Wireless Sensor Network

Subjects: Robotics

Contributor: Rami Ahmad, Raniyah Wazirali, Tarik Abu-Ain

Wireless Sensor Network (WSN) is one of the most effective methods for many real-time applications, due to its compactness, cost-effectiveness, and ease of deployment. The function of the WSN is to monitor the field of interest, collect the data, and transmit it to the base station (Access point) for post-processing analysis.

Keywords: wireless sensor networks ; ZigBee ; 6LoWPAN

1. Wireless Sensor Network (WSN) Overview

The primary advantage of the IoT is global awareness, intelligent processing, and the reliable transfer of information. The key is the realization of the information's interactions between a human and a device or device-to-device. These devices consist of embedded systems, control and automation systems, Wireless sensor networks (WSNs), and others that share information in different environments for enabling the IoT [1]. Therefore, the data can be transferred over different networks without the need for human intervention. In the real environment of IoT applications, the smart city and home are the most popular fields. These applications mostly consist of three layers, which comprise; perception, the network, and the application [2]. Network and application layers are implemented in high-power devices that will keep data secure, while the perception layer is implemented in a low-power WSN. The WSN consists of multiple sensor nodes, which are communicating with each other by using different radio frequencies that are capable of performing various tasks of sensing, surveillance, measuring, and tracking [3]. These wireless nodes are resource-constrained devices that are characterized by their low processing power, narrow bandwidth, limited battery life, and restricted memory capacity [4]. The communication between WSN layers is depicted in **Figure 1**.

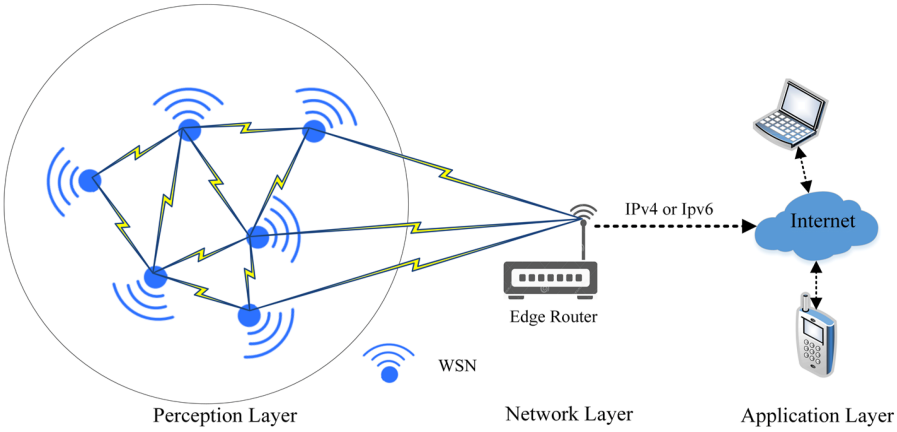

Figure 1. The communication among the WSN layers.

Based on **Figure 1**, wireless sensor networks are responsible for plotting the network topology and updating the routing table in the perception layer using different protocols to maintain the network infrastructure [5]. Then, the WSN starts collecting data from different locations and forwards it to the network layer (edge router). The WSN nodes are the basic building block of this layer and share some characteristics that distinguish them from other wireless networks [6]. Among these characteristics are the following:

- Independent nodes without a central control
- Stationary or mobile WSN nodes
- The transmission range of WSN nodes is also limited
- The WSN network topology is constantly changing

- Multiple hop connections
- Limited bandwidth

The WSN nodes, on the other hand, can generally operate in untrusted environments that are not regularly monitored. It is because of this vulnerability that valuable data can be easily leaked to uninvited parties, posing major security and privacy issues [7].

The ZigBee and 6LoWPAN are two common protocols that support management in WSNs in the perception layer [8]. Moreover, they can adapt to various other network media, such as low-power Wi-Fi [9], Bluetooth [10], and sub-1 GHz radio frequency [5]. In addition, ZigBee and 6LoWPAN were compared in [11], where 6LoWPAN provides IP capabilities for WPAN networks while ZigBee offers multiple nodes that operate at low power and cost. Moreover, ZigBee can be used in home area networks and for smart metering, as well as other devices that can be intelligently monitored from a distance using this technology. ZigBee has a reliable security system and uses strong encryption technology to secure its data. Furthermore, due to channel collision avoidance, its network technology is superior to other systems. 6LoWPAN, on the other hand, is suitable for low-power IP-based systems, such as sensors and controllers. The main features in the infrastructure of these technologies are summarized in **Figure 2**.

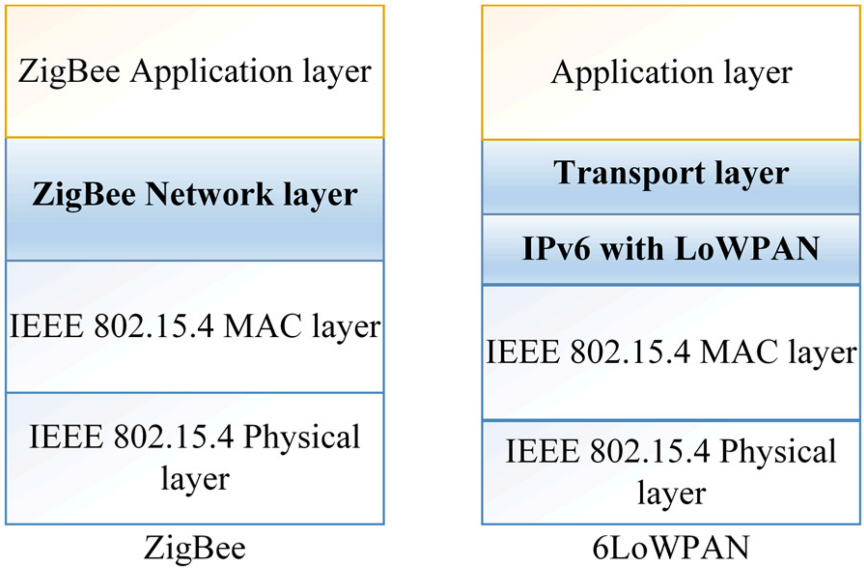

Figure 2. WSN co-management protocols.

However, in both protocols' perception layers, WSN nodes are limited by computing power and energy [12]. Since the WSN is built to work in a variety of locations, it can be difficult to offer a charger in some of those locations. To circumvent this limitation, either the battery's capacity should be raised or the security requirements should be dropped [13]. Nodes can also be charged using renewable energy, such as light, wind, and heat [14]. However, these solutions appear to be out of reach due to the size of the WSN and the requirement for additional hardware. On the other hand, decreasing security requirements allows for data breaches [15].

2. Wireless Sensor Network Applications

WSNs are used in many application areas, such as the military [16], healthcare monitoring [17], industrial automation [18], and smart homes [19], among others [20]. More than 50 companies have attempted to standardize a protocol running over Layer 6LoWPAN called "Thread" (https://www.threadgroup.org/, accessed on 16 May 2022) that perfectly connects and controls smart home devices [21]. Most of these types of WSNs applications [22] are shown in **Figure 3**.

Figure 3. WSNs applications.

However, due to the nature of broadcasting and wireless network vulnerabilities, attackers can quickly inject, intercept, reroute and change overhead connections [23]. This can be risky, especially when networking is used for healthcare applications [4], military applications [24][25], or the detection of human targets [26]. Any security breach can lead to dire consequences. Therefore, WSNs can be of great interest in the civilian sector when used in healthcare. However, these networks containing sensitive data need adequate protection from all kinds of potential security threats and attacks [24]. In addition to the availability of this data, the continuity of its flow is also one of the parts that must be preserved.

3. Security in Wireless Sensor Network

A great deal of research has addressed security concerns in WSN management protocols through the Triangle defined by Confidentiality, Integration, and Authentication (CIA). What is meant by this triangle are the three axes that must be achieved in any network for it to be called secure. Confidentiality is maintaining the privacy of important data transferred between WSN nodes. In general, before sending the packet from the sending node, important segments of the packet are encrypted, and then, at the node that received the packet, the segments are decrypted [27]. In the condition of integrity, the network must be prepared to ensure that attackers cannot alter the messages sent. Attackers can create interference beams to modify their poles. In addition, before forwarding, a malicious routing node can change important data in packets. The last condition of achieving the security triangle is availability. Availability is the availability of the WSN Services at any time required. In any case, attackers can activate attacks that reduce network performance or destroy the entire network. The most harmful risk to network availability is Denial of Service (DoS) [28]; It happens in situations where attackers, by sending wireless interference, disrupting network protocols, or exhausting WSN nodes in various ways, make the network unable to set up services. This type of attack will be discussed below.

A common protocol for the transport layer in 6LoWPAN is the User Datagram Protocol (UDP), which can be overlaid with the Datagram Transport Layer Security (DTLS) protocol to ensure data security [29]. Meanwhile, TLS is operated via the Transmission Control Protocol (TCP), and the AES-128 algorithm is used for link-layer authentication and encryption [30]. However, the TLS/DTLS implementation requires additional hardware encryption hardware to maintain the use of advanced encryption operations [31]. In addition, it is difficult to integrate Internet Protocol security (IPSec) commonly used at the network layer and Transport Layer Security (TLS) into the applications of those networks because these protocols have significant overhead costs and consume significant resources [32]. Likewise, these techniques cannot fully provide the Security Triangle (CIA), since the WSN devices use wireless communication within the range of public communication channels [33]. Therefore, there must be cooperation among a set of protocols so that these types of networks can work effectively in their environments and counteract any malicious attacks. In the domain of WSN security, malicious attacks are divided into groups [15][34], and each group has an impact on sensor nodes according to the level it belongs to. The distribution of these groups at the levels of the WSN model is shown in **Figure 3**.

Based on **Figure 4**, there are different malicious attacks in each different layer, while the DoS attack shares all layers. The DoS, Jamming, Exhaustion, and Collision disrupt network connectivity and availability. Whereas Sybil, Hole, Spoofing, Session hijacking, Eavesdropping, Man in the Middle, and Selective forwarding all threaten confidentiality and integrity [35]. In addition, these attacks that hit connectivity and availability are categorized as active while others can occur in both active and passive states.

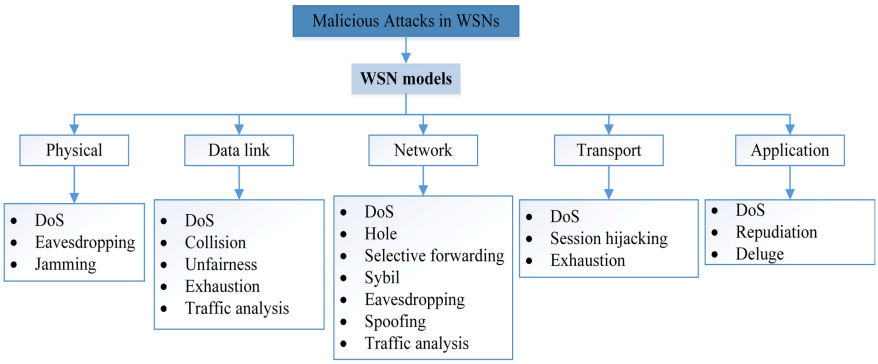

Figure 4. Malicious attacks classifications.

However, each of these layers has distinct tasks regarding reliability in data management and transmission between network nodes. The physical layer increase's reliability by reducing the effect of path loss and shadowing. At the data link layer, the communication between WSN nodes must be interoperable through error recognition and multiplexing [36]. Moreover, the network layer will provide the best route for transmitting data to the edge router. However, in WSNs, each WSN node acts as a router, and the security related to this layer is responsible for securing this path from attacks. In addition, the transport layer is responsible for transmitting data to external networks, and the application layer is responsible for managing, collecting, and processing data to obtain trustworthy results [37].

Furthermore, authentication represents another important issue in the WSN security domain. For instance, the authentication method aims to protect the WSN network from being exploited by illegal WSN nodes. Moreover, different encryption and decryption methods are used in the security domain, while the limitations of WSNs lead to searching through various security technologies [38], in addition to these basic requirements in securing the security of wireless networks and who deals with them. There is also a need to track the actions of connected WSN devices to provide feedback on the events of a breach. Therefore, network security requires what is called non-repudiation, to prove actions for each WSN device [38]. Furthermore, unauthorized access to the network is faster in a WSN environment than in a wired connection, and physical entry is easy due to the hostile environment. If such user authentication is allowed, not only will the network efficiency be affected, but the data security may also be compromised. To avoid this, access control and parsing are essential, which can be provided by a variety of access control policies and encryption methods [32].

Attacks on WSNs

As shown in **Figure 4**, various types of malicious WSN attacks cause not only security issues but also other power and CPU issues. Therefore, these types of networks need to focus more on finding realistic and viable solutions than regular types of networks. In detail, researchers discuss the effect of each type of attack on WSNs.

1. Eavesdropping

Because of the security-related constraints of WSNs (e.g., hostile environment, dynamic nodes, and untrustworthy communication), eavesdropping is a process of acquiring information exchanged between nodes by hackers, which enhances the influence of radio fading and frequency transmission or scattering [39].

2. Jamming

This type of attack is considered one of the most dangerous types for private wireless networks. Despite its risks, security measures are ignored against it, which can cause serious problems after the implementation of wireless networks. The foremost outcome of jamming is that it impedes user service or availability due to radio frequency interference [40].

3. Collision

Since the sensors are located in different environments, this attack could be caused by malicious node replacement corruption. By presenting a brief noise packet, malicious nodes can cause collisions with surrounding broadcasts because

they do not adhere to the Intermediate Access Control Protocol. Although this attack does not consume much energy from the attacker, it can lead to major network outages [41]. Moreover, due to the characteristics of wireless communication, it is difficult to determine the origin node.

4. Unfairness

This type of attack prevents authorized users from accessing network resources and exploits contract connection period settings to bypass the submission deadline [42]. Repeated collision attacks or the random exploitation of the cooperative media access control layer priority methods are examples of this type of attack.

5. Exhaustion

This type of attack recurs collision attacks until the total energy of the WSN nodes is exhausted [41]. In other words, resource depletion attacks deplete node energy by creating routing loops and path lengthening during packet transfers.

6. Traffic monitoring

In WSNs, traffic analysis is a tool for deducing patterns of communication among nodes. The analysis uses data gathered by listening in on node-to-node communication [43]. This attack specifically targets nodes that store confidential data and have the position information of the access point or sink node. As a result, if the attack is successful, a variety of knowledge is disclosed. This has the potential to be deadly to the system.

7. Hole attack

The black hole or sink attacks are network layer exploits that occur during message routing. Cluster heads are the target of this destructive bombardment. A hostile node can be chosen as the cluster head in this attack, and this node will now erase all transactional processes from its member nodes. It can potentially result in a sinkhole [44].

8. Selective forwarding

It is hard to detect a selective redirection threat, particularly when hacked nodes deliberately discard packets. Hackers can use selective redirection to establish route discovery that attracts or deletes network activity. They can also increase or decrease the range of primary routers, send bogus signals, and ignore crucial messages [45].

9. Sybil

The Sybil attack imitates the existence of a sensor node by creating several node IDs from a single current node. It also leads to system failure as a result of resource allocation issues and other issues. It has a huge effect on technologies, such as shared computing, structure management, and server protocols, which all offer load balance [46].

10.Spoofing

This attack specifically affects routing data transferred between nodes, and it can result in routing loops, root path expansions and compression, network traceability to or from selected nodes, network segmentation, bogus error messages, and elevated end-to-end latency [38].

11.Session hijacking

Another type of man-in-the-middle attack is a cookie side takeover, which gives the attacker full access to the application account. When you log in to an online account, such as Facebook or Twitter, the app sends you a ‘session cookie’, which is a piece of information that identifies the user to the server and gives them access to their account. The server will allow the user to use the app as long as their device keeps the session token.

12.Repudiation

Repudiation attacks occur when an application or system fails to implement controls to correctly monitor and log users’ activities, allowing hostile tampering or forgery of additional steps to occur. This exploit can be used to alter the data authoring of harmful user operations to log incorrect data to log files. In a similar way to spoofing electronic mail, its use can be expanded to general data processing in the name of others. If this attack succeeds, the information contained in log files may be deemed inaccurate or deceptive [38].

13.Deluge

Also known as a reprogramming assault, it is an attempt to reconfigure distributed nodes. If the assault is successful, the attacker will be able to seize control of a large portion of the network. The majority of the sensors were put in a hostile area and controlled remotely over a wireless network, which made this assault successful. It may be possible to prevent this through strong authentication.

14.DoS

This type of attack was repeated in all layers of the WSN, which means that it applies to any layer. DoS attack seeks to shut down a system or network, making it unreachable to the intended audience. DoS attacks work by flooding the victim with traffic or providing information that causes the victim to fail. A DoS attack deprives real users (workers, members, or policyholders) of the services or assets they intended to use [29].

Therefore, these attacks can affect the security infrastructure of any organization as illustrated in **Table 1**. Moreover, **Table 2** shows the security infrastructure of WSN networks, and the protection techniques for each baseline.

Table 1. Attacks in security policies.

Security Infrastructure	Attacks
Confidentiality	**Hole, Sybil, Spoofing, Session hijacking, Repudiation, Selective forwarding, Spoofing**
Integrity	**Eavesdropping, traffic analysis, Selective forwarding, Spoofing**
Availability	**DoS, Exhaustion, Jamming, Collision, Unfairness**

Table 2. WSNs protection techniques.

Security Infrastructure	Attacks
Confidentiality	**Encryption**
Integrity	**Digital signature, MAC**
Availability	**Traffic control, redundancy, Rerouting**
Non-repudiation	**Digital certificate**

In any case, malicious attack techniques change and evolve with the development of network protection software. Therefore, to be able to maintain the security of this type of wireless network, researchers must use the skills of self-development of sensors. The best option for their self-learning ability is to use machine learning techniques. Using these technologies, these devices can detect malicious cookies that are of a new type and not included in the current database list. The use of machine learning in WSN security is discussed in the next subsection.

4. Why Is Machine Learning Needed in Wireless Sensor Network Security?

In malevolent circumstances, certain WSNs interact with security-sensitive information in an unsupervised manner. It is critical to use security measures for WSNs in such scenarios. Data confidentiality, data authentication, data integrity, and data freshness can all benefit from the security procedures. Traditional network security solutions, such as user authorization, are not suitable for these applications due to the WSNs' limited resources and processing capabilities [47]. Therefore, for example, the authors in [48] designed an access gateway by using ML classification algorithms, such as Random Forest, k-NN, and Naive Bayes to assess IoT malware network activities. The k-Nearest Neighbor (k-NN) method showed the highest accuracy, according to the outcomes of performance assessment with those kinds of techniques. Moreover, the authors in [49] presented a privacy-preserving Support Vector Machine (SVM) training method for IoT data that requires only two transactions in one iteration and does not require the use of a reliable third party. When compared to conventional SVM, this technique greatly reduced computational complexity.

Therefore, ML technology provides a good model for reducing the cost of some areas of security. Anomaly detection, for example, provided excellent results against all types of malicious activity, and in the process of packet analysis [39][41][50], tracking and protection against DoS [36][42][51][52][53][54][55]. The processes of raising the availability of networks, error detection [56][57][58] and traffic congestion [59][60][61] are also based on the ML approach. In addition to the authentication

operations of the physical layer, it can be a good solution [36][51][62]. Therefore, the application of ML techniques in WSNs aims to solve many of these problems and provide tremendous advantages in terms of flexibility and accuracy.

References

1. Al-Emran, M.; Malik, S.I.; Al-Kabi, M.N. A Survey of Internet of Things (IoT) in Education: Opportunities and Challenges. In Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications; Springer: Cham, Switzerland, 2020; pp. 197–209. ISBN 9783030245139.
2. Zhang, G.; Kou, L.; Zhang, L.; Liu, C.; Da, Q.; Sun, J. A New Digital Watermarking Method for Data Integrity Protection in the Perception Layer of IoT. Secur. Commun. Netw. 2017, 2017, 3126010.
3. Yi, L.; Tong, X.; Wang, Z.; Zhang, M.; Zhu, H.; Liu, J. A novel block encryption algorithm based on chaotic S-Box for wireless sensor network. IEEE Access 2019, 7, 53079–53090.
4. Khashan, O.A.; Ahmad, R.; Khafajah, N.M. An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. Ad. Hoc. Netw. 2021, 115, 102448.
5. Kumar, V.; Tiwari, S. Routing in IPv6 over low-power wireless personal area networks (6LoWPAN): A survey. J. Comput. Netw. Commun. 2012, 2012, 316839.
6. Patel, N.R.; Kumar, S. Wireless Sensor Networks' Challenges and Future Prospects. In Proceedings of the 2018 International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 23–24 November 2018; pp. 60–65.
7. Zhang, X.; Heys, H.M.; Li, C. Energy efficiency of encryption schemes applied to wireless sensor networks. Secur. Commun. Netw. 2012, 5, 789–808.
8. Al-Kashoash, H.A.A.; Kharrufa, H.; Al-Nidawi, Y.; Kemp, A.H. Congestion control in wireless sensor and 6LoWPAN networks: Toward the Internet of Things. Wirel. Networks 2019, 25, 4493–4522.
9. Luo, J.; Zhang, Z.; Liu, C.; Luo, H. Reliable and Cooperative Target Tracking Based on WSN and WiFi in Indoor Wireless Networks. IEEE Access 2018, 6, 24846–24855.
10. Qiao, B.; Ma, K. An enhancement of the ZigBee wireless sensor network using bluetooth for industrial field measurement. In Proceedings of the 2015 IEEE MTT-S International Microwave Workshop Series on Advanced Materials and Processes for RF and THz Applications (IMWS-AMP), Suzhou, China, 1–3 July 2015; pp. 2–4.
11. Ghosh, R.K. Wireless Networking and Mobile Data Management; Springer: Singapore, 2017; ISBN 978-981-10-3940-9.
12. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet Things J. 2017, 4, 1250–1258.
13. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. Comput. Netw. 2015, 76, 146–164.
14. Akhtar, F.; Rehmani, M.H. Energy replenishment using renewable and traditional energy resources for sustainable wireless sensor networks: A review. Renew. Sustain. Energy Rev. 2015, 45, 769–784.
15. Lee, C.C. Security and privacy in wireless sensor networks: Advances and challenges. Sensors 2020, 20, 744.
16. Winkler, M.; Street, M.; Tuchs, K.-D.; Wrona, K. Wireless Sensor Networks for Military Purposes. In Autonomous Sensor Networks; Springer: Berlin/Heidelberg, Germany, 2012; pp. 365–394.
17. Pan, J.; Xu, Z.; Li, S. Security mechanism for a wireless-sensor-network-based healthcare monitoring system. IET Commun. 2012, 6, 3274–3280.
18. Calvanese Strinati, E.; Barbarossa, S.; Gonzalez-Jimenez, J.L.; Ktenas, D.; Cassiau, N.; Maret, L.; Dehos, C. 6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication. IEEE Veh. Technol. Mag. 2019, 14, 42–50.
19. Wang, H.; Wang, J.; Huang, M. Building a smart home system with WSN and service robot. In Proceedings of the 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation, Hong Kong, China, 16–17 January 2013; pp. 353–356.
20. Kasah, N.B.H.; Aman, A.H.B.M.; Attarbashi, Z.S.M.; Fazea, Y. Investigation on 6LoWPAN data security for internet of things. In Proceedings of the 2020 2nd International Conference on Computer and Information Sciences, ICCIS 2020, Aljouf, KSA, Saudi Arabia, 7–9 April 2020; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2020.

21. Seliem, M.; Elgazzar, K. IoTeWay: A Secure Framework Architecture for 6LoWPAN Based IoT Applications. In Proceedings of the 2018 IEEE Global Conference on Internet of Things (GCIoT 2018), Alexandria, Egypt, 5–7 December 2018; pp. 1–5.
22. Messaoud, S.; Bradai, A.; Bukhari, S.H.R.; Quang, P.T.A.; Ben Ahmed, O.; Atri, M. A survey on machine learning in Internet of Things: Algorithms, strategies, and applications. Internet Things 2020, 12, 100314.
23. Mo, J.; Chen, H. A Lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks. Secur. Commun. Netw. 2019, 2019, 2136506.
24. Nelli, A.; Mangasuli, S. Wireless Sensor Networks: An Overview on Security Issues and Challenges. Int. J. Adv. Eng. Manag. Sci. 2017, 3, 209–214.
25. Finogeev, A.G.; Finogeev, A.A. Information attacks and security in wireless sensor networks of industrial SCADA systems. ACM Int. Conf. Proc. Ser. 2020, 5, 6–16.
26. Yang, B.; Liu, F.; Yuan, L.; Zhang, Y. 6LoWPAN Protocol Based Infrared Sensor Network Human Target Locating System. In Proceedings of the Proceedings of the 15th IEEE Conference on Industrial Electronics and Applications, ICIEA 2020, Kristiansand, Norway, 9–13 November 2020; pp. 1773–1779.
27. Yousefpoor, M.S.; Barati, H. Dynamic key management algorithms in wireless sensor networks: A survey. Comput. Commun. 2019, 134, 52–69.
28. Wang, M.; Lu, Y.; Qin, J. A dynamic MLP-based DDoS attack detection method using feature selection and feedback. Comput. Secur. 2020, 88, 101645.
29. Kumar, P.M.; Gandhi, U.D. Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. J. Supercomput. 2020, 76, 3963–3983.
30. Bouaziz, M.; Rachedi, A. A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology. Comput. Commun. 2016, 74, 3–15.
31. Olsson, J. 6LoWPAN Demystified; Texas Instruments: Dallas, TX, USA, 2014; Volume 13, pp. 1–13.
32. Yang, Y.; Zheng, X.; Guo, W.; Liu, X.; Chang, V. Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Inf. Sci. 2019, 479, 567–592.
33. Ahmad, R.H.; Pathan, A.-S.K. A Study on M2M (Machine to Machine) System and Communication. In Security Solutions and Applied Cryptography in Smart Grid Communications; IGI Global: Hershey, PA, USA, 2016; pp. 179–214. ISBN 9781522518310.
34. Glissa, G.; Meddeb, A. 6LoWPAN multi-layered security protocol based on IEEE 802.15.4 security features. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 264–269.
35. Mamdouh, M.; Elrukhsi, M.A.I.; Khattab, A. Securing the Internet of Things and Wireless Sensor Networks via Machine Learning: A Survey. In Proceedings of the 2018 International Conference on Computer and Applications (ICCA), Beirut, Lebanon, 25–26 August 2018; pp. 215–218.
36. Liao, R.F.; Wen, H.; Wu, J.; Pan, F.; Xu, A.; Jiang, Y.; Xie, F.; Cao, M. Deep-learning-based physical layer authentication for industrial wireless sensor networks. Sensors 2019, 19, 2440.
37. Yu, J.Y.; Lee, E.; Oh, S.R.; Seo, Y.D.; Kim, Y.G. A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security. IEEE Access 2020, 8, 45304–45324.
38. Karakaya, A.; Akleylek, S. A survey on security threats and authentication approaches in wireless sensor networks. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–4.
39. Zou, Y.; Wang, G. Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack. Proc. IEEE Trans. Ind. Inform. 2016, 12, 780–787.
40. Hamza, T.; Kaddoum, G.; Meddeb, A.; Matar, G. A survey on intelligent MAC layer jamming attacks and countermeasures in wsns. In Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18–21 September 2016; pp. 42–56.
41. Reindl, P.; Nygard, K.; Du, X. Defending malicious collision attacks in wireless sensor networks. In Proceedings of the 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, 11–13 December 2010; pp. 771–776.
42. Tayebi, A.; Berber, S.M.; Swain, A. Wireless sensor network attacks: An overview and critical analysis with detailed investigation on jamming attack effects. Smart Sens. Meas. Instrum. 2015, 11, 201–221.

43. Ward, J.R.; Younis, M. A cross-layer defense scheme for countering traffic analysis attacks in Wireless Sensor Networks. In Proceedings of the MILCOM—2016 IEEE Military Communications Conference, Baltimore, MD, USA, 1–3 November 2016; pp. 972–977.
44. Karuppiah, A.B.; Dalfiah, J.; Yuvashri, K.; Rajaram, S. An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks. In Proceedings of the International Confernce on Innovation Information in Computing Technologies, Chennai, India, 19–20 February 2015; pp. 1–7.
45. Alajmi, N.M.; Elleithy, K.M. Selective forwarding detection (SFD) in wireless sensor networks. In Proceedings of the 2015 Long Island Systems, Applications and Technology, Farmingdale, NY, USA, 1 May 2015.
46. Patel, S.T.; Mistry, N.H. A review: Sybil attack detection techniques in WSN. In Proceedings of the 2017 4th International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, 24–25 February 2017; Volume 17, pp. 184–188.
47. Modares, H.; Salleh, R.; Moravejosharieh, A. Overview of security issues in wireless sensor networks. In Proceedings of the 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, Langkawi, Malaysia, 20–22 September 2011; pp. 308–311.
48. Kumar, A.; Lim, T.J. EDIMA: Early Detection of IoT Malware Network Activity Using Machine Learning Techniques. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 289–294.
49. Shen, M.; Tang, X.; Zhu, L.; Du, X.; Guizani, M. Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities. IEEE Internet Things J. 2019, 6, 7702–7712.
50. O'Mahony, G.D.; Harris, P.J.; Murphy, C.C. Investigating Supervised Machine Learning Techniques for Channel Identification in Wireless Sensor Networks. In Proceedings of the 2020 31st Irish Signals and Systems Conference (ISSC), Letterkenny, Ireland, 11–12 June 2020.
51. Chen, S.; Wen, H.; Wu, J.; Chen, J.; Liu, W.; Hu, L.; Chen, Y. Physical-Layer Channel Authentication for 5G via Machine Learning Algorithm. Wirel. Commun. Mob. Comput. 2018, 2018, 6039878.
52. Borkar, G.M.; Patil, L.H.; Dalgade, D.; Hutke, A. A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept. Sustain. Comput. Inform. Syst. 2019, 23, 120–135.
53. Premkumar, M.; Sundararajan, T.V.P. DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. Microprocess. Microsyst. 2020, 79, 103278.
54. Singh, K.J.; De, T. MLP-GA based algorithm to detect application layer DDoS attack. J. Inf. Secur. Appl. 2017, 36, 145–153.
55. Lu, X.; Han, D.; Duan, L.; Tian, Q. Intrusion detection of wireless sensor networks based on IPSO algorithm and BP neural network. Int. J. Comput. Sci. Eng. 2020, 22, 221–232.
56. Javaid, A.; Javaid, N.; Wadud, Z.; Saba, T.; Sheta, O.E.; Saleem, M.Q.; Alzahrani, M.E. Machine learning algorithms and fault detection for improved belief function based decision fusion in wireless sensor networks. Sensors 2019, 19, 1334.
57. Zhang, H.; Liu, J.; Kato, N. Threshold Tuning-Based Wearable Sensor Fault Detection for Reliable Medical Monitoring Using Bayesian Network Model. IEEE Syst. J. 2018, 12, 1886–1896.
58. Titouna, C.; Aliouat, M.; Gueroui, M. FDS: Fault Detection Scheme for Wireless Sensor Networks. Wirel. Pers. Commun. 2016, 86, 549–562.
59. Rezaee, A.A.; Pasandideh, F. A Fuzzy Congestion Control Protocol Based on Active Queue Management in Wireless Sensor Networks with Medical Applications. Wirel. Pers. Commun. 2018, 98, 815–842.
60. Masdari, M. Energy Efficient Clustering and Congestion Control in WSNs with Mobile Sinks; Springer: Berlin/Heidelberg, Germany, 2020; Volume 111, ISBN 0123456789.
61. Sangeetha, G.; Vijayalakshmi, M.; Ganapathy, S.; Kannan, A. A heuristic path search for congestion control in WSN. Lect. Notes Netw. Syst. 2018, 11, 485–495.
62. Pan, F.; Wen, H.; Liao, R.; Jiang, Y.; Xu, A.; Ouyang, K.; Zhu, X. Physical layer authentication based on channel information and machine learning. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017; Volume 40, pp. 364–365.