ISSN: 2321-6840

Security Issues in Wireless Sensor Network

Moirangthem Marjit Singh[1] and Nishigandha Dutta[2]
[1]Assistant Professor, Department of Computer Science & Engineering, North Eastern Regional Institute of Science & Technology, Deemed University under MHRD Govt. of India, Nirjuli, Arunachal Pradesh, India.
Email: marjitm@gmail.com
[2]PG Student, M.Tech., Information Technology, Department of Computer Science & Engineering, North Eastern Regional Institute of Science & Technology, Deemed University under MHRD Govt. of India, Nirjuli, Arunachal Pradesh, India. Email: nishidtt9@gmail.com

Abstract: The sensor nodes in a wireless sensor network are scattered in an area so as to sense, process and transmit information in an environment. Due to several factors such as the range of radio transmission in the network, skeptical communication and abandoned nature of sensor nodes as well as easy access to the network, wireless sensor network is prone to numerous security threats. In this paper, we will highlight various security attacks and their effect on the wireless sensor network. Furthermore these security attacks are classified into several categories as well as the mechanisms to detect and prevent these attacks are also discussed.

Keywords: Wireless sensor network, Security attacks

I. Introduction

A wireless sensor network can be termed as a set of transducers possessing specialized properties and a communication infrastructure that intends to oversee and record environmental conditions at various locations. Some of the most common parameters observed in a wireless sensor network are temperature, humidity, pressure, pollutant level, wind direction and speed, sound intensity, illumination intensity, vibration intensity, power-line voltage, chemical concentration and vital body functions. As the wireless sensor network is categorized as a part of wireless personal area network and the sensor network parameters (temperature, humidity etc.) have signals of low frequency components with low data rate and small range, the technology employed is a low power and low data rate technology. This standard is specifically designed for this kind of application. The applications in a wireless sensor network make use of a sensor as source for generating the data/ information.

II. Wireless Sensor Network

The composition of a wireless sensor network basically consists of a large number of multifunctional devices or sensor nodes which are of low cost and low power. They are scattered in an ad hoc manner over a geographical area without proper planning. The main components of the network are:

A. Sensor Nodes

A sensor is a device that can detect and process some form of input from the environment and processes an output in the form of electrical signal transmitted to a controller for further processing. Microcontroller, radio transceiver, power supply and sensors are the fundamental components of a sensor node.

B. Base Station

The base station can be considered as a fundamental item of the wireless sensor network possessing larger memory and more computational power than the sensor nodes. The objective of the base station is to gather sensed data, visualize and analyze it and then finally forward the collected data to a remote server application [14].

C. Gateway

The gateway is the device that retrieves data from sensor nodes, monitor and configure a wireless sensor network remotely. It acts as a network coordinator and provides a link between the wireless sensor network and other network.

D. Patch Network

In Figure 1, sensor nodes are spread out in two different regions. Each region known as the patch network is equipped with a gateway for communication to other networks.

E. Transit Network

It is the intermediate communication channel through which signals are forwarded to the base station.

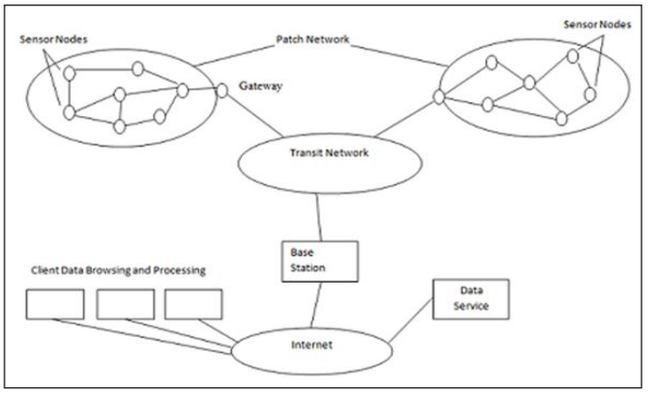

Fig. 1: A Schematic Diagram of Wireless Sensor Network

III. Security in Wireless Sensor Networks

Securing the wireless sensor network with the use of proper techniques is quite essential as the network is being set up in domains that involve sensitive information. The unattended operation, physical accessibility of the sensor devices and unreliable communication make these networks more prone to intrusions and attacks. Furthermore the limitation of resources makes the implementation of security mechanisms more complex than traditional networks. Thus there is a need to develop a secure system to achieve secrecy of credentials, operation safety and privacy of people in the sensor environment while maintaining desirable network performance [17]. For developing a secure system a wireless sensor network must satisfy several security requirements, called as security goals, during the design of the security protocol. These requirements are categorized as primary and secondary goals and are discussed below:

A. Primary/Standard Security Goals

- *Confidentiality:* An essential step in securing sensor network is to construct a secure channel in order to maintain the privacy of data as the sensor nodes may carry highly sensitive data [1]. Confidentiality refers to the ability to restrict the message for access only to authorized users and hide it from possible attacks, thus bounding the data access [19].
- *Integrity:* Integrity can be defined as the ability to ensure that the data and the resources are trustworthy. Data integrity ensures that the data received at the destination is same as the data sent by the source. Source integrity validates the sender as a trusted source [3][19].
- *Authentication:* Authentication is the process of identifying the user as an authorized one so that data access to illegitimate users can be denied. By identifying the source, authentication guarantees reliability of data so as to facilitate limited resource allocation to the sensor nodes and communicate sensitive information between authenticated nodes [5].
- *Availability:* The availability of the sensor nodes so as to provide resource services to the network is an essential security requirement to maintain an operational network. Since the nodes should be available whenever required, therefore node availability is ensured by protecting them from unnecessary processing and idle listening so as to save their energy [6] [7].

B. Secondary Security Goals

- *Data Freshness:* During network design when shared key strategy is used, it is essential to ensure freshness of data. This indicates that the security protocols should detect and discard duplicate messages and verify that the data and information retrieved by the sensor nodes are recent and up-to-date [1][3]. The freshness of data prevents the network from attacks such as replay attacks and select-and-forwarding attack [4].
- *Time Synchronization:* Time synchronization mechanisms are important for various applications that uses wireless sensor network. There are two modes available in the sensor nodes so as to save energy by switching off the sensor's radio and putting it to sleep. Moreover, as a packet travels from one sensor to another, the end-to-end delay of that packet is evaluated by the sensor node. Group synchronization is another aspect required by sensor networks performing collaborative tasks so as to track the applications [5][7].
- *Self Organization:* A massive number of independent sensor nodes are deployed over several geographical locations without any infrastructure. These nodes should have the capability of being self organized and to be self healing so that it can adapt to the topology and deployment strategy employed by the network, by themselves [1][2].
- *Secure Localization:* The sensor network should be designed with the ability to sense and resolve faults in the network by securely, accurately and automatically finding out faults in each sensor node [5]. These faults can be located by using accurate information from the network design. A non-secure network can easily fall prey to an attacker who can then manipulate the network by reporting false signal strengths and replaying old messages.

IV. Security Attacks Classification

A. Active vs. Passive Attacks

Based on the interruption during communication process of a wireless sensor network, security attacks are categorized into two types: active and passive attack.

- *Active Attacks:* During active attack, an attacker takes control of the network by implementing appropriate measures, for example: introduction of compromised nodes, modification as well as fabrication of messages, interruption of information etc. An active attack leads to obstruction of the secure and reliable communication channel thereby disrupting the normal functionality of the network.
- *Passive Attack:* A passive attack can be defined as a lay out for an attacker to successfully execute an active attack. In this context, a passive attack doesn't actually disrupt the communication of the network but silently monitors the traffic and listens for sensitive information. A passive attack is thus a violation of data confidentiality and is not easily detected due to its ability of being silent [1][3][22].

B. External vs. Internal Attack

Based on the location of the attacker, the sensor nodes can be attacked either by staying inside or outside the wireless sensor network.

- *External Attack:* The nodes that do not belong to the sensor network are responsible for external attack so as to limit the network resources by injecting bogus packets. Although the attacker doesn't have access to most of the cryptographic materials in the network, it still leads to passive eavesdropping and cause denial of service attacks.
- *Internal Attack:* The nodes belonging to the network are responsible for internal attack. The malicious nodes pretends to be a participating node and thus gains access to sensitive information. Internal attack causes severe damage to the network by sending false request and consuming energy of other sensor nodes. Furthermore it leads to eavesdropping, misrouting, modification and packet drop and also is hard to detect [4][8][20].

C. Mote Class vs. Laptop Class

The internal nodes in a network having same capabilities are used by an attacker to carry out mote class attack. However to have a wider impact, more powerful devices such as laptops are chosen in laptop class attack which have greater battery and processing power and high radio range. It can eavesdrop and corrupt the entire network and also affect the radio frequency and bandwidth of the communication channel [4][5][8].

D. Host Based vs. Network Based Attacks

Classification of host based attacks consists of three types: user compromise, hardware compromise and software compromise. The attacks that are carried out so as to reveal sensitive information about the network by compromising the users are known as user compromise attacks. To implement the attacker's program code to the compromised code, Hardware compromise attacks are done by tempering the hardware of the sensor node. Software compromise attacks are carried out to decipher the software running on the sensor nodes.

Network based attacks are launched to disrupt the layer oriented and protocol stack based functioning of the network. All attacks that tempers with information in transit are network based attacks [5][24].

E. Protocol Stack Based Attacks

The wireless sensor network architecture is based on the OSI layer model. This makes the network more vulnerable to different attacks that are carried out on different layers of the model. Physical layer attacks are hard to detect due to minimal physical control over the sensor nodes [1]. The attacker tries to decrypt and damage encrypted data thus disrupting the network service physically. The predefined behavior and cooperation of the link layer protocols are violated by the attacker in link layer attacks. Network layer attacks are launched by an attacker on the routing protocols to completely alter the routing information, control the network and disrupt the network traffic. In order to exhaust and limit the resources, an attacker in the transport layer continuously sends requests for new connection, thus constraining the resources for legitimate nodes. Attacks such as repudiation, malicious code and data corruption are carried out in the application layer to exhaust node energy and consume network bandwidth [6][22].

V. Attacks In WSN, Their Effects and Countermeasures

A. Blackhole Attack

Blackhole attack can be summarised as a denial of service attack where an intruder captures a sensor node and reprograms it so as to block packets from forwarding information to a base station and thus discarding sensitive information [12]. These attacks are easy to implement but very difficult to detect and defend.

- *Effects:* Since the network make decisions depending upon the nodes which are now unable to forward important information due to blackhole attack, thus they subsequently result in failure of the entire network [13]. Further blackhole attack leads to high end to end delay and low throughput of the sensor network.
- *Countermeasures*: Many techniques have been proposed in order to perceive and secure a network from blackhole attack. One such technique is the formation of clusters where a cluster coordinator senses the existence of an intruder in the network and removes the compromised node [11]. Another approach is to implement ActiveTrust scheme which resolve blackhole attack by using active detection routing [13].

B. Sybil Attack

The Sybil attack is an attempt of an intruder to forge multiple identities by fooling other sensor nodes to access data meant for them [3]. This attack takes place in the presence of a Sybil node which shows multiple identities to other sensor nodes either by framing or by abducting the identities of genuine nodes of the network [5].

- *Effects:* The Sybil attacks are a threat to geographic routing protocols and degrade the efficiency of fault tolerant systems by tempering with the data integrity, security and resource utilization of the sensor nodes [8]. It leads to miscommunication about the location of different nodes and packets are thus delivered to dummy nodes. By creating false routes during communication between sensor nodes, a Sybil attacker violates the routing algorithms and fairness of the network [1][7].
- *Countermeasures:* One simple way to defend the network from Sybil attack is to authenticate and encrypt sensitive information on each sensor node of the network. Another approach is to share a symmetric key that is unique for each node in the sensor network with the base station. Furthermore, proper authentication of each genuine node is essential to eliminate Sybil nodes from the network [3] [5][24].

C. Wormhole Attack

Wormhole attack can be classified as a network layer attack where an intruder make use of a link (wireless or wired) so as to receive a packet from one node positioned at one location in the network to another node located at a different location in the sensor network [26]. It requires at least two adversaries linked by a low latency wormhole link. Wormhole attack misleads distant nodes to be neighbors by forwarding routing messages.

- *Effects:* In wormhole attack, malicious nodes are able to send data between two legitimate nodes and have access to the information flowing between them. Also it creates a false scenario that two remote nodes are neighbors, thus effecting network routing by creating fake list of neighbors. This leads to rapid exhaustion of network resources [8][28].
- *Countermeasures:* Securing and authenticating the routing information doesn't always guarantee that the wormhole attack won't take place, therefore making this attack critical and hard to defend. An approach is to implement packet leashes which restrict sensor nodes from transmitting packets beyond a definite transmission range [9]. Network visualization is another mechanism used for preventing stationary sensor network from wormhole attack where a node calculates the distance to each of its neighbors by using signal strength [25]. Wormhole geographic distributed detection (WGDD) employs hop counting methods to detect disruptions created by wormhole attack [26].

D. Hello Flood Attack

An attack in the network layer, hello flood attack is an attempt to break the security by flooding legitimate nodes with hello request packets [29]. In this attack an intruder with high transmission power continuously broadcasts hello packets in order to misguide sensor nodes to think of the malicious node as its neighbor [31].

- *Effects:* Hello flood attack causes exhaustion in the network by spoofing legitimate nodes of the sensor network. Furthermore, since all messages being broadcasted are routed through the malicious node, hello flood attack increases delay and the network enters into a confusion state [1][30].
- *Countermeasures:* Hello flood attack can be detected with the inspection of signal strength of all the sensor nodes in the network since an intruder will have a node with high processing power. Mechanisms such as identity verification protocol technique and cryptographic security scheme can be used to prevent hello flood attack by generating encryption key and authenticating each and every node that claims to be a neighbor of that node [1].

E. Denial-of-Service (DOS) Attack

DOS attack is a common attack where an attacker tries to restrain the access to network services. The attacker swamps the network of the target node by flooding its communication link with continuous requests so as to deny services to legitimate clients [31][32].

- *Effects:* DOS attacks effects availability of a network by depriving legitimate users from accessing the network resources and exhausting them [1]. It leads to total distortion in the sensor network as DOS attack slower the network performance, consumes network resources, increase delay in packet transmission and block the communication path between two legitimate nodes [31].
- *Countermeasures:* By identifying and authenticating the traffic and resources in the network, DOS attack can be prevented [1]. Anti replay protocols are another way of preventing attackers from launching DOS attacks. Most of the mechanisms implemented to prevent these attacks are based on artificial intelligence, game theory, soft computing and multi agent approaches [32].

F. Sinkhole Attack

In a sinkhole attack, an attacker tries to pull all the nearby network traffic using a malicious node. With the compromised node at the centre, the attacker creates a sinkhole in the network so as to access and control all the information of the network.

- *Effects:* The malicious node in a sinkhole attack forges itself as a base station to prevent it from receiving and processing complete data from sensor nodes. Sinkhole

attack tempers the routing information and thus in turn corrupt data packets.

- *Countermeasures:* Sinkhole attack cannot be detected easily because of the difficulty in verifying the routing information being provided by the malicious node. Several schemes have been proposed to counter sinkhole attack. Some of them are data consistency and network flow information approach, RSSI (Received signal strength indicator) based scheme, hop counting and monitoring technique and mobile agent based approach [4][33][21].

G. Selective Forwarding/ Grayhole Attack

Selective forwarding (also known as grayhole attack) is somewhat similar to a blackhole attack where an unauthorized node acts as a blackhole and prevents further transmission of packets by selectively dropping them. It can be classified as a network layer attack where a malicious node include itself as the neighbor of certain legitimate nodes and isolates and prevent them from forwarding packets to the base station [23].

- *Effects:* Selective forwarding when combined with other attacks such as sinkhole and wormhole attack can disrupt the functioning of several cluster based and routing protocols [34]. It creates discontinuity in the network by isolating nodes from the base station and thus crippling the sensor network [23].
- *Countermeasures:* Selective forwarding is difficult to detect compared to blackhole attack. Detection process for selective forwarding attack includes constructing specialized systems such as intrusion detection systems. It can be countered by using techniques that uses neighbor nodes as monitor nodes and multihop forwarding and multihop acknowledgement techniques [34]

H. Jamming Attack

The attack caused by the interference of radio frequencies by an intruder to jam the sensor network with malicious packets is known as jamming attack. The attacker continuously transmits high energy signals into the network to keep the radio channels busy and consume the energy of sensor nodes.

- *Effects:* The intruder injects false packets into the channel which leads to consumption and exhaustion of energy of the nodes in the network. In the worst case scenario, a complete distortion of the normal functioning of the network will occur due to jamming attack. When nodes in the network are unable to transmit packets due to jamming in the channel, it leads to Denial of service attack.
- *Countermeasures:* To tackle with jamming attack, nodes must be put to sleep mode to avoid tempering of packets during communication. The defensive mechanisms deployed against jamming attack are spread spectrum techniques, use of hybrid FHSS-DSSS communication between nodes of the WSN and use of low transmitted power to minimize the detection possibility from an attacker [3][5][27].

I. Path Based DOS Attack

It is an application layer denial of service attack where an entire communication path is flooded with malicious packets that are injected or replayed into the sensor network [31]. This attack takes place at the leaf nodes of the network where the attacker floods the end-to-end transmission path between the nodes and the base station so as to overwhelm the sensor nodes.

- *Effects:* An attacker in path based DOS attack replays malicious packet to consume network resources and starve the traffic in the network. Also the attacker prevents the intermediate nodes from going to sleep mode and keeps them in active mode to exhaust their energy. It also prevents the sensor nodes from transmitting information to the base station [5].
- *Countermeasures:* One way to counter path based DOS attack is to reject the spurious packets injected by an adversary by successfully detecting them. Time efficient stream loss-tolerant authentication (TESLA) is a loosely time synchronized mechanism implemented to defend the network from path based DOS attack. Another way is to use a light weight secure technique that uses one-way hash chain. Furthermore, the combination of markov chain and triple exponential smoothing is another approach implemented to counter path based DOS attack [15].

J. Misdirection Attack

Misdirection attack is an active attack where an intruder transmits an incoming packet to a malicious node instead of the legitimate node expecting the packet. The attacker deprives the genuine users from network services and misleads the data information intended for them to illegitimate clients.

- *Effects:* Since the packets are deprived of reaching its destination, misdirection attack leads to delay and consequently decreased throughput in the sensor network. Furthermore, if the malicious node to which the attacker misdirects the packets is far away from the intended node, then the packets never reach their destination. This in turn will increase the network delay to infinity and will lead to zero throughput. Besides, this type of attack also decreases the lifetime of the network.
- *Countermeasures:* An effective way to detect and defend the sensor network from misdirection attack is to use cluster based technique where clusters are created to separate the malicious nodes from the network. Another way of countering this attack is to put the node that has been attacked into sleep mode [3][5].

K. Eavesdropping Attack

It is a passive attack where an adversary has the ability to perceive the contents of the communication between nodes of the network by overhearing them through a compromised channel. Thus in an eavesdropping attack, an attacker tries to accumulate sensitive information by prying into the sensor network in an illegal way.

- *Effects:* Eavesdropping attack is a threat to data confidentiality and exploits privacy of the sensor network. The attacker in this kind of attack performs eavesdropping activity to gain access to encrypted information which further leads to blackhole and wormhole attack [2].
- *Countermeasures:* One way to prevent intruder from launching eavesdropping attack is to use directional antennas for radio transmission instead of omnidirectional. This will significantly reduce the probability of eavesdropping attack [18].

L. Tempering Attack

Tempering is a physical layer attack where an attacker physically tempers with the sensor node and replace it with a malicious node. The wireless sensor network is highly prone to tempering attack as the sensor nodes are being scattered in an abandoned environment where an intruder extracts encrypted information such as cryptographic keys by capturing the node physically [7].

- *Effects:* Since an attacker is able to manipulate a node physically, therefore tempering attack is a threat to the integrity, confidentiality and availability of data in the sensor network. With the captured node, the adversaries can alter the node's program code, stop services and cause disturbance in the network.
- *Countermeasures:* The first step to tackle tempering attack is to implement physical security of the sensor nodes. Defensive mechanisms that can be used against tempering attack are temper proofing technique, optimization and use of crypto-processors and hiding of sensor nodes within some other objects [2][5].

M. Collision Attack

When two sensor nodes transmit packets concurrently over the same frequency channel, collision occurs. Due to this collision among the sensor nodes, data in the packets will get altered and this results in mismatch with the checksum being computed at the receiving end.

- *Effects:* The data packets transmitted during a collision attack becomes invalid and are thus discarded. Hence, retransmission is done which further leads to unnecessary consumption of energy and causes disruption in the network.
- *Countermeasures:* When the collision levels are low, error correcting codes are sufficient to counter collision attack. Besides, several techniques are present to defend collision attacks that are based on analyzing physical layer RSSI (Received Signal Strength Index) readings [3].

N. Routing Information Attack

This is a network layer attack where the intruder tempers the information contained in the routing protocols. This leads to misdirection of packets due to altering of the routing information and further loss of packets.

- *Effects:* As the attacker is able to spoof, alter and replay information contained in the routing protocols, there is an interruption in the traffic of the sensor network. The routing information attack creates routing loops, increases latency in the network, shorten or widen routing lengths and attract or repel network traffic. It further partitions the sensor network.
- *Countermeasures:* Proper authentication and encryption is necessary to defend the network from this type of attack. Another way is to transmit packets with a MAC (Message Authentication Code) appended to them [5].

O. Spoofing Attack

In order to advertise wrong information to neighboring nodes in a network, an attacker launches spoofing attack by spoofing themselves as another device or forges multiple illegitimate identities. This attack can be hazardous to the sensor network as it assists several traffic injection attacks such as evil twin access point attack. The attacker in a spoofing attack compromises the MAC address of a sensor node in order to forge themselves as another transmitter so as to appear as a different device to the sensor network.

- *Effects:* This type of masquerading attack can have adverse impact on the sensor network as it provides false routing information, create routing loops, degrades the network performance and exploits security weaknesses. The spoofing attack also facilitates denial of service attacks and attacks on access control mechanism.
- *Countermeasures:* The most common method of preventing this attack is to use proper authentication technique to encrypt the transmitted packets. RSS (Receive Signal Strength) can also be used to analyze and detect the presence of spoofing attack in the network [10].

P. Traffic Analysis Attack

Traffic analysis attack is typically combined with eavesdropping attack by an attacker to silently monitor and analyze the traffic

pattern in the network during communication between sensor nodes. Traffic analysis attacks are categorized into two classes. One is the rate monitoring attack where an attacker is able to identify as to where base station is located by assuming that sensor nodes having higher transmission rate are closer to the base station. Another is the time correlation attack where the intruder observes the correlation in time between two nodes that are neighbors and transmits the same packet. The intruder then follows the path taken by the nodes to forward the data packets to the base station so as to determine its geographic location.

- *Effects:* An attacker in a traffic analysis attack has the capability of tracking the base station and tempering with it, even when data packets are encrypted. The entire network can fail if the base station is damaged or destroyed by an attacker as it is the central hub of the network.
- *Countermeasures:* Anti-traffic analysis techniques such as multiple parent routing scheme, addition of controlled random walk and random fake paths and creation of multiple, random areas of communication activities can be deployed to hide the base stations and misdirect the adversaries [16].

Q. De-synchronization Attack

An attacker disrupts a transmission ongoing between two nodes by injecting malicious packets in the de-synchronization attack. The malicious packets contain bogus information and control flags that de-synchronize the end points to facilitate retransmission of packets.

- *Effects:* The retransmission of packets due to de-synchronization of end points prevents the sensor nodes from exchanging any information and leads to wastage of energy. This affects the end to end packet delivery of nodes.
- *Countermeasures:* One way to defend the sensor nodes from de-synchronization attack is to authenticate each packet being transmitted, including all control fields. Header or full packet authentication can effectively counter this attack [5].

R. Exhaustion Attack

Exhaustion is a data link layer attack where an attacker interrupts the communication channel and creates confusion in the network by constantly asking queries and transmitting irrelevant information over it. The intruder takes control of the channel and blocks genuine users from forwarding packets.

- *Effects:* The intruder in an exhaustion attack prevents transmission of data packets by occupying the channel continuously, thus leading to starvation in the network. Also while serving the unwanted malicious packets; the energy of the sensor nodes gets exhausted.
- *Countermeasures:* A method to prevent exhaustion attack is to use time division multiplexing. Detection of this attack is done through misbehavior detection technique [3][5].

Various forms of attacks encountered in wireless sensor network are summarized in Table 1, along with the effects and countermeasures to deal with these attacks.

TABLE I: VARIOUS ATTACKS ENCOUNTERED IN WIRELESS SENSOR NETWORK

Name of the attack	Attack classification	Effects on WSN	Countermeasures
Blackhole	• Active attack • Internal attack • Network layer attack	• Blocks data transmission • Low throughput • High end-to-end delay	• Cluster-based techniques • ActiveTrust scheme
Sybil	• Active attack • Both internal and external attack • Network layer attack	• Forges multiple identities • Create false routes • Degrade fault tolerant systems	• Radio resource testing technique • Proper authentication & encryption • Use of public key cryptography
Wormhole	• Active attack • Network layer attack	• Changes network topology • Exhaust network resources • Triggers blackhole, sinkhole & selective forwarding attack	• Packet leashes • Network visualization • Wormhole geographic distributed detection (WGDD) technique
Hello flood	• Active attack • Network layer attack • Laptop class attack	• Exhaust resources • Congestion of data • Increases delay • Creates network confusion	• Cryptographic & non-cryptographic techniques • Identity verification protocol technique • Inspection of signal strength of sensor nodes

Denial of service	• Active attack • External attack • Multi-layer attack	• Consume resources • Slows network performance • High delay in data transmission • Blocks communication path	• Use of anti-replay protocols • Identification & Authentication of traffic and network resources • Pushback techniques
Sinkhole	• Active attack • Network layer attack • Internal attack • Laptop class attack	• Attracts all traffic in the network • Create false routing information • Corrupt data packets	• RSSI (received signal strength indicator) scheme • Hybrid based intrusion detection technique • Key management • Use of geographic routing protocols
Selective forwarding	• Active attack • Network layer attack • Internal attack • Mote class attack	• Selectively drops data packets • Isolates nodes from base station • Creates discontinuity in sensor network • Information loss	• Data transmission through multiple paths • Multi-hop acknowledgement based detection technique • Intrusion detection technique using support vector machines
Jamming	• Active attack • Physical layer attack	• Consume & exhaust energy of nodes. • Causes DOS attack • Collision of sensor nodes	• Non-adaptive group testing • Clique-independent set technique • Channel surfing • Spatial retreats
Path based DOS	• Active attack • Application layer attack	• Starve network traffic • Consume network resources • Blocks transmission to base station	• Time efficient stream loss-tolerant authentication (TESLA) technique • Light weight secure techniques using one way hash chain
Misdirection	• Active attack	• Misdirection of packets • Delay and decreased throughput • Decreases network lifetime	• Use of Enhanced LEACH protocol • Third party monitoring • Cluster based intrusion detection technique
Eavesdropping	• Passive attack • Physical layer attack • External attack	• Exploits confidentiality & privacy • Leads to wormhole & blackhole attack	• Use of directional antennas
Tampering	• Active attack • Physical layer attack	• Data manipulation • Creates congestion • Exploits integrity, availability & confidentiality	• Temper proofing techniques • Physical security • Optimization and use of crypto-processors
Collision	• Active attack • Data link layer attack	• Change in packet contents • Unnecessary energy consumption	• Use of error correction codes • Received signal strength index (RSSI) readings analysis
Routing information	• Active attack • Network layer attack	• Alteration of information in routing protocols • Misdirection of packets • Traffic interruption	• Monitoring • Egress filtering • Use of Message Authentication code (MAC)
Spoofing	• Active attack • Network layer attack	• Creates false routing information • Degrades network performance • Creates routing loops	• Proper authentication • Receive signal strength (RSS) analysis
Traffic analysis	• Passive attack • Data link layer attack	• Track & corrupt base station • Render network useless by destroying base station	• Anti traffic analysis techniques

De-synchronization	• Active attack • Transport layer attack	• Retransmission of packets • Network energy wastage • Unreliable data delivery	• Header or full packet authentication
Exhaustion	• Active attack • Data link layer attack • External attack	• Interruption & confusion in the channel Exhaustion of power	• Rate limitation • Time division multiplexing

VI. Conclusion

The growth of wireless sensor network in the recent years has paced remarkably, garnering significant attention towards making it more reliable, secure and efficient. Because of the constraints surfacing the sensor network, the security needs to be upgraded to make it less vulnerable to attacks and to successfully accommodate the diverse applications that the wireless sensor network is capable of. In this paper, wireless sensor network is briefly discussed followed by the security fundamentals of the network. Further, the various WSN attacks, along with their effects and defensive mechanisms has been explored to understand them better and to defend them effectively. Although several research has been done to counter security attacks; still, providing a secure sensor network remains a challenge. Thus with increasing vulnerabilities towards entities of the sensor network, new and robust mechanisms are needed to prevent them efficiently.

References

[1] U. Sharma, and N. Bahl, "A review on security issues and attacks in wireless sensor network," *International Journal of Advanced Research in Computer Science,* vol. 8, no. 4, pp. 387-391, May 2017.

[2] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, and K. N. Qureshi, "Security issues and attacks in wireless sensor network," *World Applied Sciences Journal,* vol. 30, no. 10, pp. 1224-1227, 2014.

[3] H. Chawla, H. Kaur, and C. Kaur, "Review on security issues in wireless sensor networks," *International Journal of Current Engineering and Technology,* vol. 6, no. 3, pp. 942-948, June 2016.

[4] A. Singh, and K. Gupta, "Review of security issues in mobile wireless sensor networks," *Int. J. Advanced Networking and Applications,*vol. 7, no. 5, pp. 2887-2892, 2016.

[5] Pooja, and R. K. Chauhan, "Review on security attacks and countermeasures in wireless sensor networks," *International Journal of Advanced Research in Computer Science,* vol. 8, no. 5, pp. 1275-1283, May-June 2017.

[6] K. Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," *Proceedings of the World Congress on Engineering,* vol. 1, WCE, London, U.K., July 1-3, 2015.

[7] L. Kaur, and J. Malhotra, "Review on security issues and attacks in wireless sensor networks," *International Journal of Future Generation Communication and Networking,* vol. 8, no. 4, pp. 81-88, 2015.

[8] S. K. Singh, M. P. Singh, and D. K. Singh, "A survey on network security and attack defense mechanism for wireless sensor networks," *International Journal of Computer Trends and Technology,* vol. 1, no. 2, pp. 131-139, May to June Issue, 2011.

[9] P. Maidamwar, and N. Chavhan, "A survey on security issues to detect wormhole attack in wireless sensor network," *International Journal on AdHoc Networking Systems (IJANS),* vol. 2, no. 4, pp. 37-50, Oct. 2012.

[10] V. B. Srinivas, and S. Umar, "Spoofing attacks in wireless sensor networks," *IJCSET,* vol. 3, no. 6, pp. 201-210, June 2013

[11] M. Wazid, A. Katal, R. S. Sachan, R. H. Goudar, and D. P. Singh, "Detection and prevention mechanism for black-hole attack in wireless sensor network," *International Conference on Communication and Signal Processing*, pp. 576-581, April 3-5, 2013.

[12] B. K. Mishra, M. C. Nikam, and P. Lakkadwala, "Security against black hole attack in wireless sensor network: A review," *Fourth International Conference on Communication Systems and Network Technologies,* pp. 615-620, 2014.

[13] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Transactions on Information Forensics and Security,* vol. 11, no. 9, pp. 2013-2027, September 2016.

[14] M. Michal´ık, "Base station for wireless sensor network," Diploma Thesis, Masarykova Univerzita, Fakulta Informatiky, autumn 2013.

[15] K. S. Yadav, and M. Tamboli, "Defending against path-based denial of service attack in wireless sensor network," *International Conference on Examination in Modern Technology and Engineering (ICEMTE*), vol. 5, no. 3, pp. 46-51, 2017.

[16] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor net-

works," Computer Science Department, University of Colorado at Boulder, Colorado, USA.

[17] S. Hadim, and N. Mohamed, "Middleware: Middleware challenges and approaches for wireless sensor networks," *IEEE Distributed Systems Online,* vol. 7, no. 3, March 2006, art. no. 0603-o3001.

[18] H.-N. Dai, Q. Wang, D. Li, and Raymond Chi-Wing Wong, "On eavesdropping attacks in wireless sensor networks with directional antennas," *International Journal of Distributed Sensor Networks,* vol. 9, no. 8, 2013.

[19] C. D. Devi, and B. Santhi, "Study on security protocols in wireless sensor networks," *International Journal of Engineering and Technology (IJET),* vol. 5, no. 1, pp. 200-207, Feb-March 2013.

[20] K. Shabana, N. Fida, F. Khan, S. R. Jan, and M. U. Rehman, "Security issues and attacks in wireless sensor networks," *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE),* vol. 5, no. 7, pp. 81-87, July 2016.

[21] V. Soni, P. Modi, and V. Chaudhri, "Detecting sinkhole attack in wireless sensor network," *International Journal of Application or Innovation in Engineering & Management (IJAIEM),* vol. 2, no. 2, pp. 29-32, Feb. 2013.

[22] T.-G. Lupu, "Main types of attacks in wireless sensor networks," *9th WSEAS International Conference on Signal, Speech and Image Processing, and 9th WSEAS International Conference on Multimedia, Internet & Video Technologies,* pp. 180-185, Budapest, Hungary, 2009.

[23] S. Kaplantzis, A. Shilton, N. Mani, and Y. Ahmet S¸ekercio˘glu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," *Electrical and Computer Systems Engineering,* pp. 335-340, Monash University Clayton, Victoria 3800, Australia.

[24] G. Singh, "Security attacks and defense mechanisms in Wireless sensor network: A survey," *IJISET - International Journal of Innovative Science, Engineering & Technology,* vol. 3 Issue 4, pp. 129-136, April 2016.

[25] R. Shree, and R. A. Khan, "Wormhole attack in wireless sensor network," *International Journal of Computer Networks and Communications Security,* vol. 2, no.1, pp. 22-26, Jan. 2014.

[26] Y. Xu, G. Chen, J. Ford, and F. Makedon, "Detecting wormhole attacks in wireless sensor networks published in critical infrastructure protection," Edited by E. Goetz and S. Shenoi, *International Federation for Information Processing, a Springer Series in Computer Science,* pp. 267-279, 2008.

[27] A. Mpitziopoulos, D. Gavalas, and G. Pantziou, "Defending wireless sensor networks from jamming attacks," *The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07),* Athens, Greece, 2007.

[28] M. Bendjima, and M. Feham, "Wormhole attack detection in wireless sensor networks," *SAI Computing Conference,* July 13-15, London, UK, 2016.

[29] R. Singh, J. Singh, and. R. Singh, "Hello flood attack countermeasures in wireless sensor networks," *International Journal of Computer Science and Mobile Applications,* vol. 4, no. 5, pp. 1-9, May 2016.

[30] A. Dubey, D. Meena, and S. Gaur, "A survey in hello flood attack in wireless sensor networks," *International Journal of Engineering Research & Technology (IJERT),* vol. 3, no. 1, pp. 1882-1887, Jan. 2014

[31] D. Buch, and D. C. Jinwala, "Denial of service attacks in wireless sensor networks," *International Conference on Current Trends in Technology,* Nuicone, December 2010.

[32] S. Patil, and S. Chaudhari, "Dos attack prevention technique in wireless sensor networks," *7th International Conference on Communication, Computing and Virtualization,* vol. 79, pp. 715-721, 2016, Mumbai, India.

[33] G. W. Kibirige, and C. Sanga, "A survey on detection of sinkhole attack in wireless sensor network," *Department of Informatics,* vol. 13, no. 5, pp. 1-9, May 2015.

[34] B. Yu, and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," *20th International Conference on Parallel and Distributed Processing,* Rhodes Island, Greece, 2006.