MAC-Based Physical Layer Security over Wireless Sensor Network

Subjects: Computer Science, Information Systems

Contributor: Attique Ur Rehman, Sajid Mahmood, Shoaib Zafar, Muhammad Ahsan Raza, Fahad Qaswar, Sumayh S. Aljameel, Irfan Ullah Khan, Nida Aslam

Physical layer security for wireless sensor networks (WSNs) is a laborious and highly critical issue in the world. Wireless sensor networks have great importance in civil and military fields or applications. Security of data/information through wireless medium remains a challenge. The data that transmit wirelessly has increased the speed of transmission rate. In physical layer security, the data transfer between source and destination is not confidential, and thus the user has privacy issues, which is why improving the security of wireless sensor networks is a prime concern. The loss of physical security causes a great threat to a network.

Keywords: MAC ; physical layer ; wireless sensor network ; attack

1. Introduction

Science and technology have worked together to make daily lives much easier and more comfortable than ever [1]. Due to its various inventions and discoveries, human life has become much more comfortable and modernized. Nowadays, people are always connected to the mobile phones and computers twenty-four hours a day, and the data is maintained or saved either in the devices or in the cloud storage [2]. Therefore, in order to save the data from unauthorized access and from hackers, researchers use the different security approaches to make a network secure [3]. This covers the basic concept of secure networks in wireless medium along with its advantages, disadvantages and applications [4].

Wireless sensor network security is the process of making the devices such as smart phones [5], tablets, computers and all the other handheld portable devices secure along with the network to which they are connected [6]. It helps people to prevent other users who are unauthorized from accessing the devices and data so that the data cannot be manipulated [7]. Since people are more focused on the wireless medium, the most common threat which needs to be addressed is therefore to make the devices secure while using the internet, and for that, human use Wi-Fi networks [8]. Therefore, in Wi-Fi networks people use Wi-Fi security that contains Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) [9].

Wired Equivalent Privacy (WEP) was developed for the security of networks which were running on wireless medium in September 1999 [10]. As the name applies, it was designed in such a way that it could provide the same level of security as the wired mediums, but it was very hard to configure and had many security flaws [11]. WEP also managed to be broken, which exposed the personal data and devices easily to the hackers all over the internet [12]. Due to its drawbacks, many devices were updated with different security protocols which were configured on WEP, and it was officially abandoned by the Wi-Fi alliances in 2004 [13].

WEP is a security algorithm for IEEE 802.11 wireless networks, and it mainly consists of 10 or 26 hexadecimal digits which makes 40 or 104 bits, respectively [14]. In 2004, WEP-40 and WEP-104 (128 and 256 bits) were declared “dead” because of the frequent attacks and flaws [15]. Basically, WEP used to run based on two algorithms [9].

The first algorithm was RC4-Key Scheduled Algorithm (KSA) which converts the key of length ranging from 1 to 256 bits to numbers 0 to N. It works as it contains the two numbers “i” and “j” which are used as pointers to the element of S [8][16].

The second algorithm is RC4-Pseudo Random Generation Algorithm (PGRA). This algorithm works by generating a byte of random or pseudorandom characters from internal state and then updates the internal state [17][18].

As mentioned earlier, WEP was exposed to many attacks which made it a vulnerable protocol when it comes to security, and some of them include packet injection, fake authentication, FMS attack, Chop attack, and Kore K attack [19].

Wireless sensor networks (WSNs) are now a hot topic for research. After being deployed in dangerous, hostile, or isolated places, the sensors are typically left unattended. These nodes are constrained by their finite and nonrenewable energy supplies. One of the primary design goals for these sensing devices is energy efficiency [20]. Researchers outline the difficulties in developing a medium access control protocol, which is a protocol for wireless sensor networks. People discuss several protocols for the WSNs, highlighting their advantages and disadvantages whenever feasible [21]. Some cluster-based networks are also used in a WSN especially, the main tendency in this scenario being either distributed decision making via sharing information with nearby nodes till the cluster and its members are picked, or centralized decision making at the base station for the selection of the cluster and its members [22]. Due to excessive broadcasting, particularly in large networks, as well as ensuring a higher until a final decision is made, both strategies dramatically increase energy usage [23]. The cutting-edge layer-based hybrid approach for selecting cluster heads and cluster members results in a cutting-edge WSN communication architecture [24].

2. Attacks on Wireless Security

Sinkhole attacks are the most dangerous attacks in wireless sensor networks in which fake nodes distribute fake routing updates such as the shortest path to a sink node to disturb the network traffic. A comprehensive research is conducted by [25] to show the up-to-date sinkhole attacks along with their mitigation approaches. Furthermore, they also discussed the state-of-the-art challenges in the detection and prevention of sinkhole attacks in wireless sensor networks.

In wireless sensor networks, the node structure is restricted by memory, computation and energy limitations. The lifetime of a node having limited energy resources directly affects the overall performance of a wireless sensor network. Cluster head selection and data transmission strategy play a key role in the performance enhancement of WSNs. A new energy-aware as well as adaptive routing scheme was developed by [26], which is based on the fuzzy TOPSIS method and performs well in terms of energy efficiency, network life, less overhead on cluster head selection and data transmission.

2.1. Packet Injection-Based Attacks

The packet injection attack is based on the concept of ARP request. In packet injection, the hacker or unauthorized user captures the packet of a targeted network of any type. That allows the user to produce and send a large amount of traffic to the network [27]. Although the packet over a network is always secured by encryption, the packet type can be figured out easily by the packet size [28]. The size of ARP packet is 28 bytes. By reinjecting a packet into a network, it sends packets to all the clients. Encrypted packets are captured by sending additional packets, and by sending out more packets, the hacker will probably be able to break out of WEP faster [29].

2.2. Fake Authentication-Based Attacks

Fake authentication is a method through which an attacker can break into the WEP-protected network even without having access of the root key [30]. This can be achieved in two ways:

- Open system authentication: in this type of authentication, the user can access the system without any kind of user verification by the network [31]. It is also referred to as null verification because no kind of authentication takes place between the devices, and it is an exchange of frames (hellos) between the client and the AP.

- Shared key authentication; this is the same as open system authentication but it includes a challenge (requires WEP keys to be matched) and response between AP and the user [32][33]. In this method, the key is delivered to wireless clients with the help of a secured and protected channel which is independent of any standard and protocols being used. The client or user just has to simply log in by submitting their credentials and can access the network [34].

2.3. Fluhrrer, Mantin and Shamir Attacks

The FMS attack, released in 2001 by Fluhrrer, Mantin and Shamir, is based on the weakness of RC4. This can be performed as the attacker tries to manipulate RC4, which allows him to guess the byte of the key. If the key is invalid, the attacker tries again, and in order to reach fifty percent probability, the attacker has to capture a large number of packets, which can reach approximately six million [35]. The key can be figured out as the bites are somehow related to each other; therefore, if the attacker manages to figure out the first bit of the key, they will manage to have a hint regarding the other bit, and that will eventually help him to get on the right track [36].

2.4. Wi-Fi Protected Access (WPA) Attacks

Wi-Fi Protected Access (WPA) was introduced as the updated version of WEP and became available in 2003. The main motive of WPA was to overcome and eliminate the vulnerabilities which failed to be handled by WEP protocol. From then onwards, it has been recognized as the standard of security for devices over a wireless network [37]. The most common WPA configuration is WPA-PSK, and the size of the key used in WPA is 256 bits. WPA includes an integrity check, which means that it validates and checks that no packet has been altered and/or captured by an unauthorized user between the end user and the access point [38].

Moreover, WPA contains the Temporary Key Integrity Protocol (TKIP), which is more secure and effective as compared to the fixed key system which is used in WEP. However, still there have been some attacks which managed to bypass the security of this protocol [39]. Some of the attacks include Back and Tew's Improved Attack, Ohigashi-Morii Attack, Michael Attacks, etc. [40]. There are three categories of WPA attacks.

2.4.1. Back and Tew's Improved Attack

This attack is based on the poisoning of ARP. The attacker tries to exploit the weakness by decrypting the ARP and sending the flow of packets to the network, which leads to ARP poisoning [41]. Furthermore, this attack requires quality of service and allows consumption of several channels. Every channel has its own TKIP sequence counter, respectively, but channel 0 has the ability to hold down the most traffic [42].

2.4.2. Ohigashi-Morii Attack

This attack was introduced in 2009, and it was an improved version of Back and Tew's improved attack [43][44]. It was more efficient for all modes of Wi-Fi Protected Access (WPA).

2.4.3. Michael Attack

In 2010, Beck was able to discover that the internal state tends to reset if it reaches a certain point, causing the whole algorithm to start all over again. Due to this, an attacker might be able to insert some text in a packet, meaning that even though the content of the package was different, the result of the algorithm was still accurate [45]. However, the requirements of this attack were very high compared with Back and Tew's improved attack [46].

2.5. Wi-Fi Protected Access 2 (WPA2) Attacks

WPA2 replaced Wi-Fi Protected Access due to the advancements and security concerns for new technology and devices. The certification started in 2004, and by the end of March 2006, it was mandatory for every device to be compatible with and have the features of WPA2 [29]. The most important upgrade in this protocol was about the replacement of TKIP with the AES algorithm and the introduction of CCMP (AES CCMP, Counter Cipher Mode with Block Chain Message Authentication Code Protocol). However, one of the most common and frequent attacks which was found in this protocol was Hole196 [47].

2.5.1. KRACK Attack

The KRACK attack was discovered in 2016 by Mathy Vanhoef and Frank Piessens. This attack targets the four-way handshake procedure in WPA2 protocol, and it is one of the most severe replay attacks [48]. In this protocol, during disconnection from a Wi-Fi network, it is possible for the user to reconnect to the network by using the same key for a quick handshake, so that the connection can be quickly reconnected and can be continued [13]. Therefore, since it allows the user to reconnect without generating a new key, it is highly possible that a hacker or the defaulter can deploy a replay attack [49].

2.5.2. PMKID Attack

This attack was discovered on 4th August of 2014, and it is particularly dangerous for those protocols which consist of WPA/WPA-PSK (pre-shared Key). This attack allows the attacker to obtain the PSK key [50]. Moreover, this attack was discovered accidently while the protocol was being tested and new ways of failing this secure connection were being discovered. The thing which makes this attack unique and different from others is that the unauthorized person does not have to access the whole four-way hand shaking procedure [51][52]. However, it is performed with the help of an RSN IE (Robust Security Network Information System). Some of the benefits of this attack include:

- The attacker might be able to have direct communication with the access point, and therefore, it is a client-less attack as it does not need to have a regular user for its deployment [48].

- This attack is less time consuming because of the fact that the unauthorized person does not have to wait for the four-way handshaking process [53].
- They are faster because it does not require replaying of counter values.
- One of the key benefits is that the final data or result will not be shown in different format, but it will appear to be in regular hexadecimal format [32].
- There is no loss of EAPOL frames, since the AP and client are too far away from the attacker.

3. TCP/IP Model Layers Attacks

3.1. Physical Layer Attacks

The physical layer is the last layer which is present on the OSI model and it is responsible for the transmission of bits to the medium [54]. The two main types of attacks which are commonly found in the physical layer are the eavesdropping and jamming attacks. The concept of the eavesdropping attack is the interference of the unauthorized user by intercepting the communication of the clients or authorized user. As long as the coverage or communication lies in the range of the eavesdropper, the hacker can hack into it. Therefore, in order to make it secure, secret keys are used which use the concept of cryptography. In particular, SN and DN shares a secret key, and the text is encrypted with the help of cipher text. The main advantage of this is that even if the eavesdropper manages to access the data or text, it will still not manage to understand it since it will be encrypted and will only be accessible with the help of that specific special key [55].

The jamming attack is also known as the DoS attack, and in this kind of attack, the hacker tries to access the data with the help of a malicious node. The jammer helps and prevents the device from connecting to and accessing the authorized node, and instead of that, it allows the device to connect to a malicious node which is being controlled by the unauthorized user [48].

Zero Day DdoS attacks are emerging types of attacks and are increasing in IoT-based systems which are empowered by WSNs. A machine learning-empowered honeypot-based sustainable framework is proposed by [56] for preventing Zero Day DdoS attacks.

3.2. MAC Layer Attacks

In recent years, a number of authentication methods have been published, although the majority of earlier plans do not offer enough privacy for these wireless connections. It is suggest the Cogent fingerprint authentication scheme as an effective and lightweight authentication method to overcome the drawbacks of earlier methods (COBBAS). The suggested system employs lightweight procedures to improve the network's efficiency in terms of the time, capacity, and battery usage. It is dependent on biometric data. Burrows-Abadi-Needham logic is used in a formal security research of COBBAS to ensure that the system protocol offers safe mutual authentication [57].

Each network node is equipped with an NIC card which contains the MAC address of the device, which is unique worldwide [20]. This MAC address helps the user to be identified all over. MAC spoofing is performed by the hackers, allowing them to change the assigned MAC address of their devices over the Internet, and this is one of the primary attacks which target the MAC layer [58]. Although the MAC address is imprinted and hard coded, still they manage to hide their true identity and manage to have an alternative MAC address. Moreover, an unauthorized user may also be able to hear the ongoing communication between the two devices and might be able to steal and use the MAC address of another device; this kind of crime lies under identity-theft attack [35].

Moreover, MITM attacks and network injections are also quite common on this layer. In a MITM attack, the defaulter tries to break into the network with the help of sniffing, and then he tries to learn one of the MAC addresses of the communicating devices. Then, that person impersonates himself as one of the users and establishes the connection which helps them to access the data. It helps the hacker to control the whole communication environment, whereas for the users, it seems like a normal conversation as their communication is not interrupted [59]. On the other hand, the network injection consists of injecting commands in the switches and routers, which allows the devices to be re-configured. Therefore, it allows the network to be paralyzed, or it may even require the whole system to be rebooted as the configuration gets disturbed upon updating commands.

3.3. Network Layer Attacks

The network layer is responsible for delivering the packets from source to destination and vice versa with the help of the IP address. The network layers basically target the weakness of the IP address, which leads to IP spoofing, IP hijacking and Smurf attacks [60].

In IP spoofing, the user creates an IP packet which has a changed address that helps either to hide the true IP address of the hacker or to represent itself as another device [35][59]. It is a common technique which is used to initiate DoS attack against a device or a network.

The Smurf attack is also a DoS attack in which the unauthorized user sends a huge number of ICMP packets to the network. Upon request, the victim needs to respond to all the requests and it replies back, which leads to excess traffic at the victim's end. Due to the congestion produced by the large number of requests, it paralyzes the network of the victim. A possible solution to a Smurf attack is to make sure that researchers configure all the devices such as routers and switches individually, in a way that they do not respond to ICMA requests. Moreover, people can also use a firewall that will help to block the malicious packets [58].

3.4. Transport Layer Attacks

In a transport layer attack, the attackers mainly attack the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). In short, TCP is a connection oriented protocol which is used for communication between server and client. Furthermore, it allows the maintenance of a virtual pipeline which provides a secure connection between the users and is mainly used in chat applications. Furthermore, UDP is a connectionless protocol in which the data travels in stream and it is mainly used in live streams where loss of data does not matter [60]. Both of these protocols are exposed when it comes to access by an unauthorized user with the help of flooding, and hackers can also get into the network by predicting the sequence number in the TCP protocol. The UDP protocol is also exposed to flooding attacks as the attacker generates a large number of UDP packets [61]. Due to the large number of packets being generated at the victim's end, the victim will have to respond and reply to every malicious UDP packet, and it will become unreachable for other nodes.

3.5. Application Layer Attacks

In the OSI model, the application layer is responsible for providing end services to the users, which contain file transfers protocols, email configuration and services regarding the web pages. The main HTTP (web-based) attacks are Trojan horses, worms, ruses, cross-site scripting attacks and structure query language injection attacks. The SQL injections contain data-driven applications that contain SQL commands which allows the unauthorized person to access the sensitive data [62]. Moreover, in cross-site scripting attacks, client-side scripts are injected into web pages via an access control measure [63].

Active Attacks

Active attacks are those in which the hacker tries to gain access to communication information or to the network by interfering or interrupting and also changes the data as per the hacker's desire. The unauthorized person might update or alter the data and modify the data stream [34]. The most common types of these attacks are Wormhole attacks and Black hole attacks, which frequently and mostly target where wireless sensor networks are being used [38][43]. The concept of a Black hole attack is that one node of a network acts as a black hole, attracting all the network traffic to itself. The diagram below shows the view of a Black hole attack when it is found in a network.

In wireless sensor networks, the nodes send a special message that is known as a "hello" message. These messages are used in order to discover the nodes in a network and also to insert a new node into a network. While attacking this kind of network, the attacker tries to produce congestion in the network by overloading the network, which allows the attacker to consume all the energy of the nodes which are there in the network [48][49].

References

1. Dwiputriane, D.B.; Heng, S.H. No. 3. Authentication for 5G Mobile Wireless Networks. J. Eng. Technol. Appl. Phys. 2022, 4, 16–24.
2. Masher, N.; ul Mahjoob, K. IOT SECURITY THREATS AND CHALLENGES. Available online: https://www.irjmets.com/uploadedfiles/paper/issue_2_february_2022/19081/final/fin_irjmets1644942131.pdf (accessed on 24 June 2022).

3. Waqas, M.; Tu, S.; Halim, Z.; Rehman, S.; Abbas, G.; Abbas, Z.H. The Role of Artificial Intelligence and Machine Learning in Wireless Networks Security: Principle, Practice and Challenges; Springer: Berlin/Heidelberg, Germany, 2022.
4. Li, J.; Ma, H.; Li, K.; Cui, L.; Sun, L.; Zhao, Z.; Wang, X. Wireless Sensor Networks. In Proceedings of the 12th China Conference, CWSN 2018, Kunming, China, 21–23 September 2018.
5. Yadav, R.; Varma, S.; Malaviya, N. A survey of MAC protocols for wireless sensor networks. UbiCC J. 2009, 4, 827–833.
6. Ismail, A.S.; Wang, X.F.; Hawbani, A.; Alsamhi, S.; Abdel Aziz, S. Routing protocols classification for underwater wireless sensor networks based on localization and mobility. Wirel. Netw. 2022, 28, 797–826.
7. Raja Basha, A. A Review on Wireless Sensor Networks: Routing. Wirel. Pers. Commun. 2022, 1–41.
8. Moessner, K.; Majid, M.; Habib, S.; Rehman Javed, A.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.-W. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors 2022, 22, 2087.
9. Temene, N.; Sergiou, C.; Georgiou, C.; Vassiliou, V.; Sergiou, C. A survey on mobility in Wireless Sensor Networks. Ad Hoc Netw. 2022, 125, 102726.
10. Zhu, L.; Xiang, H.; Zhang, K. A Light and Anonymous Three-Factor Authentication Protocol for Wireless Sensor Networks. Symmetry 2022, 14, 46.
11. Cao, L.; Wang, Z.; Yue, Y. Analysis and Prospect of the Application of Wireless Sensor Networks in Ubiquitous Power Internet of Things. Comput. Intell. Neurosci. 2022, 2022, 9004942.
12. El Khediri, S. Wireless sensor networks: A survey, categorization, main issues, and future orientations for clustering protocols. Wirel. Pers. Commun. 2022, 104, 1775–1837.
13. Mezrag, F.; Bitam, S.; Mellouk, A. An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks. J. Netw. Comput. Appl. 2022, 200.
14. Choi, J.; Ha, J.; Personal, H.J. Physical Layer Security for Wireless Sensor Networks. Available online: https://ieeexplore.ieee.org/document/6666094?arnumber=6666094 (accessed on 25 June 2022).
15. Engineering, F.A. Energy-efficient collision avoidance MAC protocols for underwater sensor networks: Survey and challenges. J. Mar. Sci. Eng. 2021, 9, 741.
16. Gulati, K.; Sarath Kumar Boddu, R.; Kumar Boddu, S.; Kapila, D.; Bangare, S.L.; Chandnani, N.; Saravanan, G. A review paper on wireless sensor network techniques in Internet of Things (IoT). Mater. Today 2022, 51, 161–165.
17. Rajasoundaran, S.; Prabu, A.V.; Kumar, G.S.; Malla, P.P.; Routray, S. Secure Opportunistic Watchdog Production in Wireless Sensor Networks: A Review. Wirel. Pers. Commun. 2021, 120, 1895–1919.
18. Daanoune, I.; Abdennaceur, B.; Ballouk, A. A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks. Ad. Hoc. Netw. 2021, 114, 102409.
19. Chander, B.; Gopalakrishnan, K. Secure, Efficient, Lightweight Authentication in Wireless Sensor Networks. Lect. Notes Electr. Eng. 2021, 749, 303–312.
20. Shiu, Y.; Chang, S.; Wu, H.C.; Huang, S.C.H.; Chen, H.H. Physical layer security in wireless networks: A tutorial. IEEE Wirel. Commun. 2011, 18, 66–74.
21. Ahmad, A.; Rathore, M.; Paul, A.; Chen, B.W. Data transmission scheme using mobile sink in static wireless sensor network. J. Sens. 2015, 2015, 279304.
22. Jabbar, S.; Paul, A.; Rho, S.; Minhas, A.A. Multilayer cluster designing algorithm for lifetime improvement of wireless sensor networks. J. Supercomput. 2014, 70, 104–132.
23. Pinto, A.; Farooq, M.S.; Idrees, M.; Rehman, A.U.; Khan, M.Z.; Abunadi, I.; Assam, M.; Althobaiti, M.M.; Al-Wesabi, F.N. Formal Modeling and Improvement in the Random Path Routing Network Scheme Using Colored Petri Nets. Appl. Sci. 2022, 12, 1426.
24. Din, S.; Paul, A.; Ahmad, A.; Kim, J.H. Energy efficient topology management scheme based on clustering technique for software defined wireless sensor network. Peer-Peer Netw. Appl. 2019, 12, 348–356.
25. Hussain, A.; Ali, M.; Razzaq, A.; Ijaz, A.; Saeed Khan, N. Development of an Adaptive Energy Aware Routing Scheme for Wireless Sensor Networks. Int. J.Emerg. Technol. 2020, 11, 381–388.
26. Shang, W.; Yu, Y.; Droms, R.; Zhang, L. Challenges in IoT Networking via TCP/IP Architecture. NDN Project. 2016. Available online: https://named-data.net/publications/techreports/ndn-0038-1-challenges-iot/ (accessed on 24 June 2022).

27. Chan, M.C.; Ramjee, R. Improving TCP/IP performance over third-generation wireless networks. IEEE Trans. Mob. Comput. 2008, 7, 430–443.

28. Poongodi, T.; Krishnamurthi, R.; Indrakumari, R.; Suresh, P.; Balusamy, B. Wearable devices and IoT. Intell. Syst. Ref. Libr. 2020, 165, 245–273.

29. Dunkels, A.; Alonso, J.; Voigt, T.; Ritter, H.; Schiller, J. Connecting wireless sensornets with TCP/IP networks. In International Conference on Wired/Wireless Internet Communications; Springer: Berlin, Heidelberg, 2004.

30. Faria, D.B.; Cheriton, D.R. Detecting identity-based attacks in wireless networks using signalprints. In WiSE 2006—Proceedings 5th ACM Work Wireless Security; ACM: New York, NY, USA, 2006; Volume 2006, pp. 43–52.

31. Masud, M.; Gaba, G.S.; Choudhary, K.; Hossain, M.S.; Alhamid, M.F.; Muhammad, G. Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare. IEEE Internet Things J. 2022, 9, 2649–2656.

32. Mahamune, A.A.; Chandane, M.M. TCP/IP Layerwise Taxonomy of Attacks and Defence Mechanisms in Mobile Ad Hoc Networks. J. Inst. Eng. Ser. B 2022, 103, 273–291.

33. Messai, M.-L. Classification of Attacks in Wireless Sensor Networks. arXiv 2014, arXiv:1406.4516.

34. Hu, Y.; Perrig, A.; Johnson, D.B. Wormhole attacks in wireless networks. IEEE J. Sel. Areas Commun. 2006, 24, 370–380.

35. Lupu, T.G. Main types of attacks in wireless sensor networks. In Proceedings of the 9th WSEAS International Conference on Signal, Speech and Image Processing, and 9th WSEAS International Conference on Multimedia, Internet & Video Technologies, Budapest, Hungary, 3–5 September 2009.

36. Yu, B.; Xiao, B. Detecting selective forwarding attacks in wireless sensor networks. In Proceedings of the 20th IEEE International Parallel & Distributed Processing Symposium, Rhodes Island, 25–29 April 2006.

37. Noman Riaz, M.; Buriro, A.; Mahboob, A. Classification of Attacks on Wireless Sensor Networks: A Survey. Int. J. Wirel. Microw. Technol. 2018, 8, 15–39.

38. Yang, J.; Chen, Y.; Trappe, W.; Cheng, J. Detecting mobile agents using identity fraud. SpringerBriefs Comput. Sci. 2014, 0, 43–66.

39. Shahzad, F.; Pasha, M.; Ahmad, A. A survey of active attacks on wireless sensor networks and their countermeasures. Int. J. Comput. Sci. Inf. Secur. 2017, 14, 12.

40. Patel, M.; Aggarwal, A. Security attacks in wireless sensor networks: A survey. In Proceedings of the 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), Vallabh Vidyanagar, India, 1–2 March 2013.

41. Anwar, R.; Bakhtiari, M.; Zainal, A.; Abdullah, A.H.; Qureshi, K.N. Security issues and attacks in wireless sensor network. World Appl. Sci. J. 2014, 30, 1224–1227.

42. Yang, T.; Zhai, F.; Xu, H.Q.; Li, W. Design of a secure and efficient authentication protocol for real-time accesses of multiple users in PIoT-oriented multi-gateway WSNs. Energy Rep. 2022, 8, 1200–1211.

43. Sinha, P.; Jha, V.K.; Bhushan, B.; Rai, A.K.; Jha, V.K. A Review of Machine Learning Solutions to Denial-of-Services Attacks in Wireless Sensor Networks. In Proceedings of the 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, 28–29 July 2017.

44. Bouabdellah, M.; Kaabouch, N.; El Bouanani, F.; Ben-Azza, H. Network layer attacks and countermeasures in cognitive radio networks: A survey. J. Inf. Secur. Appl. 2018, 38, 40–49.

45. Farid, S.; Rehman, A.U. Enhancement in Quality of Services Using Integrated Services in 4G Cellular Network. Tech. J. 2018, 23, 82–93.

46. Proano, A.; Lazos, L. Selective jamming attacks in wireless networks. In Proceedings of the 2010 IEEE International Conference on Communications, Cape Town, South Africa, 23–27 May 2010.

47. Singh, R.; Prasad, A.; Moven, R.M.; Deva Sarma, H.K. Denial of service attack in wireless data network: A survey. In Proceedings of the 2017 Devices for Integrated Circuit (DevIC), Kalyani, India, 23–24 March 2017; pp. 354–359.

48. Edigar, M.B.; Rao, P.V. Modeling of lightweight security framework for identifying efficient route for secure communication in WSN. Int. J. Intell. Unmanned Syst. 2022, 10, 129–144.

49. Isha, A.M.; Raj, G. Dos attacks on tcp/ip layers in wsn. Int. J. Comput. Netw. Commun. Secur. 2013, 1, 40–45.

50. Zhang, L.; Restuccia, F.; Melodia, T.; Pudlewski, S.M. Taming cross-layer attacks in wireless networks: A Bayesian learning approach. IEEE Trans. Mob. Comput. 2018, 18, 1688–1702.

51. Kwon, E.; Cho, Y.; Chae, K.J. Integrated Transport Layer Security: End-To-End Security Model between WTLS and TLS. Available online: https://ieeexplore.ieee.org/document/905331 (accessed on 24 June 2022).

52. Wang, L.; Wyglinski, A.M. A combined approach for distinguishing different types of jamming attacks against wireless networks. In Proceedings of the 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, Victoria, BC, Canada, 23–26 August 2011.
53. Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of service attacks in wireless networks: The case of jammers. IEEE Commun. Surv. Tutor. 2010, 13, 245–257.
54. Ali, M.; Siddique, A.; Hussain, A.; Hassan, F.; Ijaz, A.; Mehmood, A. A Sustainable Framework for Preventing IoT Systems from Zero Day DDoS Attacks by Machine Learning. Int. J. Emerg. Technol. 2021, 12, 116–121.
55. Eriksson, J.; Krishnamurthy, S.V.; Faloutsos, M. Truelink: A practical countermeasure to the wormhole attack in wireless networks. In Proceedings of the 2006 IEEE International Conference on Network Protocols, Santa Barbara, CA, USA, 12–15 November 2006.
56. Zhang, Z.; Wu, J.; Deng, J.; Qiu, M. Jamming ACK attack to wireless networks and a mitigation approach. In Proceedings of the IEEE GLOBECOM 2008–2008 IEEE Global Telecommunications Conference, New Orleans, LA, USA, 30 November 2008–4 December 2008.
57. Butt, T.M.; Riaz, R.; Chakraborty, C.; Rizvi, S.S.; Paul, A. Cogent and energy efficient authentication protocol for wsn in iot. Comput. Mater. Contin. 2021, 68, 1877–1898.
58. Kanawat, S.; Parihar, P. Attacks in wireless networks. Int. J. Smart Sens. Adhoc Netw. 2011, 1, 17.
59. Kadhim, A.N.; Sadkhan, S.B. Security Threats in Wireless Network Communication-Status, Challenges, and Future Trends. In Proceedings of the 2021 International Conference on Advanced Computer Applications (ACA), Maysan, Iraq, 25–26 July 2021.
60. Sardar, R.; Anees, T. Web of things: Security challenges and mechanisms. IEEE Access 2021, 9, 31695–31711.
61. Taleb, H.; Nasser, A.; Andrieux, G.; Charara, N.; Motta Cruz, E. Wireless technologies, medical applications and future challenges in WBAN: A survey. Wirel. Netw. 2021, 27, 5271–5295.
62. Zaman, S.; Alhazmi, K.; Aseeri, M.A.; Ahmed, M.R.; Khan, R.T.; Kaiser, M.S.; Mahmud, M. Security threats and artificial intelligence based countermeasures for internet of things networks: A comprehensive survey. IEEE Access 2021, 9, 94668–94690.
63. Raza, M.; Bukht, T.; Ali, M.; Rehman, A.U.; Idrees, M. Analyzing the Behaviour of DDOS Cyber Attacks. Tech. J. 2021, 26, 46.
