Wireless Sensor Networks: Architecture, Topologies, Security Attacks and Techniques

Ms. Simran Uppal
Student
Apeejay College of Fine Arts, Jalandhar, India
Email-id: simranuppal6991@gmail.com

Ms. Rekha
Assistant Professor
Apeejay College of Fine Arts, Jalandhar, India
Email-id: rekha_dalia@yahoo.com

Abstract

The gradual advancement in wireless sensor networks is increasingly motivating organizations to have its potential benefits. A wireless sensor is a device that perceives any information about a real-world physical system, store it, and respond accordingly. A wireless sensor network (WSN) consists of multiple wireless sensors grouped to perform a devoted task of receiving and transmitting information of a physical environment, which is of minimal use if there is no knowledge of where it resides. This paper discusses the network architecture and various topologies used in a wireless sensor network. Furthermore, it explains security issues and techniques related to wireless sensor networks. Security is a crucial aspect to consider when it comes to wireless sensor networks. Several attacks can occur in these environments, which are extremely important to look after. Various security techniques are applied to rectify the possible threats that a wireless sensor network (WSN) can usually go through.

Keywords- *sensor network, network architecture, topology, security, techniques.*

I. Introduction

A wireless sensor network (WSN) consists of multiple wireless sensors grouped to perform a devoted task of receiving and transmitting information of a physical environment, which is of minimal use if there is no knowledge of where it resides. The multiple wireless sensors present in a wireless sensor network are known as sensor nodes, which perform a threefold task - computation, communication, and sensing[1].

The arrangement of the sensor nodes in a wireless sensor network decides the appearance of the network architecture. The architecture can be either single-hop or multiple-hop, the latter being further two types, flat-network, and hierarchical-network architecture. The orientation of the sensor nodes is called the network topology, which is of multiple types. There are around five network topologies present, of which only four are preferable for a wireless sensor network architecture, that are, star, mesh, tree, and clustered hierarchical architecture[4].

Gateway is a device used to connect two distinct networks, particularly a connection to the internet. This gateway collects the information from the sensor nodes in the respective topology, which is then forward to a root node(base station) termed sink[2]. The goal of a wireless sensor network is to be alive and serviceable[2]. The sensor nodes in the network significantly perform the task of receiving the data collected from the physical system and transmitting it to the final destination, which stores the arguments and displays them to the end-users in a network[3]. Also, coordinator nodes manage the sub wireless sensor networks of a wireless sensor network[5]. Wireless sensor networks are a novel kind of system, having restricted resources and spontaneous or impromptu construction[7].

Security is a crucial aspect to consider when it comes to wireless sensor networks. Several attacks can occur in these environments, which are extremely important to look after. For a wireless sensor network to be secure and safe, security is included in it[7]. The network has a threat of attacks from inside and outside of the network. The outsider attackers have no access to the sensor networks, and the insider attackers are among the authorized members of the sensor network[8]. Another way of dividing these attackers is mote-class attackers and laptop-class attackers. The former has access to a few sensor nodes having equal capabilities to the original, and the latter can have ingress to more powerful electronic devices[8].

Various security techniques are applied to rectify the possible threats that a wireless sensor network (WSN) can usually go through. The objective of the services provided by the security is to guard the data and resources against attackers[9]. There are seven security requirements in a wireless sensor network, viz. availability, authorization, authentication, confidentiality, integrity, nonrepudiation, and freshness[9]. The preferable security methods include encryption, which is of two types, viz. symmetric and asymmetric encryption, and cryptography[8]. Encryption is a process that rectifies unauthorized access by converting the transmitted information into a code termed encoding. The initial data that is

traveling across a path is referred to as plaintext. The encrypted data, on the other hand, is termed ciphertext. In this process, the generation of a key known as a pseudo-random encryption key occurs.

Contemporary encryption techniques use two types of keys - the public key and the symmetric key. With an increase in computer power, encryption is advancing continuously to curb security attacks. Encryption secures a network against eavesdropping[8]. In symmetric, both the sender and the receiver use a shared key, which refers to a sole secret key[8]. In asymmetric, however, two keys are used, named a public key and a private key. The data encrypted through a public key is made into plain text again through the corresponding private key[8]. Lastly, cryptography is nothing but the combination of encryption(encoding) and decryption(decoding). When this method is employed in wireless sensor networks, it must meet the sensor node constraints and be evaluated by data size, time of processing, and the length of the code[8].

II. Wireless Sensor Network Architecture

Several sensor nodes are combined to manage a real-life system. A sensor node communicates with its peer sensor nodes. This interaction is performed with the help of wireless transceivers[10]. The region where all the sensor nodes exist is the sensing region as shown in Fig. 1. This region is connected with a base station, whose task is to send commands to the nodes so that they can perform the tasks given to them with collaboration. This data is then transmitted to a leader node or to a base station termed as sink[2]. It sends the processed data to the end-user with the help of the internet, hence acting as a gateway.

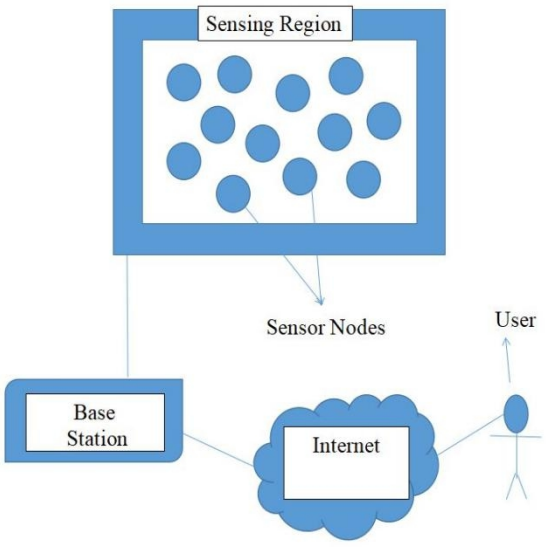

Fig. 1 Wireless sensor network general architecture

The wireless sensor network can be arranged in many ways depending upon the application in which it will orient itself. The connection of the sensor nodes in the sensing region with the base station can vary, which results in different kinds of arrangements of network architecture.

There are two basic types of wireless sensor network architectures. The first one being a single-hop network architecture, and the second one is multiple-hop network architecture as shown in Fig. 2. The latter one is further sub-divided into two types of networks, viz. flat-network and hierarchical-network architecture.

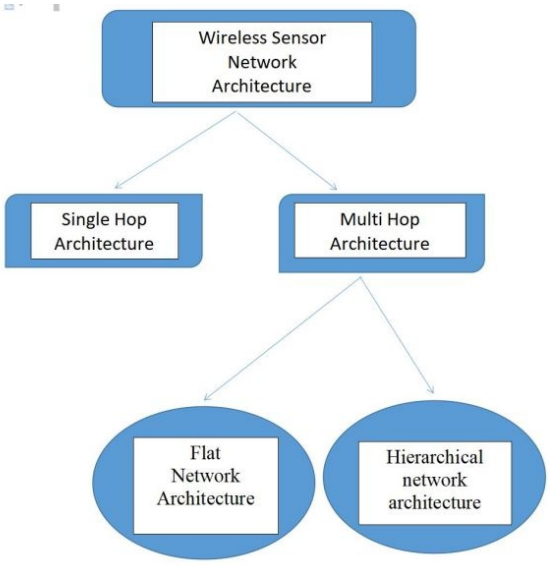

Fig. 2 Wireless sensor network architecture types

Single-hop Architecture

In this type of architecture, each sensor node in the sensing region is connected individually to the base station as shown in Fig.3. This results in higher consumption of energy but an efficient gathering of information and computing.

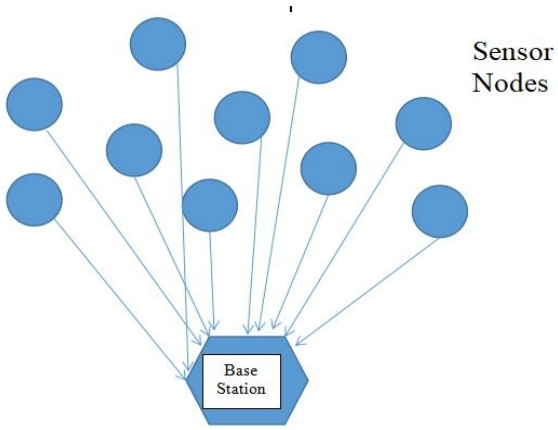

Fig. 3 Single-hop network architecture

The data packet only undergoes a single-hop while its transmission to the final destination. A single networking device is needed in order to route the packet from the sender to the receiver. As a result, the network traffic is the least and hence the total cost also becomes lower as compared to other wireless sensor network architectures. Secondly, less energy is consumed in this type of architecture. Energy consumption is a crucial apprehension in wireless sensor networks[1].

Multi-hop Architecture

The most preferred network architecture in wireless sensor networks is a multi-hop network architecture. As the name suggests, it comprises multiple links between the sensor node and the base station as shown in Fig. 4.

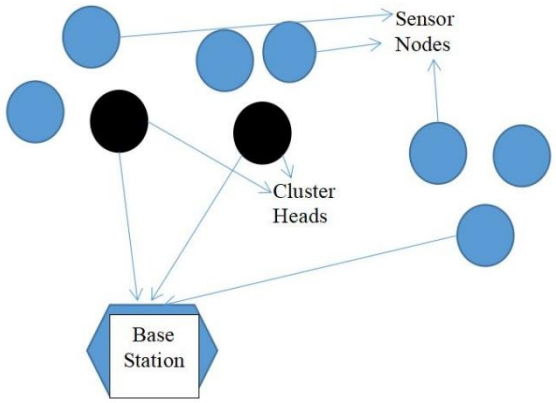

Fig. 4 Multi-hop network architecture

A.Flat-Network Architecture

This is a sub-type of multi-hop wireless sensor network architecture. In this architecture, the sensor nodes present in the sensing region are connected with their peer sensor nodes. They do not necessarily communicate with the base station directly as shown in Fig. 5. They take or give assistance to the sensor nodes present in the vicinity to pass the data to the basestation.

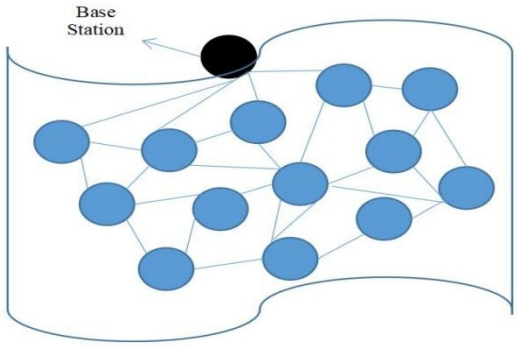

Fig. 5 Flat-network multi-hop architecture

B.Hierarchical-Network Architecture

In this architecture, the base station is not connected with every sensor node out there in the sensing region. A group of these nodes forms a cluster and one sensor node in each group is assigned the task of being a cluster head. These cluster heads receive the data or information from the other sensor nodes of the cluster and send it to the base station. Therefore, the base station is only connected with all the cluster heads of the clusters as shown in Fig. 6.

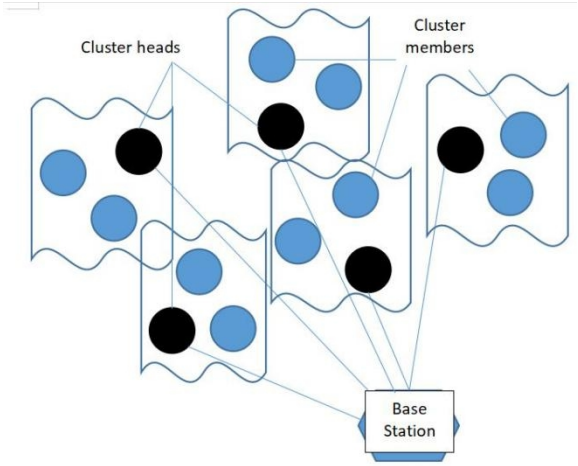

Fig. 6 Hierarchical-network multi-hop architecture

It follows a tree pattern. The root node in this hierarchy is the base station itself. Besides, the clusters in this architecture can be acknowledged as the branches of a tree. The group of all the clusters forms the crown of this architecture.

There are many factors that decide how complex the design of a wireless sensor network should be. Particular application requirements like count of sensor nodes, power consumption, sensor life span, data to be sensed, time duration, location and position of the sensors, the environment, and the context, are significant in the formation of a wireless sensor network architecture[2]. If a lesser number of sensor nodes are required, then single-hop architecture can be designed. On the other hand, if a larger number of sensor nodes are required, then more complex architectures should be designed. A number of options should be discussed in the planning phase of designing a wireless sensor network architecture. The position and geographical location of the nodes should also be considered.

III. Topologies in wireless sensor networks

Majorly, in the application areas of a wireless sensor network, the orientation of the sensor nodes is random and are stimulated to be efficient in their work[3]. This arrangement or layout is the network topology of a wireless sensor network. The network topology affects many performance criteria, such as network orientation, reliability, scalability, self-configuration, energy efficiency, the lifespan of a network, latency, etc[4]. The wireless sensor network topology is continuously constrained to a dynamic modification; it is not a solution to enhance the architecture by adding new sensors[3]. There are four common kinds of topologies in WSN as shown in Fig. 7. The sensor nodes that are mobile in nature, assist in deployment and repairing networks by moving to suitable positions inside the orientation to reach a destined stage of coverage and connectivity, and to attach a probably disconnected network arrangement[11].

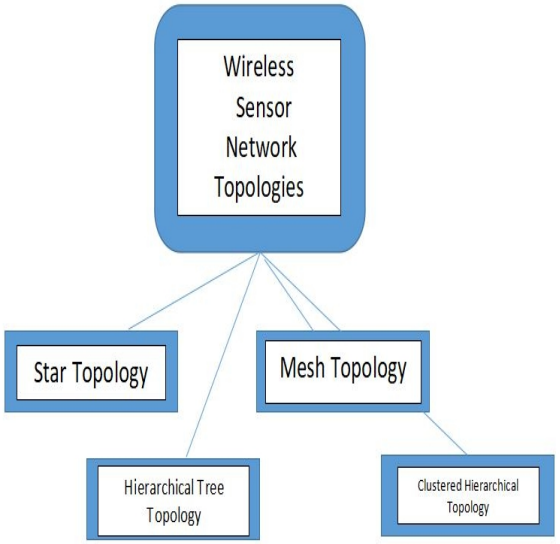

Fig. 7 Wireless sensor network topologies

Star Topology

In star topology, as the name suggests, all the sensor nodes are connected to an isolated hub or sink node in the center[3]. The transmission of the data packets is done explicitly between the sender and the receiver nodes, therefore, any sensor node's data does not need to hop to another node to reach the destination[3]. The central hub or sink can either be the base station or a gateway node that is directly connected with the base station[4] as shown in Fig. 8. This kind of arrangement of the sensor nodes and the gateway or base station is best suited for the application areas where a lesser number of sensor nodes are required.

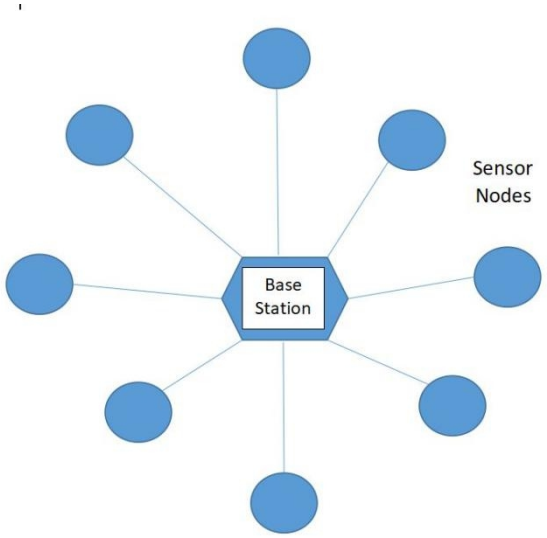

Fig. 8 Star topology

Mesh Topology

Wireless sensor networks with mesh topology have more number of connections than in star topology. The sensor nodes present in this orientation are connected to the peer or neighboring sensor nodes. In addition to this, the adjoining nodes of the base station are connected to the base station as well as shown in Fig. 9. In this way, the sensor nodes not only sends and receives their personal data but also play the role of a router by transmitting or forwarding the message packets of their neighboring nodes to the base station[4].

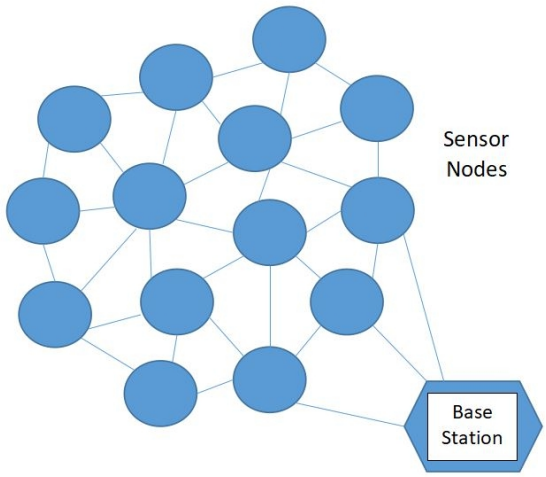

Fig. 9 Mesh topology

Hierarchical Tree Topology

In this arrangement of the sensor nodes and base station, there are multiple levels at which the same topology is followed. In the figure given below, notice that each of the three levels follows star topology[4]. Each level has a cluster head as the central hub of that cluster to which all other ordinary sensor nodes are connected in a star fashion as shown in Fig. 10.

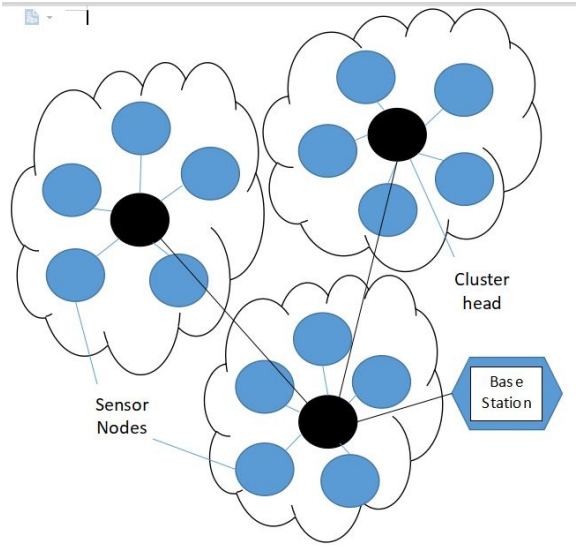

Fig. 10 Hierarchical tree topology

This topology is best oriented for application fields where large scale sensor nodes are the prime focus. To exemplify, research in seismology requires the collection of worldwide information pertaining to seismology which is quite significant, however, this arises the problem of scalability[5]. This can be fixed with the help of a hierarchical tree layout. In this arrangement, all the cluster heads of the groups or clusters are connected with each other and one of the nearest cluster heads maintains a connection with the gateway or base station.

The sensor nodes that are connected with a particular cluster head are all in a group or cluster. Every other node or cluster head is outside of the respective boundary of the cluster. Despite the presence of clusters in this orientation, it is different from the clustered hierarchical topology of the wireless sensor networks. In order to rectify the problems that might arise in large scale deployment of sensors such as in the Internet of Things(IoT) related application areas, the hierarchical tree topology can work wonders in solving the scalability problem[5].

Clustered Hierarchical Topology

The clustered hierarchical configuration in a wireless sensor network consists of clusters following a different hierarchical fashion than the tree topology as shown in Fig. 11. This orientation introduces a new type of nodes known as gateway nodes. In previous network arrangements, either a gateway or base station used to be present to perform a similar task. However, in this topology, gateway nodes are different from the base station. In addition to this, all the sensor nodes maintain a connection with the nodes of their cluster as well as the sensors of other clusters in the network. The specific nodes that are actually connected directly with nodes of other clusters are known as gateway nodes, which differ from the ordinary sensor nodes. This architecture preserves a tree rooted at the sink node or base station with a ladder of cluster heads as internal nodes and the sensor nodes as leaf nodes for the addressing and arrangement of the network[4].

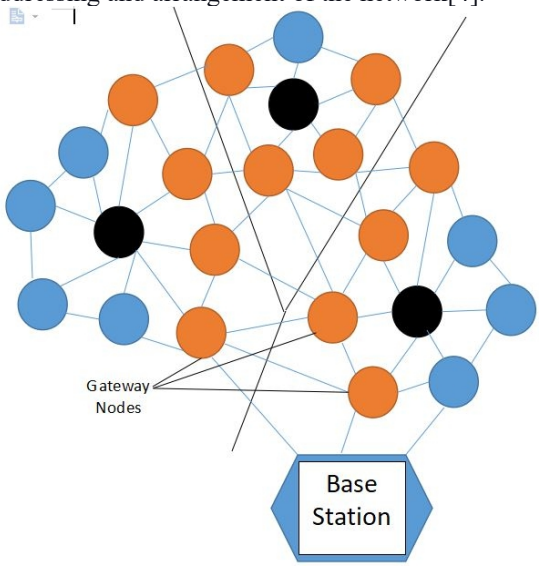

Fig. 11 Clustered hierarchical topology

There does not exist a comprehensive rule in the selection criteria of network topologies, because each layout has its own merits and demerits under particular operational conditions such as energy needs, scalability of the network, data transmission reliability, and environmental conditions[4]. Due to the energy constraints, the sensor nodes are bound to be destroyed gradually and results in a less crowded sensor network[3]. In order to maintain a healthy and durable network architecture, it needs to be fault-tolerant[3].

IV. Security threats and attacks

Security is a global term referring to the features of authentication, privacy, integrity, non-repudiation, and anti-playback[10]. All the permitted receivers should get the transmitted data meant for them and also should be capable of checking the data integrity and sender's identification[9]. Priority is being reserved for the routing strategies and the models of

the wireless sensor network, because of which security challenges are still queued up to receive immense attention[10]. However, security is often at a risk due to possible threats or attacks that can occur either from inside or outside of the wireless sensor network. There are three basic types of security threats, viz. Internal, external, and device-level capability attacks as shown in Fig. 12.

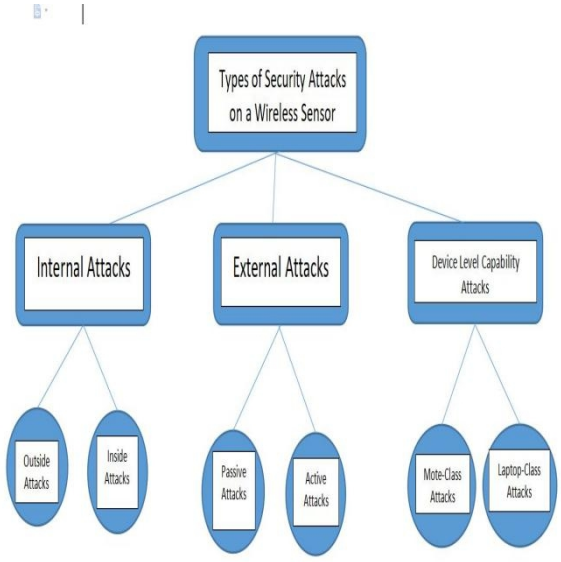

Fig. 12 Types of security attacks

When the sensor nodes are oriented according to one of the complex network architectures, then sensor nodes are deployed on a large scale which exposes them to attackers who may program each node again[8]. There are many ways an attacker can corrupt the information like affecting the routing information(spoofed, altered, or replayed routing information), adding their malicious nodes among the original sensor nodes, and refusing to transmit data ahead(selective forwarding)[9].

On a collective level, security attacks can also occur at various levels in the network like network level, application level, data level, physical level, and so on. Holistically advancing toward solving security problems takes us to the fundamentals of this
an approach which says, the security layers at every above-mentioned level should be built, hence, the security attacks at every layer should be rectified[10]. The attackers transmit spurious cluster-head client messages with the help of a very robust radio signal and trick multiple nodes into connecting to a non-existent cluster[14].

Internal Attacks

The main objective of internal attacks is to produce some compromised sensor nodes in the sensing region. These nodes either parallelize or disrupt the entire network architecture[7]. The attacker can perform a twofold task in this type of security threat. The former being the introduction of new sensor nodes from outside of the network and the latter being the reprogramming of the existing sensor nodes and converting them into malicious nodes[7].

The intention of both ways is to refuse to transmit the sensor information further through the path. The sensor nodes in the sensing region are being altered, which is internal to the network arrangement, because of which it is termed as an internal attack. The impersonation of the faulty sensor nodes have a few goals to fulfill: to get access to the keys or codes (cryptography or encryption keys) of the wireless sensor network, full or semi deterioration of the network in a gradual manner, and disclosing the secret keys of the algorithms in any security technique.

The insider attacks are capable of exposing the entire organization's information to cybersecurity imperilment. At times, an inside attack does not happen inside an organization but by the access that a company gives to contractors. According to a report - 'the case of leaked British bank accounts from call centers' in India, around 2 lakh bank accounts were compromised in Pune. This was totally due to the leniency of the security handling of the company. The sensitive information should be managed with utter care by the organizations.

External Attacks

As the name suggests, the external attacks are not pertaining to the sensor nodes of the wireless sensor networks. These act externally and can be categorized into two sub-attacks, viz. Passive and active attacks. The passive attacks include unauthorized hearing of the data packets traveling in the routing path[7]. This process is commonly known as eavesdropping. It is the act of secretly listening to a piece of confidential information or conversation of others without their permission to steal their data. This is globally an unethical and illegal practice. This can be performed by two methods - Explicitly listening to a digital or analog verbal communication, and interdicting the information pertaining to a type of conversation.
On the other hand, an active attack allows the alteration of the data stream transmitting in a routing path or creating a wrong stream of data[7]. It results in destroying the functions of a network due to the practice of attacks like DOS(denial of service), power exhaustion, and jamming threats[7].

Device-level capability attacks

The attackers attack the wireless sensor network using different kinds of devices. If the attacker considers a less powerful device such as a sensor device, then the attack is termed as a mote-class attack. Contrarily, if an attacker uses a more powerful device like a laptop, then the attack is referred to as a laptop-class attack.
In a mote-class attack, the adversary uses some sensor nodes with matching abilities to the network nodes, while, in a laptop-class attack, the attacker uses multiple powerful devices to cause a threat to a wireless sensor network[7]. In the latter, a higher transmission rate, powerful processors, and more energy is seen in the devices[7].

Table 1 Types of security attacks

Internal Attacks	Outside Attacks	Introduction of new sensor nodes from outside of the network
	Inside Attacks	Reprogramming of the existing sensor nodes to convert them into malicious nodes
External Attacks	Passive Attacks	Unauthorized listening to the routing packets
	Active Attacks	Changing the information stream in a network
Device Level Capability Attacks	Mote-Class Attacks	Less powerful device is used by the attacker
	Laptop-Class Attacks	More powerful device is used by the attacker

IV. Security techniques in WSN

In late years, a huge amount of investigation on core parts of wireless sensor network security code, protocols, algorithms, network orientation, etc has been performed and has achieved a lot[12].

Encryption

The process of transforming the original information to the encrypted data is called encryption as shown in Fig. 13. The original data is referred to as plain text, and the encrypted information is known as ciphertext or simply a code. The reverse process is called decryption. This technique is commonly used to avoid unauthorized access. This method provides security from passive attacks (eavesdropping)[7]. Encryption plays a vital role in providing safety to multiple kinds of IT assets by ensuring the following:

Confidentiality - this process keeps the data secure and safe from getting leaked or attacked. It refers to the constraints of people and organizations to use the data that has been disclosed to them and is under their management.

Authentication - It refers to the process of accessing the data with proper permission. The most common authentication procedure that is followed globally is the login process. In this, the user enters his/her name and password. This combination is assigned to all the users, however, this kind of information can be easily hacked by attackers. This phase is usually invoked when an end-user wants to perform either a query or access some information[15].

Integrity - The receiver must receive complete and accurate data from the sender. Data integrity refers to the accurateness of the information. When the data is reached at the final destination without being changed in any way, then integrity is maintained. This is usually inflicted at the time of the database design phase by making use of rules and processes. It also involves error-checking techniques and validation processes.

Non - repudiation - It is a process of making sure that every data packet between the sender and the receiver is guaranteed to get transmitted with the help of a security technique. It assures the safe transmission of data, hence, it is one of the five pillars of information assurance(IA), the other four being availability, integrity, confidentiality, and authentication.

It is extremely unimportant to add messages to a network or performing eavesdropping because the sensor nodes run in insecure wireless environments, and that is where encryption comes in to help rectify this difficulty[7].

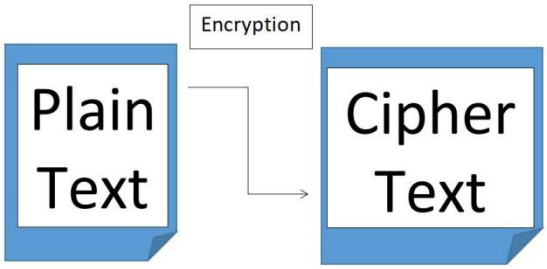

Fig. 13 Encryption

Encryption can be performed in two ways, viz. Symmetric and asymmetric encryption. Decryption is

the opposite of encryption. This is performed at the receiver's end in order to get the original documents again. The reverse algorithm is applied in order to convert the ciphertext to plain text as shown in Fig. 14.

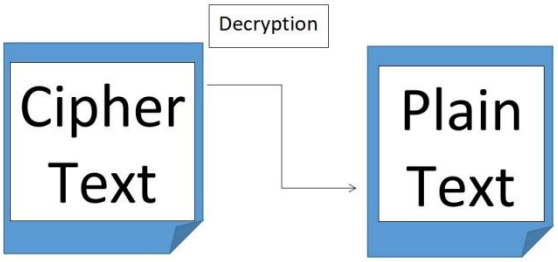

Fig. 14 Decryption

Symmetric Encryption

This technique in encryption uses a single key to both encrypt as well as decrypt, hence, also known as the sole key encryption[7]. In this encryption technique, as the name suggests, the source gives approval upon a key known as the secret or shared key[7]. As is shown in Fig. 15, the plain text(original data) is initially converted to a ciphertext(encrypted code) with the help of an algorithm and a key. The reverse(decryption) is performed by converting this ciphertext back to plain text. If the conversation is between two sensor nodes, then symmetric encryption(symmetric key cryptography) is a very suitable security technique[13].

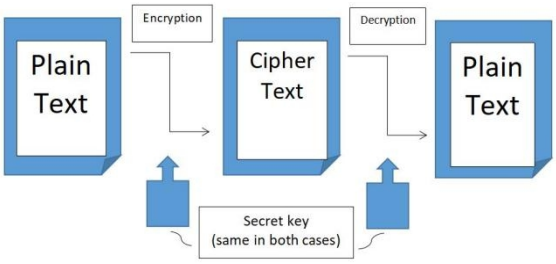

Fig. 15 Symmetric encryption

Asymmetric Encryption

In Fig. 16, it can be seen that instead of one shared key, this technique utilizes two keys named public and secret key. The public key is used to convert the plain text to cipher text(encryption), while the secret key is used to convert the ciphertext back to the plain text(decryption) after the data has traveled to its destination. It is also called public-key cryptography[7]. Both the public and the secret(or private) key are related to each other, in that a public key has a connected secret key and the data encrypted through the public key can only be decrypted with the help of the associated private key[7].

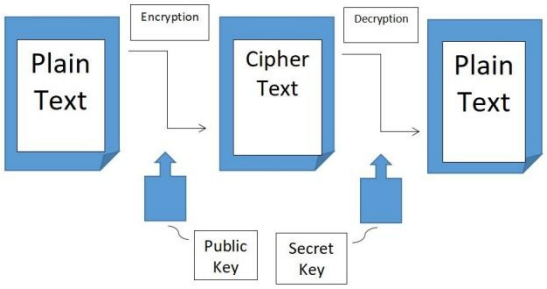

Fig. 16 Asymmetric encryption

Cryptography

The process of encoding and decoding data packets in a cipher code is known as cryptography.
When these cryptographic techniques are applied in wireless sensor networks, they must go through the sensor node constraints or restrictions and must fulfill the evaluation criteria including the size of the statistics, processing time, and length of the code[7].

Table 2 Security Techniques

Security Techniques	*Technique followed*
Encryption and Decryption	Encryption - conversion of plain text to cipher text Decryption - conversion of cipher text to plain text
Symmetric Encryption	Conversion of plain text to cipher text and reverse, both with the help of a single key(shared key)
Asymmetric Encryption	Conversion of plain text to cipher text with the help of public key and cipher text to plain text through private(secret) key
Cryptography	Study of techniques like encryption, decryption, symmetric and asymmetric encryption

V. Conclusion

The letter explored a wireless sensor network that comprises several sensor nodes combined together to execute a dedicated work of accepting and

forwarding data of a real-life system, which is of least importance if there is little information about its location. In this paper, we have discussed the two common kinds of wireless sensor network architectures. The first one is a single-hop network architecture, and the second one is multiple-hop network architecture. The latter one is further sub-divided into two types of networks, viz. flat-network and hierarchical-network architecture. This discussion is further followed by the explanation of components of the wireless sensor network that can be oriented in various ways, which give rise to network topologies like a star, mesh, tree hierarchical, and clustered hierarchical topology. Furthermore, we focused on an extremely significant factor, i.e., the security of a wireless sensor network. Several threats pertaining to security are obliged to be taken into consideration, such as internal attacks, external attacks, and device-level capability attacks. To eradicate or avoid these attacks, many security techniques have been discussed in this paper such as encryption, symmetric, and asymmetric encryption, and cryptographic methods.

VI. References

1 - Elson, J., & Römer, K. (2003). Wireless sensor networks: A new regime for time synchronization. *ACM SIGCOMM Computer Communication Review*, *33*(1), 149-154.

2 - Carlos-Mancilla, M., López-Mellado, E., & Siller, M. (2016). Wireless sensor networks formation: approaches and techniques. *Journal of Sensors*, *2016*.

3 - Meena, S. S., & Manikandan, J. (2017, March). Study and evaluation of different topologies in a wireless sensor network. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 107-111). IEEE.

4 - Shrestha, A., & Xing, L. (2007, May). Performance comparison of different topologies for wireless sensor networks. In *2007 IEEE Conference on Technologies for Homeland Security* (pp. 280-285). IEEE.

5 - Huang, L. (2011, September). Virtual hierarchical tree topology for large scale wireless sensor network. In *2011 Second International Conference on Networking and Distributed Computing* (pp. 259-261). IEEE.

6 - Zhang, L., Qu, J., & Fan, J. (2016, December). Topology evolution is based on the complex networks of the heterogeneous wireless sensor network. In *2016 9th International Symposium on Computational Intelligence and Design (ISCID)* (Vol. 2, pp. 317-320). IEEE.

7 - Sengar, P., & Bhardwaj, N. (2017). A survey on security and various attacks in a wireless sensor network. *Int. J. Comput. Sci. Eng*, *5*(4).

8 - Li, Y. X., Qin, L., & Liang, Q. (2010, December). Research on wireless sensor network security. In *2010 International Conference on Computational Intelligence and Security* (pp. 493-496). IEEE.

9 - Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, *1*(2-3), 293-315.

10 - Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In *2006 8th International Conference Advanced Communication Technology* (Vol. 2, pp. 6-pp)

11 - Ahmed, N., Kanhere, S. S., & Jha, S. (2005). The holes problem in wireless sensor networks: a survey. *ACM SIGMOBILE Mobile Computing and Communications Review*, *9*(2), 4-18.

12 - Yang, Q., Zhu, X., Fu, H., & Che, X. (2015). Survey of security technologies on wireless sensor networks. *Journal of Sensors*, *2015*.

13 - Ozdemir, S., & Xiao, Y. (2009). Secure data aggregation in wireless sensor networks: A comprehensive overview. *Computer Networks*, *53*(12), 2022-2037.

14 - Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, *7*(1), 74-81.

15 - Das, M. L. (2009). Two-factor user authentication in wireless sensor networks. *IEEE transactions on wireless communications*, *8*(3), 1086-1090.