled technologies and future challenges," *Ieee Access,* vol. 7, pp. 7606-7640, 2018.
[14] M. Tao, X. Hong, C. Qu, J. Zhang, and W. Wei, "Fast access for ZigBee-enabled IoT devices using raspberry Pi," in *2018 Chinese Control And Decision Conference (CCDC)*, 2018, pp. 4281-4285: IEEE.
[15] A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal, and S. W. Kim, "Multimedia Internet of Things: A comprehensive survey," *IEEE Access*, vol. 8, pp. 8202-8250, 2020.
[16] G. Nebbione and M. C. Calzarossa, "Security of IoT application layer protocols: Challenges and findings," *Future Internet*, vol. 12, no. 3, p. 55, 2020.
[17] K. Pahlavan and P. Krishnamurthy, "Evolution and impact of wi-fi technology and applications: a historical perspective," *International Journal of Wireless Information Networks*, vol. 28, no. 1, pp. 3-19, 2021.
[18] A. Jurcut, T. Niculcea, P. Ranaweera, and N.-A. Le-Khac, "Security considerations for Internet of Things: A survey," *SN Computer Science*, vol. 1, pp. 1-19, 2020.
[19] R. Gauniyal and S. Jain, "IoT Security in Wireless Devices," in *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2019, pp. 98-102: IEEE.
[20] F. Xia, H. Song, and C. Xu, "Securing the wireless environment of IoT," in *2018 IEEE International Conference of Safety Produce Informatization (IICSPI)*, 2018, pp. 315-318: IEEE.
[21] H. M. Almohri, L. T. Watson, and D. Evans, "An attack-resilient architecture for the Internet of Things," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3940-3954, 2020.
[22] A. Samandari, M. Ge, J. B. Hong, and D. S. Kim, "Evaluating the security of IoT networks with mobile devices," in *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, 2018, pp. 171-180: IEEE.
[23] K. Lounis and M. Zulkernine, "Attacks and defenses in short-range wireless technologies for IoT," *IEEE Access*, vol. 8, pp. 88892-88932, 2020.
[24] J. Luo and Q. Ji, "Password Acquisition and Traffic Decryption Based on L2TP/IPSec," in *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, 2020, pp. 1567-1571: IEEE.
[25] A. Kondoro, I. B. Dhaou, H. Tenhunen, and N. Mvungi, "Real time performance analysis of secure IoT protocols for microgrid communication," *Future Generation Computer Systems*, vol. 116, pp. 1-12, 2021.
[26] F. Farha, H. Ning, W. Zhang, and K.-K. R. Choo, "Timestamp scheme to mitigate replay attacks in secure zigbee networks," *IEEE Transactions on Mobile Computing*, 2020.
[27] L. Oliveira, J. Rodrigues, S. Kozlov, and R. Rabêlo, "Albuquerque VHCd MAC Layer Protocols for Internet of Things: A Survey," *Future Internet*, vol. 11, p. 16, 2019.
[28] O. A. Savchenko, "Security Model of IoT-based Systems," 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics," *Telecommunications and Computer Engineering (TCSET) Lviv-Slavske, Ukraine*, pp. 398-401, 2020.
[29] C. Boyd, A. Mathuria, and D. Stebila, *Protocols for authentication and key establishment*. Springer, 2003.
[30] M. Hagan, F. Siddiqui, S. Sezer, B. Kang, and K. McLaughlin, "Enforcing policy-based security models for embedded SoCs within the internet of things," in *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, 2018, pp. 1-8: IEEE.
[31] J. Bugeja, B. Vogel, A. Jacobsson, and R. Varshney, "IoTSM: an end-to-end security model for IoT ecosystems," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2019, pp. 267-272: IEEE.
[32] O. Faraj, D. Megías, A.-M. Ahmad, and J. Garcia-Alfaro, "Taxonomy and challenges in machine learning-based approaches to detect attacks in the internet of things," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1-10.
[33] A. T. al., "Formal Methods Analysis of the Secure Remote Password Protocol," 2003.
[34] W. Stone, D. Kim, V. Y. Kemmoe, M. Kang, and J. Son, "Rethinking the Weakness of Stream Ciphers and Its Application to Encrypted Malware Detection," *IEEE Access*, vol. 8, p. 191602, 2020.
[35] W. Zhijun, L. Wenjing, L. Liang, and Y. Meng, "Low-rate DoS attacks, detection, defense, and challenges: a survey," *IEEE Access*, vol. 8, pp. 43920-43943, 2020.
[36] I. C. Eian, K. Y. Lim, M. X. L. Yeap, H. Q. Yeo, and Z. Fatima, "Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges," 2020.

[37] Y. Borse, D. Patole, and P. Ahirao, "Geo-Encryption: A location based encryption technique for data security," in *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, 2019, pp. 1-4: IEEE.