ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Review on Security attacks and Countermeasures in Wireless Sensor Networks

Pooja
DCSA, Kurukshetra University
Haryana, India

Dr. R.K.Chauhan
DCSA, Kurukshetra University
Haryana, India

Abstract: Wireless sensor network consists of sensor nodes having sensing and computation capabilities. Because of their availability and less cost than the traditional networks, they are widely used. As the demand of sensor networks increases, they are more prone to security attacks. There are many classifications of attacks and one of them is discussed in this paper. This paper discusses the architecture of sensor network and sensor nodes, and then how wireless sensor network different from the traditional networks. After then, concept of Security in sensor networks is discussed. This paper presents one of the classifications of attacks in WSN and countermeasures of each attack are discussed with each attack.

Keywords: wireless sensor networks; sensor nodes; applications; challenges; security; attacks

I. INTRODUCTION

Wireless Sensor Networks depends on a simple equation [1] i.e. Sensing + CPU +Radio= Thousands of applications. It consists of thousands of tiny nodes, called sensor node sand is also called motes. These are deployed over a geographical area to monitor a wide variety of environmental conditions such as: temperature, pressure, humidity, lightening conditions, noise levels etc.[2].These sensor nodes communicate and work together to achieve a common task, for example, in the area of environment monitoring, healthcare monitoring, military surveillance, transportation systems, industrial process control and so on.

Architecture and Working of WSN

The main components of sensor network are: sensing field, sensor nodes, Base station and Internet. In wireless sensor network, sensor nodes are deployed in sensor field and are usually scattered [3]. Fig.1 shows the architecture of wireless sensor network [36]:

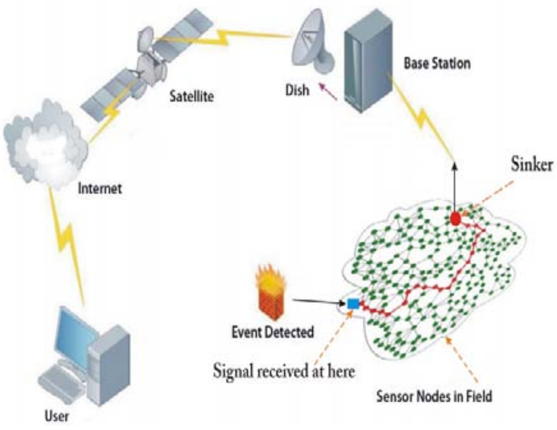

Fig.1 Architecture of Wireless sensor Network

They communicate among themselves and collect high-quality information about the environment, process it and send it to Base Station (BS). Base station acts as a gateway or an interface between user and internet. Then Base station transmits that data to the internet so that user can easily access the data. As WSN is a collection of sensor nodes. These nodes may be of different sizes and their size depends on the type of application where they have deployed. The main components of sensor node are: controller, transceiver, power supply, memory and one or more sensors [4]. The architecture of sensor node [1] is shown in fig. 2:

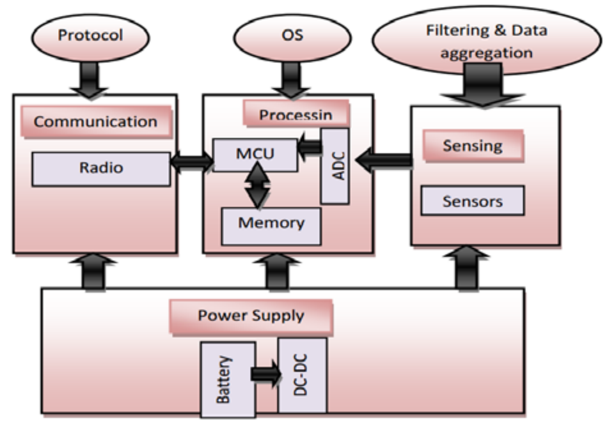

Fig.2 Architecture of Wireless Sensor Node

Controller

The duties of controller are: to perform tasks, to process data and to control the functionality of other components in the sensor node. The most common controller is microcontroller which is used in many embedded systems such as sensor nodes because it has so many advantages like low cost, ease of programming, flexibility to connect to other devices and low power consumption. To conserve the energy, microprocessor acts in four modes [1]: active, idle, sleep and off. In active mode, CPU and all other peripheral devices are active. In idle mode, only CPU is inactive and peripheral devices are working. In sleep mode, CPU and internal peripheral are turned off and they will be awake by an external event. Alternatives of micro-controller are general purpose desktop microprocessor, FPGAs, ASICs and digital signal processor.

Transceiver

Sensor nodes frequently make use of ISM band, because it provides spectrum allocation, free radio and global availability [18]. The likely choices of wireless transmission media for a sensor node are radio frequency (RF), optical communication also called laser and infrared. The property of Laseris that it demands less energy, but needs line-of-sight for communication and lasers are very sensitive to atmospheric conditions. Infrared needs no antenna but it is restricted in its broadcasting power. Radio frequency-based communications are the most appropriate that fits most of the WSN applications. WSNs uses short range unlicensed communication frequencies and these are: 173, 433, 868, and 915 MHz; and 2.4 GHz. The functionality of both transmitter(used to transmit the signals) and receiver(used to receive the signals) are combined into a one device known as a transceiver. Transceivers often lack unique identifiers. The transmitter operates in four states: receive, transmit, idle, and sleep. Transceivers when operating in idle state consumes same amount of energy when transceiver is in receive state [5]. So, it is better to totally shut down the transceiver rather than leave it in the idle state when it is not doing anything (transmitting or receiving). A considerable amount of power dissipates when transceiver switches from sleep mode to transmit mode to transmit a packet [1].

Power Supply

Power is the important component of sensor node. The lifetime of the sensor node depends on the power and lifetime of the sensor network depends on the sensor node. Sensor node needs power in data processing, communication and sensing. Most of the power is used in communication. The power cost of transmitting data of 1Kb over a distance of 100 meters (330 ft) is just about the same as that used for the execution of 3 million instructions by a 100 million instructions per second/W processor.The sources of providing power to sensor nodes are many but they are classified into three categories [6]: store energy on the node (i.e. a battery), distribute power to the node (i.e. a wire), and scavenge/search available ambient power at the node (i.e. a solar cell). Energy reservoirs are: macro-scale batteries, micro-scale batteries, micro-fuel cells, micro heat engines, and radioactive power sources. Under power distribution category, Electromagnetic (RF) Power Distribution and Wires, Acoustic, Light, etc. For power scavenge, Photovoltaic (Solar cells), Temperature gradients, Human power, Wind / air flow and vibrations.

Memory

Memory in current sensor nodes is grouped under three categories [7]: RAM (for fast data storage), internal flash (for code storage), EEPROM (for data storage), and external flash which is required for data persistence. Flash memories are used because of their cost and storage capacity.

Sensor Nodes

Sensor node is the hardware which responds to an environment changes. Basically three types of sensors are there [18]: passive, Omni-directional sensors; passive, narrow-beam sensors; and active sensors. The size of a sensor node may be small or may be large, it depends on the applications. Sensor node covers a definite area up to which it senses the objects.

Features of Sensor Networks which make it distinguishable from other Ad Hoc Networks:

The important features of sensor networks which distinguish WSN from the ad hoc networks are [2]:

i. The order of magnitude of number of sensor nodes in WSN is higher than that of the ad hoc networks.
ii. Sensor nodes in WSN are closely deployed.
iii. Sensor nodes in the sensor networks are more prone to failures/attacks.
iv. The topology in sensor network changes very repetitively.
v. Sensor nodes generally use broadcast communication standards whereas nearly all ad hoc networks use point-to-point communications.
vi. Sensor nodes have memory constraint, computational capacities constraint and power constraint.
vii. WSN uses the data centric approach whereas traditional networks uses address centric approach.
viii. WSN stresses more on power management.

The WSNs are used for the research purpose in agriculture [8], underground communications [9] [10], underwater communications [11] [12], wireless multimedia [13] [14] and in mobile WSN [15].

II. APPLICATIONS OF WSN

Wireless sensor networks are used everywhere. Sensor networks are used in tracking and monitoring. We can record the movements of moving vehicles and wildlife habitats. A Radio Frequency Identification (RFID) technology is used in tracking the animals. The applications of Wireless sensor networks [16]are shown in fig.3.

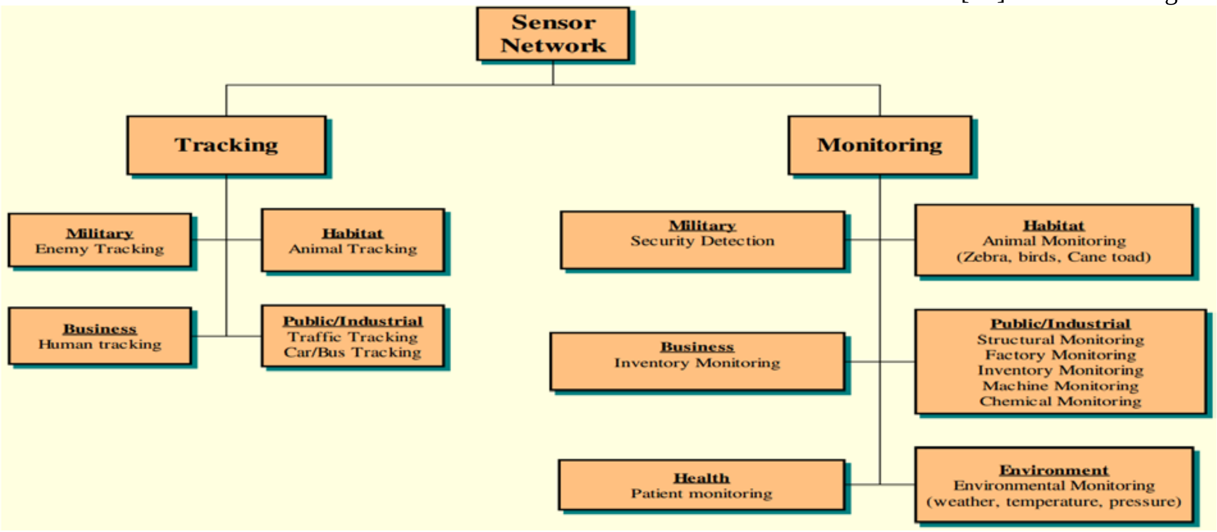

Figure 3: Applications of WSN

III. NETWORK CHARACTERISTICS, OBJECTIVES AND CHALLENGES

- Network Characteristics:
  As compared to the Mobile Ad hoc Network (MANET) and cellular systems, wireless sensor networks have some exceptional characteristics and constraints.
- Network Design Objectives:
  Many of the sensor networks are application specific and they have different application requirements. Thus, we have to keep in mind certain design objectives while designing any network system.
- Network Design Challenges and Routing Issues:
  As WSN has limited energy, bandwidth, central processing unit and storage, it's challenging to design routing protocols for WSN.

The table 1 shows the network characteristics, objectives and design issues [17].

Table 1: Network Design Issues

S.NO.	Network Characteristics	Network Design Objectives	Design Challenges And Issues
1	Dense sensor node deployment	Small node size	Limited energy capacity
2	Battery-powered sensor nodes	Low node cost	Sensor locations
3	Severe energy, computation, and storage constraints	Low power consumption	Limited hardware resources
4	Self-configurable	Scalability	Massive and random node deployment
5	Unreliable sensor nodes	Reliability	Network characteristics and unreliable environment
6	Data redundancy	Self-configurability	Data Aggregation
7	Application specific	Adaptability	Diverse sensing application requirements
8	Many-to-one traffic pattern	Channel utilization	Scalability
9	Frequent topology change	Fault tolerance	
10		Security	
11		QoS support	

IV. SECURITY IN WIRELESS SENSOR NETWORKS

Security is important for these types of networks and security issues is more challenging task for MANETs than those in traditional wired computer networks and the Internet. When we provide security to sensor networks, it is more complicated than that of MANET because of the resource limitations of sensor nodes. Sensor networks actively monitor their surroundings, and infer information. Moreover, the sensor networks also facilitate eavesdropping and packet injection by an adversary. By keeping these factors in mind, sensor networks demand security at design time to ensure secrecy of our credentials, operation safety, and privacy for people in sensor environment [20].Significant amount of research and considerable efforts have been done to improve security levels of wireless networks.

There are primary security goals for WSN:

- ***Confidentiality:*** Confidentiality ensures the concealment of the message from an attacker so that any message communicated via the sensor network remains confidential [19]. Sensor identities and keys are public and these should be secured using cryptography to ensure the data confidentiality[21]. Since public key cryptography is too resource demanding for commodity sensors, we can use symmetric key encryption (e.g. DES,AES) and ashared secret key between the communicating partiesto achieve confidentiality[22]. Information should encrypt to protect from traffic analysis attack [23].
- ***Integrity****:* Integrity ensures the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while transmitting on the network [19]. The integrity of the network sacrifices when a malicious node (insider node) injects false data, and secondly when unstable conditions due to wireless channel cause damage or loss of data[24].
- ***Authentication:*** Authentication ensures the reliability of the message by identifying its origin i.e. who sends the message. After authentication, we can easily grant limited resources to the nodes or reveal information to authenticated nodes [19]. Data integrity and sensor authentication are essential security requirements in most sensor applications. MAC and digital signature are the most common approaches to provide data authentication[22].
- ***Availability*:** Availability ensures the services of resources offered by the network, or by a single sensor node must be available whenever required or we can say it ensures the availability of the nodes while communication [19].Availability of the nodes can be secured by protecting the sensor nodes from idle listening or unnecessary processing to save energy of sensor nodes [21].

The secondary security goals for WSN are:

- ***Data Freshness:*** Sensor networks are data-centric as they have to collect the data from an environment and the property that arises from this fact is freshness [25]. Data freshness means that the data is recent (or fresh), and it ensures thatno old messages have been send as adversary can jam the network by sending same data multiple times through the network nodes in order to deplete the energy of sensor nodes so as to sensor network [21]. This requirement is important where sensor nodes use shared keys for communication. The obsolete information will cause problems to the applications deployed in the network. An example of this problem is the wormhole attack in WSNs[26]. Countermeasures of this problem are Key establishment, ensures session freshness and a nonce, or another time related counter, can be incorporated into the packet to ensure data freshness [24].

- ***Self-Organization:*** Another property of sensor networks is self-organization: sensor nodes are independent and flexible enough to organize and heal themselves according to situation[25]. WSN has no fixed infrastructure; nodes are randomly deployed in the environment. They must also be self-organize to perform key management and building trust relation among sensors. A number of key pre-distribution schemes have been planned in the context of symmetric encryption [26]. WSN is reliable in nature i.e. if any node becomes damage, then new node will substitute the damaged node through self-organizing mechanism [21].
- ***Time Synchronization:*** Sensor networks depend on some form of time synchronization mechanisms. One way to save the energy is turned off the sensor's radio regularly [21]. End-to-end delay of packet is also calculated by the sensor nodes. Group synchronization is required by collaborative sensor networks for tracking applications, multi-hop sender-receiver (means nodes are not single-hop range),offers a set of secure synchronization protocols for sender-receiver (pair wise) and group synchronization [21].
- ***Secure Localization:*** WSN uses the location based information to locate the nodes [23]. Wireless sensor network are mainly designed to find out the faults in the network and for this they need accurate information so that they can pinpoint the location of the fault [24].If the network is non-secured then unfortunately an attacker can easily manipulate the information by reporting false signal strengths, replaying old messages and signals [24]. This is one of the most important factor during implantation of security in the network [23].

Taxonomy Of Attacks In Sensor Networks

Wireless networks are more prone to security attacks due to their broadcast nature of the transmission medium as compared to wired networks. The one factor of this vulnerability is that nodes are deployed in very hostile and unfriendly environment where they are not physically protected.It is very difficult to monitor and protect individual node from the physical and logical attacks in the large-scale networks. Attackers can deploy various types of security attacks to hinder the security of WSNs [20].

In WSN, there are so many attacks on each layer of protocol stack. Most of them severely affect the operations of network layer and they are: Sybil attack, sinkhole attack, wormhole, cloning, eavesdropping and many more. There are so many classifications of security attacks, the author is explaining one of those classification and is known as layer-based classification [20]:

A. Based On the Capability of the Attacker

- ***Outsider versus insider (Node Compromise)attacks:***

  Some papers refer these attacks as External and Internal attacks. Outsider attacks are carried out by the nodes which do not belong to a network (WSN). External or outsider attacks cause passive eavesdropping on data transmissions and can inject spurious data into the network in order to consume network resources and launch denial of service (DoS) attack [26]. Insider or internal attacks occur when genuine nodes of a WSN behave as an unintended or unlawful way [12].Internal attacks are more dangerous when compared with external attacks as the insider attacks know important and secret information, and they possessed privileged access rights [27].

  The attacks of WSN are classified as shown in fig. 4.
- ***Passive versus active attacks:***

  Passive attacks are mostly launched against data confidentiality. An attacker continuously sensing unencrypted traffic to collect sensitive information from the network so that it can be used to launch some severe attacks. Examples of Passive attacks are traffic analysis, decrypting weakly encrypted traffic, capturing authentication information and monitoring communications. Passive attacks are launched just to see the future actions of the network. Aftermath of this attack is revelation of information and other data files without any e of the user [28]. In contrast to active attacks, here the attacker is not passive buttakes some major actions to take control over the network. In active attacks, some type of modifications of the data steam and making of a false stream have been done. Examples of active attacks are jamming, DoS, fabrication, modification of data, wormhole, black hole, sinkhole, replay, spoofing, man-in-middle attack, flooding, overwhelm, Hello flood, selective forwarding, node subversion, lack of cooperation, modification, etc. [28].
- ***Mote-class versus laptop-class attacks**:*

  In mote-class attacks, an attacker uses a few nodes with same capability to attack a WSN [20].In laptop-class attacks, an attacker uses some powerful devices (e.g. laptop) to attack a WSN [20], because these devices have superior transmission range, more energy reserves and more processing power than the network nodes.

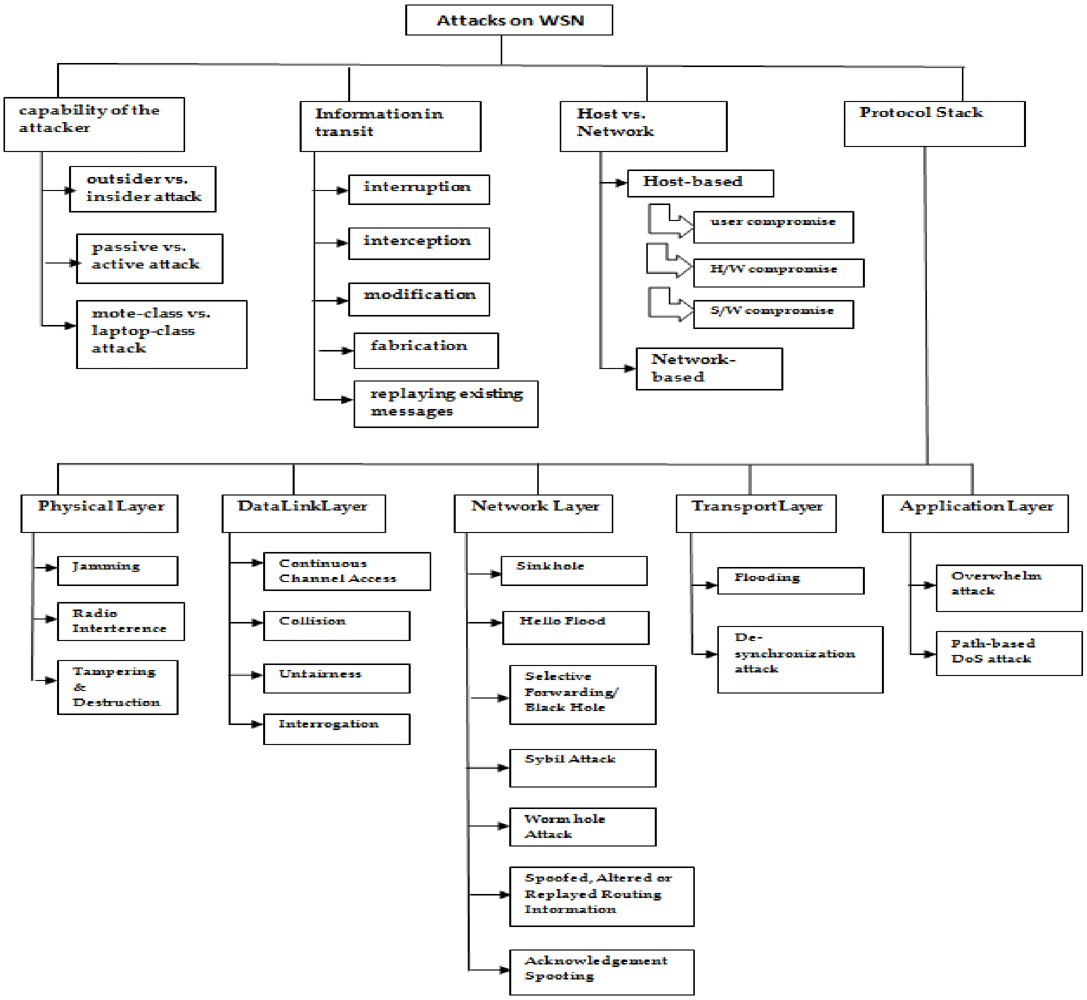

Figure 4: Taxonomy of Attacks

B. *Attacks on Information in Transit*

In a sensor network, sensors are used to examine the behavior of surroundings and report them to the sink according to the situation. While sending the report, it may be possible that the information intransit is attacked by the attackers and sends bogus information to the base stations or sinks. Pfleeger [29] has recognized four classes of security in computing systems as shown in fig. 5. The attacks are:

- ***Interruption***: In interruption, communication link in the network becomes vanished or occupied. Service availability becomes affected by this operation. Examples of this sort of threats are node capture, message corruption, addition of malicious code etc. [30]. The main purpose of this attack is to raise Denial-of-Service (DoS) attack. If layer-specific viewpoint has considered, then this type of operation launched at all layers of OSI model [20].
- ***Interception***: In interception, an attacker takes control over the sensor network and gains unauthorized access either to the network nodes or to the data. Node capture is one of the examples of Interception attack. Message confidentiality has been affected by this operation [20]. The main purpose of this operation is to eavesdrop on the information carried in the messages. If layer-specific viewpoint has considered then this operations usually launched at the application layer.
- ***Modification****:* In modification, unauthorized parties not only got access on the data but also tampers with it. Message integrity has been affected by this operation. This is usually launched at the network layer and the application layer, because of the very rich semantics of these layers [20].
- ***Fabrication:*** Fabrication means injection of false data stream to the network which results into the loss of trustworthiness of information. Message authenticity gets threatens by this operation [20]. Fabrication helps DOS attacks by flooding the network.
- ***Replaying existing messages***: This operation threatens message freshness by sending old messages again and again.

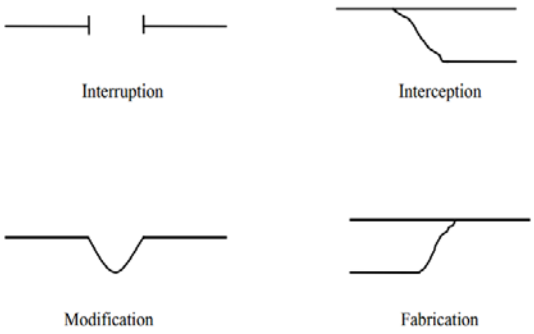

Fig.5 Pfleeger's four classes of system security threats

C. Host Based Vs Network Based

- ***Host-based attacks:***

  It is further classified into three attacks [20]:

  User compromise*:* In this operation, users of WSN are compromised. Users are cheated to reveal sensitive information of the network e.g. passwords or keys about the sensor nodes.

  Hardware compromise: This operation tampers the hardware in order to take out the program code, data and keys stored within a sensor node's hardware. Not only this, the attacker also tries to implement its program code to the compromised node.

  Software compromise: This operation breaks the software which is running on the sensor nodes. These software are more susceptible to popular attacks i.e. buffer overflows.

- ***Network-based attacks:***

  Network based attacks are launched on the information in transit. It also deviates the protocol from its pre-planned functioning. When the attacker is an insider of the network, but the attacker's intention is not to intimidate the service availability, integrity, message confidentiality and authenticity of the network, it only gains an undue advantage for itself in the usage of the network so that it can uses the information in future for his purpose, the attacker manifests selfish behaviors, behaviors that deviate from the planned functioning of the protocol.

D. Based On Protocol Stack

This section explains the WSN layer wise attacks.

a. Physical Layer

- ***Jamming:*** This is basically a Denial of Service (DoS)attack in which an attacker interrupt the successful operation of the network by continuously sending the high energy signals to the network to keep the network busy. Jamming is tremendously successful against single channel networks, because all nodes transmits in small band with single wireless spectrum [35]. For the protection against this attack, we use spread-spectrum techniques for radio communication.
- ***Radio interference:*** In this attack, an attacker either produces large amounts of interference irregularly or steadily. Solution of this attack is to use of symmetric key algorithms [20]. By using these algorithms the revelation of the keys is postponed by some time interval.
- ***Tampering or destruction*****:** Due to unattended and dispersed nature of the Wireless sensor networks, the nodes are more prone to physical attacks [26]. Given physical access to a node, an attacker gets the crucial information such as cryptographic keys, passwords or other data on the node, they can interfere (tamper) the node's circuitry, they alter the program codes or replace it with a malicious sensor [26]. One solution to this attack is tamper-proofing [20] the node's physical package. Tamper-proofing is also called Self-Destruction and is when somebody tries to access the sensor nodes physically the nodes vaporize their memory contents and this prevents any leakage of information, i.e. sensor node destroys its own contents.

b. Data Link Layer

- ***Continuous Channel Access (Exhaustion):*** An attacker interrupts the Media Access Control protocol, by continuously requesting for data or transmitting irrelevant information over the channel so as to make it occupied for itself. This action leads to starvation for other nodes in the network that are waiting for the channel access [26]. Defense against this attack is time division multiplexing.
- ***Collision:*** This attack is similar to the continuous channel attack. A collision occurs when two or more nodes try to send on the same frequency simultaneously. When packets have a collision, a change will occur in the data portion, which causes a checksum mismatch at the receiving end. The packet will then be discarded as invalid. Defense against this attack is using error-correcting codes [20].
- ***Unfairness:*** This attack is due to the repetitive usage of the exhaustion or collision based MAC layer attacks or an unpleasant use of cooperative MAC layer priority mechanisms. This kind of attack can be a partial DoS attack, but it results in trivial performance degradation [20]. Only defensive measure against these attacks is the usage of small frames, so that any individual node can occupy the channel for a smaller period only [26].
- ***Interrogation:*** Interrogation attack initiates Exhaustion. A compromised sensor node could constantly transmit RTS (Request to Send) packets in order to develop CTS (Clear to Send) packets from an uncompromised neighbor, finally draining the battery power of both nodes [35]. First measure against thistype of attack is, a node can bound itself in accepting connections from same identity and second is, node can use strong link-layer authentication and anti-replay protection [20].

c. Network Layer

- ***Sinkhole:*** A Sinkhole attack attracts almost all the traffic towards the compromised node, and other nodes think this is the trustworthy node and creating a symbolic sinkhole with the adversary at the center [20]. Sinkhole attack is very difficult to stop because routing information supplied by a sinkhole node is difficult to verify. As an example, a laptop-class adversary has a high power transmission range that provides a high-quality route so as to reach a wide area of the network [31]. Opposite to sinkhole attacks Geo-routing protocols are there, because localized information is used to construct the topology for geo-routing protocols. The model of sink hole attack [25] is shown in fig. 6:

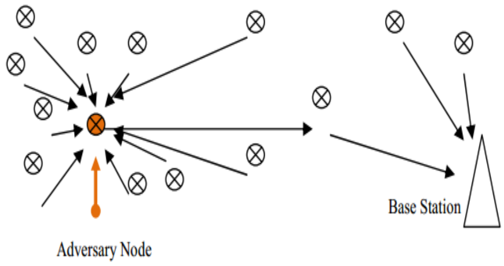

Fig.6 Model of Sinkhole Attack

- ***Hello Flood:*** Hello flood attack uses the Hello packets which are commonly used in every communication to publicize nodes to their neighbors. When a node receives such packets it assumes that node is in its radio range. In laptop-class attack, an adversary sends these packets to all sensor nodes in the network so that they consider the compromised node belongs to their neighbors. This results into a large number of nodes sending packets to this unreal neighbor. There is one solution to these types of attacks is Authentication. Such attacks can easily be avoided by confirm bi-directionality of a link before taking action based on the information received over that link. The model of Hello flood attack [32] is shown in fig. 7:

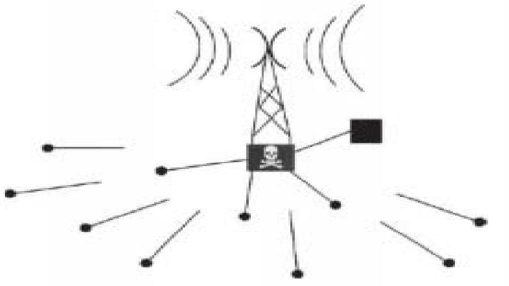

Figure 7: Hello flood attack

- ***Node Capture:*** It is analyzed that only a single node capture is enough for an attacker to control the entire network. The solution to this problem would constitute a groundbreaking work in WSN.
- ***Selective Forwarding/ Black Hole Attack (Neglect and Greed):***WSNs are multi-hop networks and based on the theory that the participating nodes will forward the messages loyally. Malicious nodes can decline to route some messages and sometime drops them. If nodes selectively forward the packets, then it is called Selective Forwarding, and if node drops all the packets through them, then it is said to be Black Hole Attack. The countermeasure of this attack is to use Multi path routing combined with random selection of paths to destination, or braided paths can be used that signify paths which have no common link or which do not have two successive common nodes, or use implicit acknowledgments, which ensures that packets are forwarded as they were sent[20]. The model of Hello flood attack [33] is shown in fig. 8:

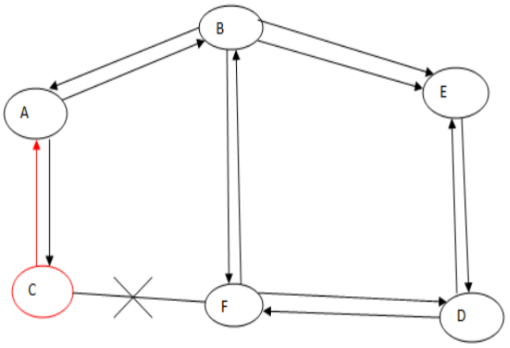

Fig.8 Model of Black Hole Problem

- ***Sybil Attack:*** Sybil attack can be defined as a malicious device illegally taking on multiple identities and adversary can act to be in many places at the same time. In other words, a single node which shows multiple identities to other nodes in the sensor network either by fabricating or stealing the identities of authorized or legal nodes is called Sybil node [26]. By showing multiple identities to all other nodes this may mislead genuine nodes of the network. Sybil attack tries to corrupt the integrity of data, resource utilization and security that the distributed algorithm attempts to accomplish [37]. To overcome this attack, unique shared symmetric key for each node with the base station is used [20]. The model of Sybil Attack [34] is shown in fig. 9:

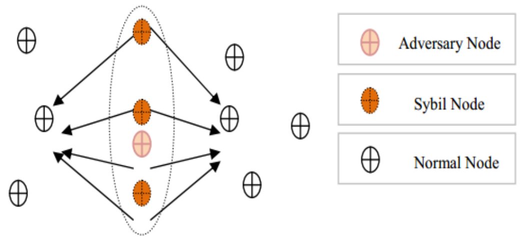

Fig.9 Model of sybil attack

- ***Wormhole Attacks:*** An adversary can tunnel messages received in one part of the network and replay them in another part of the network. This is generally implemented with the organization of two adversary nodes, where the nodes try to compute their distance from each other. To overcome this attack, the traffic is routed to the base station along a geographically shortest path, or which uses very tight time synchronization among the nodes (it’s infeasible in practical environments). First node sends a packet directly to another node through a tunnel in the same network over a high speed private wireless link or wired link. These packets are then resent from that node’s location into the network. The tunnel which exists between two nasty nodes is called as wormhole. This attack can easily be launched against communications that remedy to authenticity and confidentiality. Fig.10 shows the Wormhole attack. Node S2 and Node S9 are not directly connected to each other. Node S9 sends messages to Node S2 through tunnel called Wormhole tunnel. There are two points in this attack; origin point and destination point9.

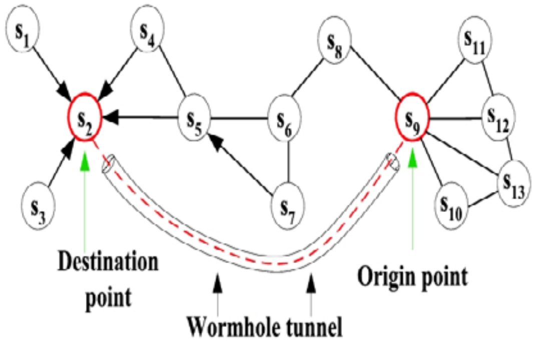

Fig.10 Model of Worm Hole attack

- ***Spoofed, Altered, or Replayed Routing Information***:When attackers directly target the routing information when it is in transit, then this type of attack is said to be False Routing Information [35]. The false information allows an intruder to attract or repel traffic, create routing loops, shorten or extend route lengths, increase latency, and even partition the network, as shown in fig. 11. An attacker may spoof, alter, or replay routing information in order to interrupt traffic in the network. The countermeasure of this attack is to append a Message Authentication Code (MAC) with message. Efficient encryption and authentication techniques are also used as countermeasure of spoofing attacks.

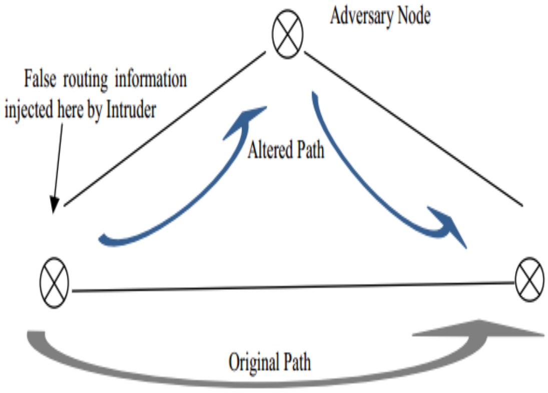

Fig.11 Redirecting traffic through an adversary node via False Routing Information attack

- ***Acknowledgment Spoofing:***Sometimes routing algorithms used in sensor networks need Acknowledgements. An attacking node can spoof the Acknowledgments of overheard packets that are destined for neighboring nodes to provide fake information to those neighboring nodes. The most common solution to this problem is authentication via encryption of all sent packets and also packet headers.
- ***Misdirection:***This is a more active attack in which an attacker node present in the routing path and can send the data packets in wrong direction which spawns the destination unreachable problem. Instead of sending the packets to correct direction an attacker misdirects those packets to the victimized nodes. If it gets observed that a node's network link is getting flooded with an irrelevant information then the victim node's active state is switched to sleep mode for some time to overcome this.
- ***Internet Smurf Attack:*** In this type of attack an adversary floods the network link of victim node. In this attack, an attacker forges the victim's address and broadcasts it in the network and also routes all the replies to the victim node. By doing this an attacker floods the network link of the victim node. For this attack, solution is same as that for misdirection attack.

d. Transport Layer

- ***Flooding:***An attacker may continuously make new connection requests until the resources required by each connection are exhausted or reach upper limit. It produces severe resource constraints problem for legitimate nodes. One proposed countermeasure to this problem is to require that each connecting node demonstrate its commitment to the connection. And second may option may be that a limit can be set on the number of connections from a legitimate node.
- ***De-synchronization Attacks:***It tries to disturb the present connection [38]. In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence, these messages are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information. This will cause a considerable drainage of energy of legitimate nodes in the network in an endless synchronization-recovery protocol. A possible solution to this type of attack is to require authentication of all packets including control fields communicated between hosts. Header or full packet authentication can defeat such an attack.

e. Application Layer

- ***Overwhelm attack:***An attacker tries to overwhelm network nodes with sensor stimuli, so that network forwards the large volumes of traffic to a base station. This attack consumes network bandwidth and decreases the node's energy.
- ***Path-based DOS attack:*** In this attack, attacker injects spurious or replayed packets into the network at leaf nodes which causes starvation of the network traffic. It consumes resources on the path to the base station and thus preventing other nodes from sending data to the base station.

V. CONCLUSION

In recent years, WSN has gained remarkable attention leading to inimitable challenges and design issues when compared to traditional wired networks. In the future, the wide range of application areas mentioned above will make sensor networks a vital part of our lives. In this paper we discussed the architecture of wireless sensor network and wireless sensor node. Each and every component of sensor node had been discussed above. Our paper discussed one of the classification of security attacks. Then each attack is discussed with their countermeasures. Security issue remains a challenge in wireless networks for researchers. Though countermeasure are there for each attack, even then an attacker maliciously takes an undue advantage for itself.

REFERENCES

[1] K. Maraiya, K. Kant and N. Gupta, “Application based Study on Wireless Sensor Network”, International Journal of Computer Applications, Vol. 21, No.8, May 2011.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “Wireless sensor networks: a survey”, Elsevier, Computer Networks 38, pp. 393–422, 2002.

[3] J. N. Al-Karaki and A. E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey”, this research was supported in part by the ICUBE initiative of Iowa State University, Ames, IA 50011.

[4] A. Ranjan and S. K. Gupta, “Localization System for Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 5, Issue 1, January 2015.

[5] Y. Xu, J. Heidemann and D. Estrin, “Geography-informed Energy Conservation for Ad Hoc Routing”, Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking(ACM Mobicom), July 16-21, 2001, Rome, Italy.

[6] S. Roundy, D. Steingart, L. Frechette, P. Wright and Jan Rabaey, “Power Sources for Wireless Sensor Networks”.

[7] M. Pathak, “An Approach to Memory management in Wireless Sensor Networks”, International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229-3345, Vol. 4 No. 08 Aug 2013, pp: 1171-1176.

[8] X. Yu , P. Wu, W. Han and Z. Zhang, “The research of an advanced wireless sensor networks for agriculture”, African Journal of Agricultural Research, OI:10.5897/AJARX11.067, ISSN 1991-637X, Academic Journals, Vol. 7(5), 5 February, 2012, pp. 851-858.

[9] E. P. Stuntebeck, D. Pompili and T. Melodia, “Wireless Underground Sensor Networks using Commodity Terrestrial Motes”, 1-4244-0732-X/06, 2006 IEEE, pp. 112-114.

[10] I. F. Akyildiz and E. P. Stuntebeck, “Wireless underground sensor networks: Research challenges”, Elsevier, Science Direct, Ad Hoc Networks 4 (2006) pp. 669–686.

[11] I. F. Akyildiz, D. Pompili and T. Melodia, “Underwater acoustic sensor networks: research challenges”, Elsevier, Science Direct, Ad Hoc Networks 3 (2005) pp.257–279.

[12] J. Heidemann, M. Stojanovic and M. Zorzi, “Underwater sensor networks: pplications, advances and challenges”, Phil. Trans. R. Soc. A (2012) 370, doi:10.1098/rsta.2011.0214, pp.158–175.

[13] I. F. Akyildiz, T. Melodia and K. R. Chowdhury, et al., “Wireless Multimedia Sensor Networks: Applications and Testbeds”, Proceedings of the IEEE, Vol. 96, No. 10, October 2008.

[14] I.F. Akyildiz,T. Melodia and K. R. Chowdhury “A survey on wireless multimedia sensor networks”, Elsevier, Science Direct, Computer Networks 51 (2007), pp.921–960.

[15] J. Rezazadeh, M. Moradi and A. S. Ismail, “Mobile Wireless Sensor Networks Overview”, International Journal of Computer Communications and Networks (IJCCN), Volume 2, Issue 1, February 2012.

[16] K. Sohraby, D. Minoli and T. Znati, “WIRELESS SENSOR NETWORKS Technology, Protocols, and Applications”, 2007 by John Wiley & Sons, Inc. Publication.

[17] S. K. Singh, M. P. Singh and D. K. Singh, “Routing Protocols in Wireless Sensor Networks – A Survey”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.

[18] Wikipedia.

[19] G. Sharma, S. Bala, and A. K. Verma, "Security Frameworks for Wireless Sensor Networks-Review", in Proc. 2nd International Conference on Communication, Computing & Security [ICCCS-2012], Elsevier, pp. 978 – 987, 2012.

[20] T. Kavitha and D. Sridharan, "Security Vulnerabilities in Wireless Sensor Networks: A Survey", Journal of Information Assurance and Security, pp. 031-044, May 2010.

[21] L. kaur and J. Malhotra, "Review on Security Issues and Attacks in Wireless SensorNetworks", International Journal of Future Generation Communication and Networking Vol. 8, No. 4 (2015), pp. 81 -88.

[22] Y. Ren, V. Oleshchuk, F.Y. Li and X. Ge, "Security in Mobile Wireless Sensor Networks - A Survey", Journal of Communications, vol. 6, no. 2, April 2011.

[23] R. W. Anwar, M. Bakhtiari, A. Zainal, A. Hanan Abdullah and K. N. Qureshi, "Security Issues and Attacks in Wireless Sensor Network", World Applied Sciences Journal 30 (10), 2014.

[24] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[25] J. Lopez, R. Roman, and C. Alcaraz, "Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks", in Proc. International Conference FOSAD 2009, Springer-Verlag Berlin Heidelberg , pp. 289–338, 2009.

[26] M. Chowdhury, M. F.Kader and Asaduzzaman, " Security Issues in Wireless Sensor Networks: A Survey", International Journal of Future Generation Communication and Networking, Vol.6, No.5 (2013), pp.97-116.

[27] T. G. LUPU, "Main Types of Attacks in Wireless Sensor Networks", Recent Advances in Signals and Systems, pp. 180-185.

[28] K. CHELLI, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", in Proc. World Congress on Engineering, 2015, Vol I.

[29] C.P. Fleeger, Security in computing, 3rd edition, Prentice-Hall Inc. NJ. 2003.

[30] T. Zia and A. Zomaya, "Security Issues in Wireless Sensor Networks", in Proc. IEEE, International conference on Systems and Networks Communications 2006.

[31] M. M Patel and A. Aggarwal, " Security Attacks in Wireless Sensor Networks: A Survey", in Proc. IEEE, International Conference on Intelligent Systems and Signal Processing (ISSP) - 2013, pp. 329-333.

[32] S. Magotra and K. Kumar, "Detection of HELLO flood Attack on LEACH Protocol", in Proc. IEEE International Advance Computing Conference (IACC), 2014, pp. 193-198.

[33] Pooja and V. Kumar, "A Review on Detection of Blackhole Attack Techniques in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Iss. 4, April 2014, pp. 364-368.

[34] D. Martins and H. Guyennet, " Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", in Proc. IEEE 13th International Conference on Network-Based Information Systems, 2010, pp. 313-320.

[35] D. Juneja, A. Sharma and A.K. Sharma, " Wireless Sensor Network Security Research and Challenges: A Backdrop", in Proc. International Conference HPAGC 2011, Springer-Verlag Berlin Heidelberg 2011, pp. 406-416.

[36] X. Huang, D. Sharma, and M. Ahmed, " Security Computing for the Resiliency of Protecting from Internal Attacks in Distributed Wireless Sensor Networks", in Proc. International Conference ICAPP 2012, Part I, Springer-Verlag Berlin Heidelberg 2012, pp. 16-29.

[37] A. S. K. Pathan, H. W. Lee and C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges", in Proc. IEEE, 8th International Conference Advance Communication Technology, pp. 1043-1048.

[38] S.Lalar , S. Jhangra and S. Bhushan, Study of Attacks & Countermeasures on Layers of Wireless Sensor Networks, International Journal of Control Theory and Applications, 2017; 10(15): 153-162