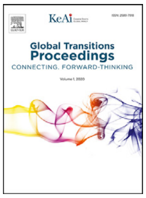
Contents lists available at ScienceDirect

Global Transitions Proceedings

journal homepage: http://www.keaipublishing.com/en/journals/global-transitions-proceedings/



Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures

M. Keerthika[a,*], D. Shanmugapriya[b]

[a] Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore-641043, India
[b] Department of Information Technology, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore-641043, India

ARTICLE INFO

Keywords:
Active attacks
Challenges
Constraints
Passive attacks
Wireless Sensor Network(WSN)

ABSTRACT

Wireless sensor network has attracted significant attention in research and development due to its tremendous applications in medical, military and defence, medical, environmental, industrial, infrastructure protection, and commercial applications to enable to interact with each other controlled remotely. A Wireless Sensor Network (WSN) has wide applications such as environmental monitoring and tracking of the target nodes for communication. The sensor nodes are equipped with wireless interfaces used for communication between the nodes and another network. Wireless Sensor Network suffers from many constraints that make security a primary challenge. When the sensor node is deployed in a communication environment unattended, the nodes are vulnerable to various attacks. This paper deals with the different types of Active and Passive security attacks in Wireless Sensor Networks to design effective countermeasures for secured communication. This paper will help researchers identify the most vulnerable attacks in the communication and defensive mechanisms to encounter the attacks in WSN.

1. Introduction

Wireless Sensor Networks are large-scale networks made of Self-configured and spatially distributed, small size devices, low cost, low power using sensors to collect and transfer the data in the wireless communication channel. The sensor nodes are designed so that it is feasible to work with limited facilities like energy, memory, computation, and the transmission channel. The WSN consists of several sensing nodes that interact with each other, and they are distributed and in a spatial way on any physical/environmental phenomenon. The classic wireless sensor node consists of four main parts Sensor Module, a Processing & Memory Module, Transceiver Module, and a Power Unit. The sensor nodes in a network can process, gather information, and interact with other nodes [1]. The main goals of the WSN are privacy or confidentiality, integrity, authentication, and availability. WSNs utilize multiple services to share the frequency spectrum and use similar and different protocols [2]. WSNs are self-organizing, self-repairing, and operate a dynamic topology in the multi-hop environment, which faults tolerance and vulnerability to malicious attacks.

The rest of the section in the paper is organized as follows: In Section 2, the literature review work of various security attacks has been explored. Section 3 describes the Security requirements of WSN. The basic clustered architecture of the WSN and the most common architecture that follows the OSI model are reviewed in Section 4. The significant challenges and constraints faced in a Wireless Sensor Network are discussed in Section 5, and the final section gives the details of the various security attacks in WSN.

2. Literature Review

The Wireless Sensor Network is vulnerable to numerous security attacks, and there is loss of information variable to the physical environment and invasion of the attacks. The author in [3] proposed a survey of protocols and design constraints of specific tools. The main challenge is to design robust security protocols with low maintenance. The author proposed in [4] has improved and discussed the security mechanism at the different layers of the network. The author also stated that improving the efficiency and defense mechanisms to overcome the attacks in all the layers. The work is given in [5] a security scheme for the system with robust security protocols for managing sensor nodes in networks and energy efficiency.

The author of [6] listed out the classification of protocols at various layers with high-level and application-based protocols and its defensive measures against each attack in the OSI layers with a security framework. In [7], the author proposed the security problems in IoT and WSN using machine learning algorithms. It does not need interactions with humans that suit both the environment to overcome the data set for learning and the availability of the resources. The author surveyed

[*] Corresponding author.
E-mail address: 20phcsp001@avinuty.ac.in (M. Keerthika).

https://doi.org/10.1016/j.gltp.2021.08.045
Received 16 June 2021; Accepted 5 July 2021
Available online 12 August 2021

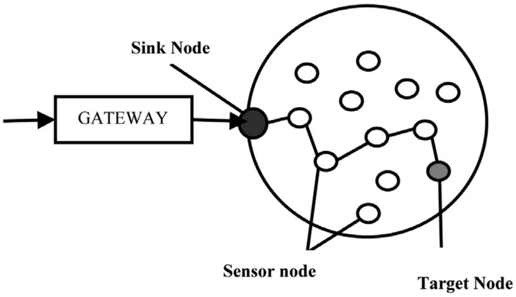


Fig. 1. The basic architecture of WSN.

[8] the security requirements with future research scopes and resource constraint nature and the types of sensors available for different applications.

To evaluate the performance of existing detection methods, the author [9] has reviewed eleven types of mainstream attacks with the existing detection methods. Detection is based on the percentage of the verified packets that reached the base station by checking the probability of packets forwarding [1].

In [11], the author has evaluated different types of attacks; the most vulnerable attack is resolved by using the sharing of key and ensuring security in transmitting the data in the communication channel. The attacker can flood into the network by replicating the nodes by which traffic exists; the power and energy of the node are entirely drained to halt the communication between the nodes. The observations in the above review are that the authors detailed the security attacks of WSN, its detection methods and counter mechanisms.

3. Security Requirements

The main goal of the security services in the WSN is to provide data and information protected from any types of attacks [13]. The various security requirements in WSN, which are as follows:

- Availability: It is essential that the resources are available in the operational network for the message to move on and ensures that the nodes can utilize the resource and the network also [23].
- Authorization: It ensures that authorized sensors provide information to the services in the operational network.
- Authentication: It implies that sensor nodes in the communication are genuine and have proper access to the network.
- Confidentiality: It ensures that the message in the communication network cannot be read and understood by the attackers.
- Integrity: It refers that the message is not altered or tampered with while it was on the network communication. By simply injecting additional packets, the entire packet can be changed [23].

4. Basic architecture of wireless sensor network

The author(s) of [12], has described the architecture of WSN where the sensor nodes self-organize among themselves into a multi-hop network through the wireless channel for communication and forward the data from one base station to another station. It has one or more base stations called sink with a large number of sensing devices. Each node in the network has one or more sensors that are low-powered and battery operated. The sensor network has many sensor nodes used to transfer data, and several resource-constrained sensor nodes form it. The following Fig. 1 shows the basic architecture of WSN.

The sensor nodes are the primary field devices in the WSN architecture, and they are responsible for routing packets [17]. The sensor nodes have three subsystems: Sensor Subsystem, Processing subsystem, and Communication subsystem.

The sensor network has five layers based on the OSI model: Application layer, Transport layer, Network layer, Data Link layer, Physical layer [9]. In addition to the above listed five layers, the Sensor network has three cross-layer planes: Task management plane, Mobility management plane, and Power management plane, to increase overall efficiency and make the sensor nodes work together in the network shown in Fig. 2.

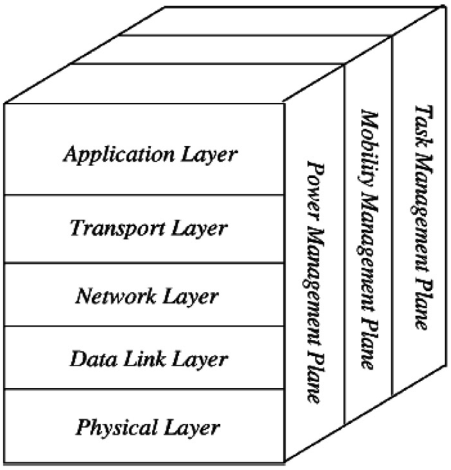


Fig. 2. The Layered architecture of WSN.

5. Challenges and Constraints of WSN

In the WSN, there are many challenges faced by the sensor network to develop reliable communication in the transmission of data, Quality of Service, and also in energy consumption, hardware, and software complexity. The constraints of WSN rely on Power consumption, storage, and computation.

5.1. Wireless Sensor Network Challenges

The challenges in the WSN [8] according to the requirement of the applications in which some are listed below:

(1) **Energy efficiency: -** Energy efficiency is the main issue as WSN is a resource-constrained network. The consumption of energy is utilized during the data packet routing activity. It mainly depends on the lifespan of the sensor nodes' battery.
(2) **Prolonged network lifetime: -** Another challenge is to prolong the lifetime of the nodes by decreasing the energy consumption and extend the WSN's life cycle.
(3) **Quality of service: -** Each application has its terms of QoS, and it may request different QoS Processing. Due to the limitations of hardware devices, providing QoS is still a challenging task.
(4) **Fault tolerance: -** The nodes can sustain the functions carried out in the network even when there is limited power in the battery, failure rate of nodes, and interference from the external environment.
(5) **Dynamic environment: -** The ability of the WSN to withstand harsh environmental conditions where they are primarily deployed in hazardous areas and some of the locations may be unattended.
(6) **Hardware and software complexity: T**he hardware units of the nodes perform the functions as processing, storage, and energy source to connect a sensor to the radio transmitter [5]. The hardware devices used in the network should be energy efficient and reliable. The OS should be independent to manage the hardware of the nodes, and also, the data extraction and manipulation should manage the concurrency according to the requirement of the application.

5.2. Constraints in Wireless Sensor Network

In [6], the author has detailed how to develop security mechanisms in wireless sensor network, and it is primarily necessary to understand the resources of the network

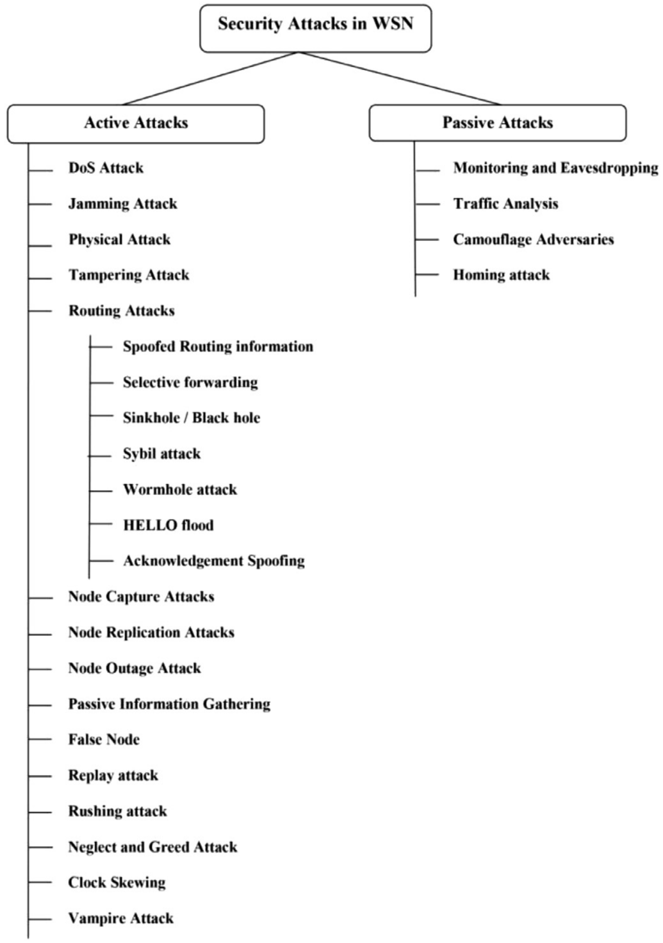


Fig. 3. Security attacks in WSN.

Resource constraints are as follows:

(1) **Limited Storage:** It refers to data storage and key mechanisms to secure the data. It is a challenge to develop a secured network with high security-designed protocols.
(2) **Limited Computational power:** The computation is based on energy for designing and executing the keys. The designed algorithm for key mechanisms should reduce the computation power.
(3) **Limited Power:** Due to the lack of wires and the small size of sensor nodes, power restriction is there in WSNs. Sensor nodes are battery-driven. Power limitation affects security since encryption algorithm causes communication overhead.

6. Security attacks on Wireless Sensor Network

The issues in wireless sensor network privacy and security have been systematically reviewed. In the wireless sensor network, two types of attacks are mainly due to the transmission medium's nature: Active Attacks and Passive Attacks [15]. In Active attacks, the attackers intend to search and destroy the information, whereas, in Passive attacks, the attackers only intend to steal valuable information like passwords and confidential data. However, in the wireless network, the users and organizations must be aware of both attacks for secure communication between the sensor nodes. Fig. 3 shows the classification of the various security attacks in WSN.

6.1 Active Attacks – The main objective of the attackers is to harm the network by altering and modifying the data. The attacker sets up regular communication by altering or destroying the data which has to be communicated in the network [11].

(1) DoS Attack – DoS attacks in which the attackers reduce the network services by providing the malicious node to distract them. The main threat is an attack on the availability of the resources and services to transmit data. The attackers either destroy or distract the configuration of the infrastructure in the sensor network. The DoS attack can occur in any layer of the OSI model of the WSN by affecting the protocols of the transmission medium, consuming the resources, destroying the physical components [16].

(2) Jamming Attack – The attack can be launched both externally and internally by an attacker. The attacker uses the high-power transmitter to interfere with legitimate wireless communication. The attacker prevents the source from transmitting the packets or denying the transmission of legitimate packets. There are various jammers and jamming techniques that can interfere with the capabilities of WSN [14].

(3) Physical Attack – The wireless sensor network is operated in remote and unreceptive environments. The distributed and unattended nodes on the nature of WSN make them vulnerable to physical attacks. The nodes are destroyed eternally in the physical, so there is a permanent loss of the nodes [4]. Tamper proofing is one method of preventing physical attacks.

(4) Tampering Attack – The intruder modifies the nodes or damages the node's services and takes complete control over the captured node. The physical devices are damaged in this attack, so that the resources will be deficient [6]. The attack is prevented by changing the key frequently, and proper key management schemes are implemented.

(5) Routing Protocol Attacks – In the sensor nodes, routing and data forwarding are essential tasks in which the protocols are energy-efficient and robust against any attack. The secure routing protocol must provide availability, authentication, integrity, and confidentiality. The authorized receiver should receive the original message that the sender proposed in the network and the message's integrity and sender's identity. The routing attacks and mitigation methods of these attacks have been investigated thoroughly [17]. Some of the routing protocol attacks in WSN are as follows:

- **Spoofed Routing information** – The attacker disrupts the network's functioning by spoofing or impersonating one entity by another and makes the victim believe that communication with a different entity. This attack can be prevented by MAC authentication. The spoofed routing and how the attacker impersonates or spoofs its own identity as another entity make the receiver believe that communication with a different entity [17]. The normal functioning of the network is interrupted and disrupted. This attack leads to false error messages, changing the routes, and discarding the messages in the network. Spoofing attacks can be prevented by using MAC to use the same hash functions and generate the secret keys [11].
- **Selective forwarding** – The attacker selects some of the nodes or particular packets for forwarding and then drops or deletes the rest of the packets in the sensor network. In the Multi-hop WSN, whether all sensor nodes forward the received messages to the neighbor nodes, some nodes might deny forwarding the message [7]. Multi-path routing, sensor node monitoring, and finding a different routing path are the defense mechanisms against this attack [11].
- **Sinkhole Attack** – In [18], sinkhole attack detection and its prevention strategies have been reviewed. In this attack, the entire traffic from a specific area is diverted by a compromised node in the false routing metric. So the neighboring nodes believe that there exists a high-quality path and start forwarding the packets to the malicious node. The process of gathering traffic is called a sinkhole attack. The sinkhole attack [19] aims at harming the data at the collection point, which compromises the reliability and integrity of the data sent by the sensor nodes in the network. This attack can be avoided by giving each node a certificate that combines the node's identification with unique information. As a result, to communicate, the identity node must provide certificates.

- **Blackhole attack** – The security attacks in WSN in which the black hole attack has two distinct characteristics. The malicious node act as a black hole when the packets pass through these black holes, then the attacker can manipulate the data. First, the path is amended by announcing itself as having a route from the source to the destination node, next without forwarding the invader intercept messages for its purpose [10]. A black hole attack can be avoided by monitoring the network, changing packet routing, or using authentication mechanisms.
- **Sybil attack** – In the Sybil attack, the attackers use malicious nodes to present or duplicate themselves with multiple identities to the other nodes. They are components of the network that lures the victim that certain redundancy is achieved [10]. The malicious Sybil attack in online social networks and its defense techniques, including authentication and ID-based encryption symmetric-key techniques, have been detailed [20].
- **Wormhole attack** – The most devastating and complicated attack in a wireless sensor network is the Wormhole attack. In this attack, the attacker keeps track of the packets and makes a tunnel with other nodes of different communication networks, and thus the attacker passes the packets through this tunnel [21]. Pocket leashes and geographic and temporal leashes can prevent this attack because the receiver can detect packets traveling over long distances.
- **HELLO flood attack** – The attackers replicate the messages in the sensor network. It broadcasts itself as a parent node Hello packet with high power so that all nodes and even distant nodes will communicate with the Hello Packet node [22]. The identity verification protocol can be used to authenticate and raise the alarm if an attacker attempts to become a neighbor node, preventing this attack. The Packet leash mechanism is also used when this attack is detected in the network layer.
- **Acknowledgment Spoofing** In this attack, the attacking node spoofs the acknowledgment of the neighboring nodes and gives away the fake information to the neighbor sensor nodes. The purpose is to provide false information or convince the dead node to be alive or energy degradation [11]. To prevent this attack, the bi-directional link verification mechanism is used in both directions.

(6) **Node Capture Attack –** The node capture attack is a severe issue in the WSN. The intruder performs various operations and compromises the whole network. The Node Capture attack removes some of the sensor nodes and redeploys them to perform multiple attacks. A redeployed malicious node is used to modify the information in the communication channel in the WSN [4].

(7) **Node Replication attack** – This attack is also known as a Clone attack. The WSN is exposed to an insecure environment where the malicious nodes can be replicated into several clones. The replicated nodes will have legitimate ID and keys to communicate with other nodes as normal nodes in the operational network [9]. The countermeasure is to provide a unique pair-wise key that supports secure communication between the neighbours.

(8) **Node Outage attack** – In this attack, the functionality of the Wireless sensor components like sensor nodes or communication link or parent node is stopped completely. Hence, the communication to other clustered nodes in different areas is interrupted [4]. The time protocols are designed in such a way that they provide packets with an alternate routing path.

(9) **Passive Information Gathering** – The attacker uses powerful algorithms to intercept the messages that permit them to find nodes and destroy them provided for the unencrypted information, including the sensor nodes' physical location. The attacker also gains access to application-specific message contents [27]. To counteract this attack, a well-designed antenna with encrypted data and powerful algorithms is used.

(10) **False Node** – The intruder inserts a malicious node with inaccurate data or impedes the channel of correct data. So the malicious node sends incorrect data that reaches all the nodes in the operational network, which potentially captures the entire network in control of the intruder or annihilating the network as the whole [27]. To counteract the false node attack, an En-routing scheme is used.

(11) **Replay attack** – In WSN, the attacker replays the malicious node repeatedly for energy consumption and also dominates the communication channels [5]. In this attack, the network's topology keeps on changing due to the mobility of the sensor nodes. The effective way to overcome this attack is to spending session tokens and including timestamps with the messages.

(12) **Rushing attack** – The attack takes place in On-demand routings protocol. The malicious node rushes to take the data from the neighbour to the other destination node in the different tunnel. In the wormhole attack, the packets tunneled through the network can disseminate than any usual multi-hop route; if the packets are tunneled through a speedy transmission route between the wormhole attack ends, it is called a Rushing attack [24]. The countermeasure of this attack is to providing route records by embedding a node list.

(13) **Neglect and Greed Attack –** The malicious node selects the longest path to send the packets by routing them to the wrong node. The primary motivation is to target the information loss and availability of the node in the network. The attacker receives the packets and refuses to forward them to the neighboring nodes [11]. Authentication mechanisms as well as detecting malicious nodes both can help to avoid this attack.

(14) **Clock Skewing** – In this attack [25], the attacker fakes the target skew by altering the timestamp of the forwarding packets. The clock skew of every physical device for the Wireless Sensor Network differs according to the application. By changing the time synchronization period, flooding time synchronization protocol (FTSP) can defend against clock skew attacks.

(15) **Vampire Attack** – This attack is the class of DoS attack where it consumes power of the sensor nodes and completely disables the network [26]. Bcast id is an additional field in the routing table at each node and in data packets used by the AODV routing protocol to detect directional antenna attacks. To counteract the vampire attack, various validations are performed to ensure that packets are not transmitted in infinite loops, which disable the network and drain the battery.

6.2. Passive Attacks

The gathered multiple instances from different resources to describe the Passive attack in the wireless sensor network [4], that the message is not altered or damaged. The unauthorized invaders monitoring the communication channels are termed Passive Attacks. These attacks do not change anything in the communication; the attackers are listeners but the preliminary stage of all the active attacks. The most common Passive Attacks are discussed below:

- **Monitoring and eavesdropping** – Eavesdropping attacks do not affect the integrity of the network. The malicious node intercepts the message in the operational network. The attackers snoop the data to find out the communication channel and violate the privacy of the communication network. It is the most common attack on data privacy.
- **Traffic analysis** – In this type of attack, the attacker analysis the patterns followed in the communication. The attacker discloses the pattern to the opponent to harm and facilitate damage to the wireless sensor network by any type of active attack. The network is monitored regularly to prevent this attack.
- **Camouflage Adversaries** – The attacker hides the desired number of nodes in the wireless sensor network and imitates them as a regular node, leading to the packets' misrouting to different communication channels.
- **Homing Attack** – The attacker does not modify or alter the packets, only aims to find out the network's insight resources, which is

Table 1.
Summary of attacks in Wireless Sensor Network.

Year	Authors	Type of attack	Active / Passive	Description	Counter Measures
2021[16]	Shi. L et al.	DoS Attack	Active	The availability of the resources and services. Destroy or distract the configuration of the infrastructure	Encryption algorithms, Monitoring, Prioritizing messages.
2019[14]	Verma. R et al.	Jamming Attack	Active	Externally and internally by an attacker. Prevents the source from transmitting the packets or denying the transmission of legitimate packets.	Spread spectrum, Mapping region, Jamming Techniques
2019[4]	Butun, I., Osterberg, P., & Song, H.	Physical Attack	Active	The nodes are destroyed eternally in the physical attack.	Tamper proofing
2018[6]	Dewal. P et al	Tampering Attack	Active	Damages the node's services and takes complete control over the captured node.	Changing the key frequently, proper key management schemes
2019[17]	Raoof. A et al.	Spoofed Routing information	Active	Disrupts the network's functioning by spoofing or impersonating one entity by another. Makes the victim believe that communication with a different entity.	MAC authentication
2018[7]	Mamdouh. M et al.	Selective forwarding	Active	Selects some of the nodes or particular packets for forwarding and then drops or deletes the rest of the packets in the sensor network.	Multi-path routing, sensor node monitoring, and finding a different routing path
2019[18]	Rehman, Au, Rehman, S.U. & Raheem, H.	Sinkhole Attack	Active	The entire traffic from a specific area is diverted by a compromised node in the false routing metric.	Identification with unique information
2020[10]	Jilani, S. A., Koner, C., & Nandi, S.	Blackhole attack	Active	Node act as a black hole when the packets pass through these black holes, then the attacker can manipulate the data	Monitoring the network, changing packet routing, authentication mechanisms
		Sybil attack	Active	Components of the network that lures the victim that certain redundancy is achieved	Authentication and ID-based encryption symmetric-key techniques
2018[21]	Giri, Diksha & Borah	Wormhole attack	Active	Makes a tunnel with other nodes of different communication networks, and thus the attacker passes the packets through this tunnel	Pocket leashes and geographic and temporal leashes
2018[22]	Gill, R. K., Sachdeva M.	HELLO flood attack	Active	The attackers replicate the messages in the sensor network.	Packet leash mechanism
2020[11]	‘ Verma, R., & Bharti, S.	Acknowledgment Spoofing	Active	Spoofs the acknowledgment of the neighboring nodes and gives away the fake information to the neighbor sensor nodes.	Bi-directional link verification mechanism
		Neglect and Greed Attack	Active	Selects the longest path to send the packets by routing them to the wrong node.	Redundancy, Authentication mechanisms.
		Homing Attack	Passive	Aims to find out the network's insight resources, which is used to launch any active attacks	Encryption
2019[4]	Butun, I., Osterberg, P., & Song, H.	Node Capture Attack	Active	Removes some of the sensor nodes and redeploys them to perform multiple attacks.	LEAP protocol
		Node Outage attack	Active	Components like sensor nodes or communication link or parent node is stopped completely.	Time protocols, Powerful algorithms
		Monitoring and eavesdropping	Passive	Intercepts the message in the operational network.	Directional Antenna
		Traffic analysis	Passive	The attacker discloses the pattern to the opponent to harm and facilitate damage	Network monitoring
		Camouflage Adversaries	Passive	Leading the packets' misrouting to different communication channels.	Privacy analysis
2019[9]	Xie. H et al.	Node Replication attack	Active	Replicated nodes will have legitimate ID and keys to communicate with other nodes as normal nodes .	Unique pair-wise key
2018[27]	Muhammad Noman Riaz et al.	Passive Information Gathering	Active	Powerful algorithms to intercept the messages that permit them to find nodes and destroy them.	Well-designed antenna
		False Node	Active	Inaccurate data or impedes the channel of correct data. So the malicious node sends incorrect data	En-Routing Scheme
2017[5]	Jadhav, Rutuja & Vatsala, Vatsala.	Replay attack	Active	Replays the malicious node repeatedly for energy consumption	Session tokens, timestamps with the messages.
2019[24]	Bharti, D., Nainta, N., & Monga, H.	Rushing attack	Active	Rushes to take the data from the neighbour to the other destination node in the different tunnel.	Embedding a node list
2014[25]	Huang, D.-J., & Teng, W.-C.	Clock Skewing	Active	The attacker fakes the target skew by altering the timestamp of the forwarding packets.	FTSP and Changing Time Synchronization period
2017[26]	Sharma M. K. and Joshi B. K.	Vampire Attack	Active	This attack is the class of DoS attack where it consumes power of the sensor nodes and completely disables the network	Validation techniques

used to launch any active attacks [11]. Cluster heads, also known as cryptographic key managers, use traffic pattern analysis and header encryption technique to identify and target nodes to prevent this type of attack.The following Table 1 describes about the summary of various active and passive attacks in Wireless Sensor Network are as follows.

7. Conclusion

The paper summarized the security challenges and constraints of wireless sensor networks and various security attacks in the WSN. The active and passive attacks are analyzed, which gives the researchers an insight into various attacks in WSN. The users should also know about the privacy issues and permissions given for the data and how they misuse the information and propose future research exploring the effective security mechanisms and countermeasures.

References

[1] A. Johnson, J. Molloy, J. Yunes, J. Puthuparampil, A. Elleithy, Security in wireless sensors networks, IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2019.

[2] G.D. O'Mahony, J.T. Curran, P.J. Harris, C.C. Murphy, Interference and intrusion in wireless sensor networks, IEEE Aerosp. Electron. Syst. Mag. 35 (2) (2020) 4–16.

[3] K.Z Turakulovich, S.L. Tokhirovich, Analysis of security protocols in wireless sensor networks, in: International Conference on Information Science and Communications Technologies (ICISCT), 2019, pp. 1–4.

[4] I. Butun, P. Osterberg, H. Song, Security of the Internet of Things: vulnerabilities, attacks and countermeasures, IEEE Commun. Surv. Tutor. (2019) 1–1.

[5] Jadhav, Rutuja & Vatsala, Vatsala, Security issues and solutions in wireless sensor networks, Int. J. Comput. Appl. (2017) 14–19.

[6] P. Dewal, G.S. Narula, V. Jain, A. Baliyan, "Security attacks in wireless sensor networks: a survey", 2018.

[7] M. Mamdouh, M.A.I. Elrukhsi, A Khattab, Securing the Internet of Things and wireless sensor networks via machine learning: a survey, in: International Conference on Computer and Applications (ICCA), 2018, pp. 215–218.

[8] N.R. Patel, S. Kumar, Wireless sensor networks' challenges and future prospects, International Conference on System Modeling & Advancement in Research Trends (SMART), 2018.

[9] H. Xie, Z. Yan, Z. Yao, M. Atiquzzaman, Data collection for security measurement in wireless sensor networks: a survey, IEEE IoT J. 6 (2) (2019) 2205–2224.

[10] S.A. Jilani, C. Koner, S Nandi, Security in wireless sensor networks: attacks and evasion, in: National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), 2020, pp. 1–5.

[11] R. Verma, S. Bharti, A survey of network attacks in wireless sensor networks, in: Information, Communication and Computing Technology, 2020, pp. 50–63.

[12] A. Karakaya, S. Akleylek, A survey on security threats and authentication approaches in wireless sensor networks, 6th International Symposium on Digital Forensic and Security(ISDFS), 2018.

[13] S. Sharma, A. Yadav, M. Panchal, P.D. Vyavahare, Classification of security attacks in WSNs and possible countermeasures: a survey, IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2019.

[14] R. Verma, S.J. Darak, V. Tikkiwal, H. Joshi, R Kumar, Countermeasures against jamming attack in sensor networks with timing and power constraints, 11th International Conference on Communication Systems & Networks (COMSNETS), 2019.

[15] S.J. Ee, J.W. Tien Ming, J.S. Yap, S.C.Y. Lee, F. tuz Zahra, "Active and passive security attacks in wireless networks and prevention techniques", 2020.

[16] L. Shi, Q. Liu, J. Shao, Y. Cheng, Distributed localization in wireless sensor networks under denial-of-service attacks, IEEE Control Syst. Lett. 5 (2) (2021) 493–498.

[17] A. Raoof, A. Matrawy, C. Lung, Routing attacks and mitigation methods for RPL-based Internet of Things, IEEE Commun. Surv. Tutor. 21 (2019) 1582–1606.

[18] Au Rehman, S.U. Rehman, H Raheem, Sinkhole attacks in wireless sensor networks: a survey, Wireless Pers Commun 106 (2019) 2291–2313.

[19] S. Choudhary, N Kesswani, Detection and prevention of routing attacks in the Internet of Things, in: 17th IEEE International Conference on Trust, Security and Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 1537–1540.

[20] S.A. Jilani, C. Koner, S Nandi, Security in wireless sensor networks: attacks and evasion, National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), 2020.

[21] D. Giri, S. Borah, R. Pradhan, "Approaches and measures to detect wormhole attack in wireless sensor networks: a survey", 2018.

[22] R.K. Gill, M. Sachdeva, Detection of hello flood attack on LEACH in wireless sensor networks, in: D. Lobiyal, V. Mansotra, U. Singh (Eds.), Next-Generation Networks. Advances in Intelligent Systems and Computing, 638, Springer, Singapore, 2018.

[23] P. Sinha, V.K. Jha, A.K. Rai, B. Bhushan, Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: a survey, International Conference on Signal Processing and Communication (ICSPC), 2017.

[24] D. Bharti, N. Nainta, H. Monga, Performance analysis of wireless sensor networks under adverse scenario of attack, in: 6th International Conference on Signal Processing and Integrated Networks (SPIN), 2019, pp. 826–828.

[25] D.-J. Huang, W.-C Teng, A defense against clock skew replication attacks in wireless sensor networks, J. Netw. Comput. Appl. (2014) 26–37.

[26] M.K. Sharma, B.K. Joshi, Detection & prevention of vampire attack in wireless sensor networks, in: International Conference on Information, Communication, Instrumentation and Control (ICICIC), 2017, pp. 1–5.

[27] M.N. Riaz, A. Buriro, A. Mahboob, Classification of attacks on wireless sensor networks: a survey, Int. J. Wirel. Microw. Technol. (IJWMT) 8 (6) (2018) 15–39.