WIRELESS SENSOR NETWORK: KEY SECURITY ISSUE AND CHALLENGES

Shahana.P.N
pnshahana@yahoo.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.09/Issue05/MYAE10080
Research Article | Open Access
Peer-review: Double-blind Peer-reviewed
Article ID: IJIRAE/RS/Vol.09/Issue05/MYAE10080
Received Date: 06, May 2022 | Accepted Date: 14, May 2022 | Available Online: 31, May 2022
Volume 2022 | Article ID MYAE10080 http://www.ijirae.com/volumes/Vol9/iss-05/03.MYAE10080.pdf
Article Citation: Shahana (2022). Wireless Sensor Network: Key Security Issue and Challenges. International Journal of Innovative Research in Advanced Engineering (Vol. 9, Issue 5, pp. 116–123). AM Publications, India
https://doi.org/10.26562/ijirae.2022.v0905.03
BibTeX key shahana2022wireless
Academic Editor-Chief: Dr.A.Arul Lawrence Selvakumar

Abstract: Wireless sensor networks (WSNs) are interconnected sensor nodes that communicate wirelessly to collect data about the surrounding environment. A typical sensor node is made up of different components to perform the task of sensing, processing and transmitting data. WSNs are used for many applications in diverse forms from indoor deployment to outdoor deployment. The basic requirement of every application is to use the secured network. Providing security to the sensor network is a very challenging issue along with saving its energy. Many security threats may affect the functioning of these networks. Because of their low cost and adaptability, wireless sensor networks are widely used in civil, military, and commercial fields and other fields. However, since the sensor node in the calculation of the capacity, battery capacity, and storage capacity are restricted by the limitations and inherent characteristics of the sensor networks, compared to traditional networks, which makes wireless sensor networks face more security threats. This paper summarized the various security issues and security threats in WSNs and solutions. It identifies various possible attacks at different layers of the communication protocol stack in a typical WSN and presents their possible countermeasures. A brief discussion on the future direction of research in WSN security is also included.
Keywords: Wireless sensor network (WSN), Security

I. INTRODUCTION

Wireless sensor networks, as an emerging network technologies, have risen gradually recently. They can obtain a lot of detailed and reliable information in the network distributed area anytime and anywhere; thus, they are widely used in military defense, industry, agriculture, construction and urban management, biomedical and environmental monitoring, disaster relief, public safety and antiterrorism etc. [2]

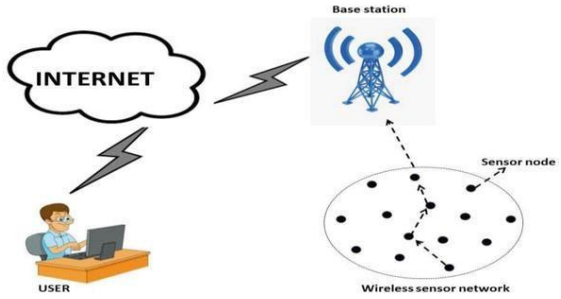

Fig 1: A typical wireless sensor networks (WSN)

Fig 1 shows a wireless interconnected network which consists of independently setup devices that monitor the conditions of its environment using sensors. In WSNs, sensor nodes have the ability to communicate with one another, but their primary task is to sense, gather, and compute data. These data are forwarded, via multiple hops, to a sink which may use it or relay it to other networks. [5] To achieve an effective communication, WSNs need efficient routing protocols. There are two modes of transmission in WSN; single hop involves the source node sending its data packets to the destination within a hop. Meanwhile, WSNs' sensor nodes may rely on one another in order to relay packets to remote destinations.

This mode of transmission is called multi-hop. Multi-hop is a routing phenomenon that involves the transfer of data between source and destination nodes with the cooperation of intermediary nodes. It enhances the performance of WSNs by allowing energy-depleted node to transfer data through its neighboring nodes along the routing path to the destination node. There are several security and privacy issues associated with multi-hop routing. Some of these issues like snooping, sinkhole, tampering Sybil, clone, wormhole, spoofing, etc. Affect the integrity, availability, and data confidentiality of the WSNs. WSN is used in many applications from indoor to outdoor. While transmitting information in the network it is important to provide security. Security is considered to be the most challenging task in WSN as its tough to keep a watch on the sensor nodes/network every time. But it must be secured to prevent an intruder from attacking the transmission of data. [3]

II. OVERVIEW OF SECURITY CONSTAINTS IN WSN

A WSN is a special network which has many constraints compared to a traditional computer network. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, some constraints are listed below

- Memory and power limitations: A sensor is a tiny device with only a small amount of memory and storage space for the code. It is necessary to limit the code size of the security algorithm to build an effective security mechanism; Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced or recharged because of high operating cost. [5]
- Unreliable Communication: It is one of the major threats to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. The major parameters are unreliable transfer, latency and conflicts.

There are lots of constraints with a sensor node specially its size and cost that should be minimum. These constraints result in very small size memory, limited energy source and transmission range. This ultimately results in no encryption, decryption and authentication that can be actualized on sensor node. Attack and attacker are the most common terms used in the security. Attacker is the one who is an unauthorized to access the data of the network or tries to mislead the information. When an attacker accesses the services of the network is known as attack. [6]

2.1 Security Requirements

Sensor network have to fulfill some requirements for providing a secure communication. General security requirements of WSNs are availability, confidentiality, integrity and authentication. Some other requirements known as secondary requirements are source localization, self-organization and data freshness. These requirements give protection against attacks to the information transmitted over the sensor network. [8]

Following are the Security Requirements in Wireless Sensor Networks.

- Confidentiality – In sensor network, data flows from many intermediate nodes and chance of data leak is more. To provide the data confidentiality, an encrypted data is used so that only recipient decrypts the data to its original form. It ensures that sensitive information is well protected and not revealed to unauthorized third parties. Helps to protect information traveling between the sensor nodes of the network or between the sensors and the base station from disclosure, since an adversary having the appropriate equipment may eavesdrop on the communication. [1]
- Integrity - Data received by the receiver should not be altered or modified is Data Integrity. Original data is changed by intruder or due to harsh environment. The intruder may change the data according to its need and sends this new data to the receiver. Data in transit can be changed by the adversaries. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity ensures that the information is not changed in transit, either due to malicious intent or by accident. Use of message integrity code is a standard approach for ensuring data integrity. [9] Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous, for example for the healthcare sector where lives are endangered. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications such as pollution and healthcare monitoring rely on the integrity of the information to function with accurate outcomes; it is unacceptable to measure the magnitude of the pollution caused by chemicals waste and find out later on that the information provided was improperly altered by the factory that was located nearby the monitored lake. Therefore, there is urgent need to make sure that information is traveling from one end to the other without being intercepted and modified in the process. [2]
- Authentication - It the procedure of confirmation that the communicating node is the one that it claims to be. It is important for receiver node to do verification that the data is received from an authenticate node. In any decision making process, the receiving nodes need to ensure that the data originates from the reliable source. Similarly, authentication is necessary during an exchange of control information in the network. Data authenticity is an assurance of the identities of communicating nodes. [1] In the case of sensor networks, it is essential for each sensor node and base station to have the ability to verify that the data received was really send by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data.

- If such a case happens and false data are supplied into the network, then the behavior of the network could not be predicted and most of the times will not outcome as expected. Authentication objective is essential to be achieved when clustering of nodes is performed. clustering involves grouping nodes based on some attribute such as their location, sensing data etc. and that each cluster usually has a cluster head that is the node that joins its cluster with the rest of the sensor network (meaning that the communication among different clusters is performed through the cluster heads).[8] In these cases, where clustering is required, there are two authentication situations which should be investigated; first, it is critical to ensure that the nodes contained in each cluster will exchange data only with the authorized nodes contained and which are trusted by the specified cluster (based on some authentication protocol). Otherwise, if nodes within a cluster receive data from nodes that are not trusted within the current community of nodes and further process it, then the expected data from that cluster will be based on false data and may cause damage. The second authentication situation involves the communication between the cluster heads of each cluster; communication must be established only with cluster heads that can prove their identity.
- Data Availability - Data Availability means that the services are available all the time even in case of some attacks such as Denial of service. Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. It may happen that an attacker may jam communication to make sensor(s) unavailable. The requirement of security not only affects the operation of the network, but is also highly important in maintaining the availability of the network. Lack of availability may affect the operation of many critical real-time applications like those in the healthcare sector that require a 24/7 operation that could even result in the loss of life. Therefore, it is critical to ensure resilience to attacks targeting the availability of the system and find ways to fill in the gap created by the capturing or disablement of a specific node by assigning its duties to some other nodes in the network.
- Data Freshness - Data freshness means that each message transmitted over the channel is new and fresh. It guarantees that the old messages cannot be replayed by any node. This can be solved by adding some time related counter to check the freshness of the data. Data freshness objective ensures that messages are fresh, meaning that they obey in a message ordering and have not been reused. To achieve freshness, network protocols must be designed in a way to identify duplicate packets and discard them preventing potential mix-up. This requirement is especially important when the WSN nodes use shared keys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN. The out-dated information contained in the packet can cause many problems to the applications deployed in the network. [7]
- Source Localization - For data transmission some applications use location information of the sink node. It is important to give security to the location information. Non-secured data can be controlled by the malicious node by sending false signal strengths or replaying signals.
- Time Synchronization - In order to conserve power, an individual sensor node may be turned off periodically. Any security mechanism for WSN should also be time-synchronized. [2]
- Self-Organization - In WSN no fixed infrastructure exists, hence, every node is independent having properties of adaptation to the different situations and maintains self-organizing and self-healing properties. This is a great challenge for security in WSN.

III. SECURITY ISSUE IN WSN

Attackers may devise different types of security threats to make the WSN system unstable. Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. WSNs are vulnerable against so many attacks. Attackers can attack the radio transmission; add their own data bits to the channel, replay old packets and any other type of attack. A secure network ought to support all security properties. [3] Attackers may deploy some malicious nodes in the network with similar capabilities as of normal node or may overwrite the memory of normal deployed node by capturing them. [5]

3.1. Security Attacks

Attacks in wireless sensor network are shown in Fig 2. They are roughly categorized as follows:

1. **Based on Routing**
2. **Based on Capability**
3. **Based on Protocol Layer**

1. On the Basis of Routing: There are lots of routing protocols proposed for transmitting the data in the network from source to sink. In this transmission process, an attacker can steal or modify the information with the help of different attacks. Some of the routing attacks are explained below: [4]

a. Wormhole Attacks: In this attack there are two or more malicious nodes present in the network at different locations. When sender node sends information then one malicious node tunnels the information to another malicious node. The receiving malicious node then sends information to its neighbor nodes. A wormhole is low latency link between two portions of a network over which an attacker replays network messages. This link may be established either by a single node forwarding messages between two adjacent but otherwise no neighboring nodes or by a pair of nodes in different parts of the network communicating with each other.

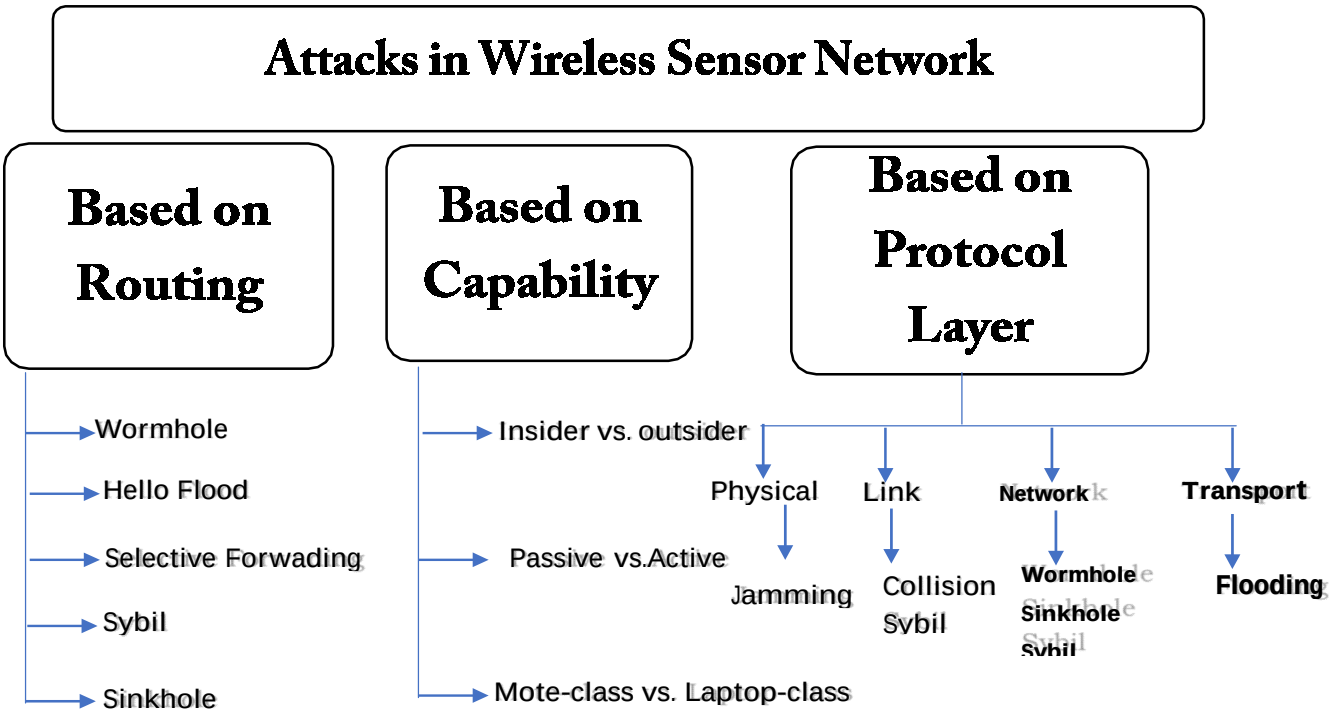

Fig 2: Attacks classification in WSN

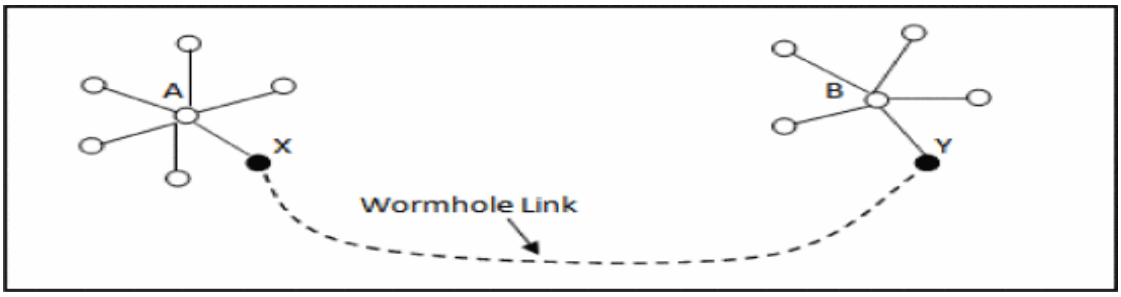

Fig 3: Wormhole attack

Fig 3 shows that the node X and node Y are nodes which are maintaining the wormhole link in the network and they are the two malicious nodes. There is a shortcut link between both malicious nodes known as wormhole link. Node A sends message which is received by node X. Node X sends message to Node Y through wormhole link which further sends it to its neighbor node B.

b. HELLO Flood Attacks: In a sensor network to discover the neighbors HELLO message is broadcasted by the nodes. The receiver node considers that the source node is in the range of data transmission and sends its sensed data to the broadcaster.

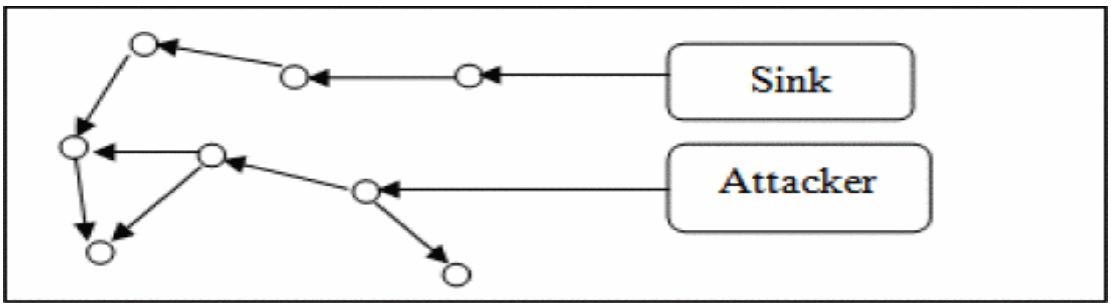

Fig 4: HELLO flood attack scenario-hello packet send by the attacker

In a HELLO Flood Attack, HELLO message is broadcast with high transmission power by the attacker. The nodes which receive this HELLO message send the data packets to the attacker node. Attacker may change or modify the data packet or may drop the packet. In this way, a lot of energy is wasted and also network congestion occurs. This attack is one of the least difficult attacks in WSN. As shown in Fig 4 attacker node broadcasts the HELLO packet with high transmission power than the sink. Fig 5 shows that the nodes which receive HELLO packet from attacker node consider it as a neighbor node and send/reply the sensed data packet to the attacker node. [6]

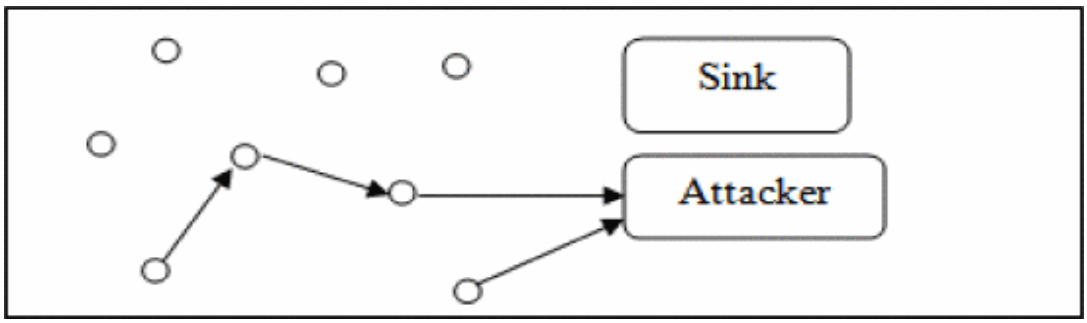

Fig 5: HELLO flood attack scenario-sensor node replying back to the attacker considering it as its neighbor node

c. Selective Forwarding Attack: In this attack, a malicious node in the network interrupts the communication process. There may be the case of multiple malicious nodes in the network that depends upon the attacker. This node selectively forwards some of the received packets. This malicious node can also be referred as a black hole as it may drop all the received packets. In such case, neighboring nodes assumes that this has failed and starts searching for another route. This attack is easy to detect if it acts as a black hole and drop all the received packets but is complicated if it forwards packet selectively. On the off chance that an attacker included externally to the path then selective forwarding attacks are more viable. [7] On the premise of packets drops, it is divided into two categories:

- Drops packets of some specified nodes
- Drops packets of some specified types

d. Sinkhole Attack: In sinkhole attack, a malicious node advertises fake routing information to attract the network traffic. WSNs are vulnerable to this type of attack because communication happens in many to one form i.e. many sensor nodes to a single BS. Wormhole attack can also be used in combination with this attack. In Fig 6, malicious node has more power than other nodes in the network and connects with the sink node using single hop. It claims and displays to have the shortest possible path to the sink so that more network traffic is attracted towards it. Most of the routing algorithms select the shortest path for data transfer. [10]

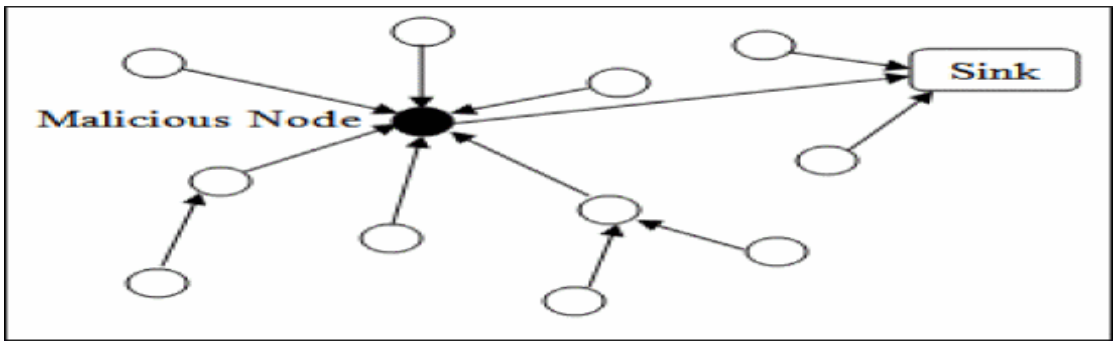

Fig 6: Sinkhole attack

2. Based on Capability

a. External Attacker (Outsider)

If the attacker launches an attack by using the malicious node(s) outside of the network that was not a part of the network when the network was initially deployed, then this type of attack is termed as external attack. While launching the external attack the aim of the adversary is to effect traffic congestion, disseminate bogus routing information or disturb nodes from extending desired services.

Some salient features of outsider attacks include:

- The adversary or attacker exists outside the perimeter of the network i.e. does not fall within range of wireless sensor networks
- illegal or unauthorized parties execute this attack
- Attacks are initiated before being authenticated [7]

b. Internal Attacker (Insider)

If an adversary launches an attack by using or impersonating one of the actual nodes of the network that was originally the part of the network at the time of its deployment then this type of attack is termed as internal attack [5]. Some of the goals of these attacks are [3]:

- The adversary has got a right to cryptographic keys or other codes of wireless sensor network
- Partial or total degradation
- Secret keys disclosed

c. Passive and active attacks criteria

Attacks can be classified into two major categories, according the interruption of communication act, namely passive attacks and active attacks.

From this regard, when it is referred to a passive attack it is said that the attack obtain data exchanged in the network without interrupting the communication. When it is referred to an active attack it can be affirmed that the attack implies the disruption of the normal functionality of the network, meaning information interruption, modification, or fabrication. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay. [8]

d. Mote-Class Attack

The mote-class attack is an attack in which devices comparable to WSN sensor nodes to be attacked. This depicts that this attack:

- Occurs within the perimeter of wireless sensor networks
- Uses compromised sensor nodes or granted access to alike motes/nodes (which contain comparable functional capability as wireless sensor network's motes/nodes)
- Ensures the execution of programs of malicious nature An attacker of Mote-Class may have many objectives, which include: [9]
- To ensure the jamming of radio link
- To paved way for the stealing of cryptographic keys

e. Laptop-Class Attack

Laptop-class attack is an attack which utilizes extra powerful devices as compare to ordinary wireless sensor nodes, to achieve the following:

- Injection of unwanted traffic eavesdropping of the entire wireless sensor networks data will be carried out by a device which belongs to a laptop-class. Attackers of laptop-class have many effects on wireless sensor networks, for instance: [1]
- more grave attacks will be launched which may then lead to more severe damage
- Possesses the capability to provide way in to low latency communication channel and high bandwidth

3. Based on Protocol Layer

a. Physical layer attacks

Deal with the specification of the frequencies bands. This layer must ensure of the techniques of emission, reception and modulation of data in a robust way. The attacks associated in the physical layer are very few but, at the same time, can be most difficult to prevent: jamming on the same frequency that the network uses, and the physical attack of a node. [7] One standard defense against jamming employs spread spectrum communication. Node capture is the more upsetting problem in the security of WSNs. The use of resistant hardware against capture attack (tamperproof node) can solve this problem, but increase the node cost.

- Jamming: It is caused due to interference with the radio frequencies of the network's devices which is an attack on the availability of the sensor network. It is different from normal radio propagation in the way that it is unwanted and disruptive, thus resulting in denial-of-service conditions.
- Tampering: It is also called node capturing in which a node is compromised, it is easy to perform and is pretty harmful. Tampering is physically modifying and destroying sensors nodes.

b. Link layer attacks

- Collision: It is caused in link layer that handles neighbor-to-neighbor communication along with channel arbitration. Entire packet can be disrupted if an adversary is able to generate collisions of even part of a transmission, CRC mismatch and possibly require retransmission can be caused by a single bit error.
- Exhaustion: Exhaustion of a network's battery power can be induced by an interrogation attack. A compromised node could repeatedly send thus consuming the battery power more than required. [5]

c. Network layer attacks

Depending on the routing algorithm technique, a sinkhole attack tries to lure almost all the traffic toward the compromised node, creating a metaphorical sinkhole with the adversary at the center. Network layer is responsible for routing packets from the source node to the destination node. The network layer is vulnerable to many threats and attacks which aim to disturb the routing of the network, including the Replay Attack, Selective Forwarding Attack, Neglect and Greed, Misdirection Attack, Black hole/Gray hole Attack, Sinkhole Attack, Wormhole Attack, Sybil Attack, Hello Flooding Attack, and Homing Attack. Authentication is a solution. Such attacks can easily be avoided by verify bi- directionality of a link before taking action based on the information received over that link. [4]

d. Transport layer attacks

An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes. Solution: each connecting client demonstrates its commitment to the connection by solving a puzzle. Flooding attack – It is a Denial of Service (DoS) attack designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks usually occur when a network or service becomes weighed down with packets, thus initiating incomplete connection requests that it cannot, longer process genuine connection requests.

By flooding a server with connections that cannot be completed, flood attack eventually fills the server's memory buffer and once this buffer is full, no further connections can be made, and thus resulting in a Denial of Service. [10]

IV. SECURITY CHALLENGES

WSNs have many characteristics that make them very susceptible to malicious attacks in hostile environments such as a military battlefield as well as civilian applications: -

i. A wireless channel is open to everyone. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications. This provides a convenient way for attackers to break into WSNs. [1]
ii. Most protocols for WSNs do not include potential security considerations at the design stage and are known publicly. Therefore, attackers can easily launch attacks by exploiting security holes in those protocols.
iii. The constrained resources make it very difficult to implement strong security algorithms on a sensor platform due to the complexity of the algorithms.
iv. A WSN can scale up to thousands of sensor nodes. These pose the demand for simple, flexible, and scalable security protocols.
v. The design such security protocols is not an easy task. A stronger security protocol costs more resources on sensor nodes, which can lead to the performance degradation of applications.
vi. Weak security protocols can be broken easily by attackers and thus pose a great threat to the sensor networks.
vii. A WSN is usually deployed in hostile areas without any fixed infrastructure. Thus, difficult to perform continuous surveillance after network deployment. So, it may be susceptible to various kinds of attacks. [7]

V. APPLICATIONS

a. Military Applications: Possibly, WSNs is an essential fragment of military intelligence, facility, control, communications, computing, frontline surveillance, investigation and targeting systems. [2]
b. Vehicle Detection: Wireless sensor networks can use a range of sensors to detect the presence of vehicles ranging from motorcycles to train cars.
c. Medical/Health Applications: Some of the medical/health benefits of WSNs are in the areas of diagnostics, investigative, and drug administration as well as management, supporting interfaces for the incapacitated, integrated patient monitoring and management, tele-monitoring of human physiological information, and tracking and monitoring medical practitioners or patients inside the medical facility. [9]
d. Environmental monitoring: A number of WSNs have been deployed for environmental monitoring. This comprises of sensing oceans, seas, glaciers, atmosphere, volcanoes, forest, etc. However, there are presently some biosensors that have been developed for use in agricultural and environmental sustainability. Some other key aspects are; air contamination monitoring and management, forest fires discovery/detection, greenhouse (GH) monitoring and management, and Landslide discovery/detection. [6]
e. Industrial Applications: WSNs have been advanced for "Technological Condition-based Maintenance (TCBM)" since they could offer momentous cost reductions/investments and allow innovative functionalities. In wired classifications, the installation of adequate sensors is habitually limited by the amount involve in wiring. [4]
f. Agricultural Applications: The employment of WSNs has been reported assist farmers in various aspects such as the maintenance of wiring in a problematic environment, irrigation mechanization which aids more resourceful water use and reduction of wastes. [5]

VI. SECURITY GOAL

Since of nature of broadcast in transmission medium, restriction of resource on sensor nodes and environments without control where they are deserted without any participant, wireless sensor networks are susceptible to several attacks. WSNs have the mentioned general security purposes similarly to other communication systems. In confidentiality, just to authorize parties, information is attainable to read. In authentication, the data is originating from an authorized party. If data was changed from the secure to the destination, it is detected in integrity. In non-repudiation, the sender and the receiver of massage do not have capability to reject the transmission. Just authorized parties can employ particular resources in access control. In availability, resources attainable to authorized parties.

VII. CONCLUSION

WSN needs high level of security due to its harsh environment. This leads to intense security and survival requirements. The demand for security in WSNs becomes more obvious during ability growth of WSNs and they are used much more, however, in WSNs the node nature causes limitations like restricted energy, capability of processing, and storage capacity. These restrictions create WSNs so distinctive from conventional ad hoc wireless networks. Specific methods and protocols have been advanced to utilize in WSNs. All of the mentioned security dangers including the Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, offer one usual goal which is for compromising the integrity of the network they attack. To uphold the authenticity and data integrity measures are to be taken to resist against the attacks. Even though there are many security mechanisms the important one is the cryptographic techniques and protocols. The fundamental means of providing a security in WSNs is through the way of selecting the best suitable cryptographic technique. In this paper, a detailed analysis is given on security requirements, Issues and challenges of WSNs.

REFERENCES

1. Singh, C., Kaur, R., Kaur, M.: Review of security enhancement techniques for wireless sensor network. Int. J. Electron. Eng. Res. 9(8), 1185–1196 (2017). ISSN 0975-6450 Research India Publications
2. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Communications Magazine 40 (8) (2002) 104–112. https://doi.org/10.1109/mcom.2002.1024422
3. J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, Security for sensor networks, 2002 CADIP Research Symposium. https://doi.org/10.1007/978-1-4020-7884-2_12
4. Karlof and D. Wagner, Secure routing in wireless sensor networks: Attacks and Countermeasures, Elsevier's Ad Hoc Networks Journal, Special Issue on https://doi.org/10.1016/s1570-8705(03)00008-8
5. Sensor Network Applications and Protocols, Vol. 1, No. 2-3, pp. 293-315, 2003.
6. Roman R, Zhou J, Lopez J (2005) On the Security of Wireless Sensor Networks. In Proceedings of 2005 ICCSA Workshop on Internet Communications Security, LNCS 3482, pp. 681–690. https://doi.org/10.1007/11424857_75
7. Pathan ASK, Lee H-W, Hong C S (2006) Security in wireless sensor networks: issues and challenges. Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, 2(20–22). https://doi.org/10.1109/icact.2006.206151
8. Giruka, V.C., et al., 2008. Security in wireless sensor 9. Kalita, H.K. and A. Kar, 2009. Wireless sensor networks. Wireless communications and mobile network security analysis. International Journal of computing, 8(1): 1-24 https://doi.org/10.1002/wcm.422
9. Culler, D. E and Hong, W. Wireless Sensor Networks, Communication of the ACM, Vol. 47, No. 6, 2004, pp. 30-33.
10. Adrian Perrig,John Stankovic, and David Wagner,(2004)" Security in wireless sensor networks",Commun;ACM,4796):53-57. https://doi.org/10.1145/990680.990707
11. Al-Sakib Khan Pathan et al.,(2006)" Security in Wireless sensor networks: Issues and Challenges", in feb. 20-22,2006,ICACT2006,ISN 89-5519-129- 4,pp(1043-1048).