Volume 6, Issue 2, February 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Risks in Wireless Sensor Networks and the Remedial Measures to Deal with Such Threats

Hebziba Jeba Rani. S*

PG Scholar, SNS College of Technology,
Tamilnadu, India

Abstract*— In recent years of wireless environment, the development and research of wireless sensor networks plays a major impact because of its tremendous and vital applications. Wireless sensor network senses the environment and sends the sensitive information to the destination. The sensitive and time critical information need to be monitored periodically to track the progress of the products in the industries and also for saving human life from natural calamities. Not only in industries and for life saving but also in military, medical field, weather monitoring, forest monitoring widely utilizes the benefits of the wireless sensor networks. Thus all of these time critical sensitive data cannot be monitored solely by the human since it is not possible to accurately monitor the environment periodically and also more manpower is needed. Thus the deployment of the wireless sensor network is becoming an unavoidable and most necessity need in recent years. Since the sensed data is propagated through the air medium in the wireless environment, the capture of the sensed data by the unauthorized nodes in the path of the transmission is also increasing. Even though security mechanisms are already imposed in the network, the attackers are coming up with the new tactics to steal the confidential data. Thus the security mechanisms need to concentrated more to compete with the attackers. To provide additional security to the already available security mechanisms, the attacks and the prevention techniques that are so far available need to be known. This paper thus deals with the various possible attacks that may occur in the wireless sensor network and the countermeasures that can be taken to overcome such attacks.

Keywords*— wireless sensor network, applications, security, attacks, countermeasures.

I. INTRODUCTION

Wireless sensor network (WSN) is a type of network which is specially used for monitoring or sensing the environment. Thus WSN consists of the nodes having the capability to monitor the environment, processing the sensed data and communicating the data with other nodes. Such a type of node in the network is called as the sensor nodes. Thus the sensor node consists of the processor, transceiver, memory, power source and sensors [10]. The functionality of the processor in the sensor node is to schedule the tasks that are coming to it and to process the scheduled data. There are various types of processors that can be utilized in a sensor node. They are microcontroller, digital signal processor (DSP), integrated circuits etc. The basic block diagram of WSN is show in Fig. 1. Among the various available processors, the one that is widely deployed in the sensor environment is the microcontroller. It is because microcontroller is considered to the flexible and cheap one. The transceiver is a device which is used to send and receive the data to and from the other devices. The transceiver can perform any of the following tasks like send, receive, idle and sleep. Without the transceiver the sensed data cannot be forwarded or received to and from other nodes. The memory plays a vital role in sensor networks. It is because the sensed data need to be stored somewhere before transmitting it. Only then the scheduling and the processing tasks that are to be carried out in the sensor node can be made. Thus memory needed for the functioning of the sensor node may be in-chip flash memory, RAM of the microcontroller, external flash memory. To perform all of the functioning, power source is needed. Without the power, it is not even possible to switch on the sensor node. Thus power source is required in sensor network. The power which is needed for communicating the sensed data is much higher than the power which is needed for sensing and processing of the data. Power can thus be stored in batteries or capacitors. Batteries are manly used in the sensor network but batteries are limited in its capacity. Thus there is also a necessary need to utilize the power in efficient way due to the limited capacity of the batteries. Thus recently several researches are going on to improve the power issues in the wireless sensor networks. One of the techniques which were proposed was the utilization of energy harvesting techniques. Energy harvesting also called power harvesting or energy scavenging in which energy is utilized from the external sources like solar power, thermal energy, wind energy etc. finally the sensors in the sensor node makes the sensor node a meaningful one. It is because sensors are the ones which perform the root task of sensing or monitoring the environment. The sensors sense the analog signal from the environment and the sensed analog data is then converted to digital signal using analog-to-digital converter. And the digitized data is then sent to the processor for further processing of the data [9].

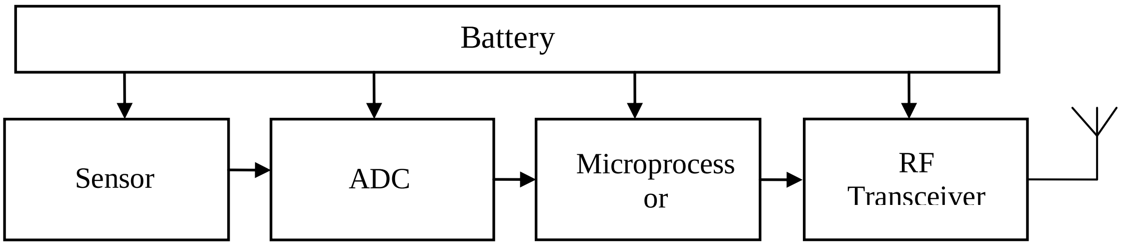

Fig. 1 Basic Block Diagram of Wireless Sensor Network

II. APPLICATIONS OF WIRELESS SENSOR NETWORKS

Wireless sensor networks applications are not limited to particular fields. It is widely used in numerous applications from home monitoring to military applications. Wireless sensor networks provide timely data to the intended parties regarding the status of the environment or other aspects. Thus in case of receiving abnormal data, the countermeasures can be taken at a timely manner to avoid unacceptable damages and life threatening issues. Thus the various places where the wireless sensor networks can be deployed are summarized as follows [11]:

- **Agricultural applications:** Agriculture is the main source of income for many countries. Wireless sensor networks can be deployed in the agriculture fields to monitor the conditions like nutrient content in the soil, humidity level, temperature level, amount of weeds present in a particular area, water quality and several other factors. These factors are to be monitored periodically to improve the productivity of the agriculture. Even though these factors can be monitored by the farmers itself, the changing conditions in the field cannot be monitored every second manually which results in inaccurate results about the field. Thus the sensors can be utilized in the farming fields to improve monitoring and to improve the productivity. This in turn leads to better standard of living of the farmers.
- **Disaster Monitoring:** wireless sensor networks are deployed mainly in areas where natural calamities may occur. Wireless sensor networks provide very useful applications in disaster monitoring. For example forest fire monitoring, earthquake detection, fire accident detection in industries and in other buildings, landslide detection, machine health monitoring, heart rate monitoring among patients, rising of sea level detection etc.
- **Smart home monitoring:** Recently smart home systems are widely being implemented in many areas. Smart home system works mainly using the application of sensors. In smart home system intruders can be detected by placing the sensors in the door. The sensors may sense the finger print of the person and processing of the data is done to compare the finger print of the owners with the finger print of the other people opening the door. If any unauthorized person tries to open the door, the alarm system gets activated. Also automatic switching on and off of the home appliances can also be done using the sensors monitoring the temperature of the room or the sensor sensing the movement of the person in the room. Automatic switching on and off of the motor when water level of the tank exceeds or goes beyond the limit. Similarly several other sensors can be placed in the home to make our home a smart home.
- **Industrial monitoring:** wireless sensor networks have its wide applications in industries also. In industries sensors can be placed in particular machinery region to monitor the number of products that are going out of that particular machine, number of defect products from a machine. Sensors can also be placed to monitor the temperature produced by a particular machine. There may be a case that when a machine produces a temperature above certain threshold then fire accident may occur due to the explosion of the machine. Such time critical and sensitive data regarding the fire thus need to be monitored periodically. In such as case wireless sensor networks help to monitor and provide information regarding such critical environmental conditions. Also to sense the data regarding people entering the industry, people leaving the industry, people entering the restricted area of the industry can be done using wireless sensor networks [12].
- **Military applications:** The wireless sensor network came into existence due to the various needs in military applications like intruder detection. The border of the country is needed to be monitored keenly to avoid illegal people entering the country. If detected timely about the illegal entering of people in the country, countermeasures can be taken immediately to avoid them harming the country. Thus sensors in the border areas play a major role in protecting our country. Also the military people can use the sensors to find their troop. The vehicles entering and leaving the region can be sensed.
- **Health care monitoring:** In hospitals sensors can be used to detect the health of the patients like heart beat rate, body temperature, position of the patients body while sleeping, location of the person etc. the sensors can be used in either way among the patients. One of the ways to place sensors is through wearable devices. In wearable equipment the sensor can be fitted to monitor the status of the patient's body. The other way to monitor the health of the patient is through the implants. Implant refers to placing the sensors inside the human body.
- **Smart cities:** Recently smart city concept is being undertaken by the nations to improve the standard of the country by deploying digital technologies to improve the performance of the urban services and so the citizens can utilize the digitized services easily and effectively. The smart city concept mainly utilizes the sensors that are it utilizes the sensor network for deploying the smart city concept. Smart city project utilizes the sensors for the following [14]
  a. Monitoring the parking space.
  b. Monitoring the vibrations and materials in bridges and buildings.
  c. Noise monitoring in hospitals and in other centric zones of the city.
  d. Monitoring the energy radiated by the mobile stations and routers.

e. Monitoring the environment conditions (weather) automatic on and off of the street lights.
f. Monitoring the vehicles for the traffic congestion, monitor the garbage level in the containers and so the trash collection can be made without any delay and so the city can be kept clean.
g. The climatic conditions can be sensed and based on the sensed data, the warning messages and the diversion details can be given along the road side to avoid accidents that may occur due to sudden change in the climate like the fog deposition, heavy rain etc.
h. Landslides, earthquakes, snow level, forest fires can be monitored.
i. The sensor can be used to monitor the emission levels of CO2 from the factories and vehicles and so measure can be taken to reduce such emission if emissions go beyond the limit which in turn reduces the air pollution..
j. Sensors can be used to monitor about the leakages like chemicals and waste into the rivers.
k. The swimming pool conditions can be monitored and controlled through sensors
l. Sensors can be used for intrusion detection in industries, ATMs, BANKs, and Hospitals etc
m. The ultraviolet radiations can be sensed and the sensed data can be processed to find the acceptable level of UV rays and warnings can be given to people if UV rays level goes beyond the limit regarding not to get exposed in the sun during these hours
n. In hospitals and old age homes the sensors can be used to monitor the patients
o. The signs of the sportsmen can be monitored in the fields to protect the health of sportsmen
p. Sensors can be used to monitor the environment and based on the sensed data automatic switching on and off of the appliances can be done for energy saving.

III. REQUIREMENT FOR SECURITY IN WIRELESS SENSOR NETWORK

Wireless sensor network monitors not only data like temperature, vibration, pressure which does not require much security but also senses some confidential data like the number of products produced from a machine which needs to kept secret from the competing parties, in military applications and in government applications the sensed data need to be transmitted in secured way to protect the nation from illegal people. Thus security also plays a major role in wireless sensor networks [17] [15]. Thus the most important security requirements or the goals are listed below.

A. Data Confidentiality

Confidentiality refers to hiding of the data from the unauthorized users. Only the sender and the receiver should be able to view the message. Apart from the sender and receiver, during the transmission path the data should not be viewed by the intermediate nodes which are referred to as the confidentiality. Thus to achieve the confidentiality, the data and the keys need to be encrypted before the transmission. The attackers in the transmission path may try to access the confidential data through their tactics. The data should be concealed in such a way that it should not be able to unlock by the attackers in the path. Thus the data is said to highly confidential if the data is strictly locked and it is very difficult and time consuming activity for the attackers to unlock the confidential data locked inside strict security mechanisms. Thus in wireless sensor network, the sensors should not reveal the content of the data to the neighbours.

B. Data Integrity

Data Integrity refers to the reliability of the data. Thus Data integrity refers to the trust that the data has not been altered, modified or false data has been added. Even though if data confidentiality measures are taken in wireless sensor networks to protect the data against the attackers, the attacker on receiving the confidential data may not be able to view the actual contents of the sensed data due to the deployment of confidentiality mechanisms, the attackers can still add some false data into the existing data or modify the existing data. Thus simply providing confidentiality doesn’t mean the data is fully secured. The attackers may inject some false contents in the data and forward the malicious content. Thus it is necessary that the data must have integrity mechanisms that the unauthorized users must not be able to add or modify the contents of the data.

C. Data Authentication

Data authentication refers to the reliability of the message which is achieved by identifying the identity of the sender and the receiver. This authentication can be achieved through the symmetric and asymmetric mechanisms. In symmetric mechanism, the sender and the receiver shares a key containing the information which is needed to encrypt and decrypt the message. Thus the key is need is needed to unlock the message. But once if the key is captured by the intruders then the intruders can easily decrypt and encrypt the message. The wireless sensor networks where the broadcasting of data is done the key may get heard by the blackhats due to the broadcast nature of the signal. Thus asymmetric mechanism can be used where two keys are used for authentication. One of the keys is the secret key which is kept private and the other one is the public key which is distributed to the neighbours. Both of the keys are mathematically linked. The private key is utilized by the sender and kept private. Thus no others in the network can have the private key except the sender. The sender utilizes the private key to encrypt the data. This data can be decrypted using the public key. Thus the receiver on receiving the locked data uses the public key to unlock it. If the data is being decrypted by the attacker using the public key, the attacker may not be able to encrypt again because the attacker cannot get the private key. If the attacker sends the data without encryption, the receiver can easily identify it since the data is not being locked or his public key doesn’t work. In this way the authentication can be achieved in such environments.

D. Data Availability

Even though security mechanisms are employed to protect the sensed data, the data need to be available only then it can reach the destination. The secured data will be of no use if the data becomes unavailable. The data will become unavailable if the node is not having the enough power to transmit the data or if the base station fails to perform its tasks. If the node or a base station thus suffers from any failure may lead to the inability to transmit the data leading to the unavailability of data. Also the attackers try to make the data unavailable through dropping of the received data. Additionally the security mechanisms which are deployed in the wireless sensor network may drain more battery power from the nodes thus making the nodes unavailable to forward the sensed data. Thus availability should also be considered as a major factor in wireless sensor networks.

E. Data Freshness

In wireless sensor networks, the applications include the major use in the real time applications like the temperature monitoring. Water level monitoring, intrusion detection etc. these data need to be transmitted to the destination without any delay. Only then the countermeasures can be taken in a timely manner to gain fruitful results out of the deployment of wireless sensor environment. For example consider a scenario where the sensors are deployed to monitor the temperature of a machine. If the temperature crosses the threshold of upper limit then the machine may get exploded due to the hike in temperature. Thus this sensitive data need to be transmitted to the controller room (receiver) without any delay. Sending the time critical data after long time will be of no use and also leads to loss of life due to delay in receiving the packet. That is in short the data need to be fresh at the receiver only then timely counter measures can be taken in response to the received data. If the data gets aged, it may of no use in receiving such old packets. Thus the old packets need to be dropped then and there to avoid the traffic and to avoid receiving of the useless packets. Thus the timestamp can be fixed in each packet to fix the lifetime of the packet. Only then unnecessary old packets will be no where revolving in the network and it will be dropped when the time to live expires.

F. Time Synchronization

In Wireless sensor networks time synchronization plays a major role for the applications that require accurate mapping between the time in which the event has occurred and the time in which the event is captured. For example consider the application of tracking location of the mobile node, when the mobile node that is to be tracked reaches the particular sensor node, the node sensing such node needs to have time synchronization scheme. The node monitoring the location and the time in which the mobile node passes that sensor node need to be transmitted to the aggregator. The aggregator on receiving this time and location information from different sensors placed at different locations, fuses received information to predict the path in which the mobile node is moving. Thus the time synchronization is needed to get the accurate time and path in which the mobile node is passing. Is improperly synchronized the actual and the estimated data will show major deviations and so sensed data will be of no use. Hence time synchronization plays a major role in wireless sensor environment [16].

G. Self-Organization

Wireless sensor network is similar to adhoc network consisting of the independent nodes without fixed infrastructure. The nodes in the sensor network act independently and flexibly to the different situations in the network. There is no infrastructure to perform the network management activities. Thus because of this, the security in wireless sensor network is a major challenging task. Hence the self organizing should be incorporated in the sensor network to handle the mobility and the attacking in the wireless sensor networks. The lack of the self organization may lead to dropping of packets, security issues in the sensed data, damage to the sensed data and thus may lead to failure in achieving the benefits of the wireless sensor network.

H. Secure Localization

Sensor network requires the nodes to find the location of sensor nodes. The location of the sensor nodes need to be known so that while aggregating the data from different nodes, the location information can be utilized and also when the location information are known it will become an easy task to pinpoint the node from where it is suspected to spread the malicious contents. But the location information has to kept and transmitted secretly else the attacker may use tactics like reporting false signal strength to manipulate the non secured location information.

IV. WIRELESS SENSOR NETWORK ATTACKS

Wireless Sensor Networks are vulnerable to various types of attacks due to the broadcast nature of the wireless environment. There are some of the major attacks that may occur in the wireless sensor networks. They are Attacks on Secrecy and authentication, Attacks on network availability, Attack against integrity. The attack against the secrecy and the authentication can be prevented using the cryptographic techniques. Thus cryptographic techniques can be used to protect the secrecy and the authentication against outside attackers like eavesdropping attacks, packet replay attacks, spoofing or the modification of the packets. Attacks on the availability of wireless sensor network are often represented as the Denial of Service Attack (DoS). It is because the availability attacks are mainly done to jam the transfer the sensed data that is to deny services so that the data will never receive any services from the nodes leading to unavailability. Finally the integrity attack refers to imposing false data into the sensed data. In this case the attacker tries to compromise a sensor node and through the compromised sensor node, the attacker tries to inject the false information into the sensed data [17].

V. ATTACKS IN DIFFERENT LAYERS

Wireless sensor Network uses the layered architecture like the wired architecture. [10].The layers are physical layer, data link layer, network layer, Transport layer, Application layer.

A. Attacks in physical layer

The physical layer is responsible for the signal detection, channel selection, carrier frequency generation, modulation, encryption, data rate etc. The major types of attacks that may occur in physical layer are jamming and tampering.

1) Jamming: Jamming attacks are mainly performed to degrade the performance of the network. To degrade the performance of the network, the intruders (jammers) generate high power noise across the network. Thus depending on the power capacity of the jammers, the jammers may perform full or partial degradation of the network. The jamming attack example is shown in Fig. 2. The jammers with the very limited power also disrupt the network through distributing the jammers.

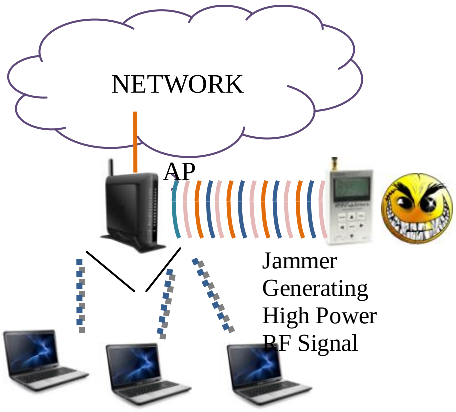

Fig. 2 Example of Jamming Attack

Countermeasures: Spread spectrum can be used to tackle the jamming attack in the physical layer. In frequency hopping spread spectrum, the nodes changes the frequency required for transmission. Changing of the frequencies for the transmission of a data will be protecting against the jamming attack since the jammer will be unsure regarding in which frequency the data is getting transmitted. If the attacker tries to jam a wide range of frequencies, this may be very effective. Thus code spreading can be used to defend against the jammers but still this technique cannot be employed in wireless sensor network. It is because every extra frequency requires additional processing. But code spreading can be used in mobile networks to protect against jamming.

2) Tampering: Tampering refers to compromising a node. The compromising of a node is done by an unauthorized node called attacker or intruder. Fig. 3 shows the presence of a compromised node in the network. Wireless sensors networks are not deployed in a secured room but the wireless sensor network is widely deployed in the areas like open environment, in buildings where more number of people will be coming and going and also in the surroundings of the buildings. Thus the sensor node may be reached by anyone who is passing through those sensor nodes. The intruder may try to get physical access to the sensor node and the attacker tries to capture the keys that are used to perform cryptographic techniques. The intruders may even try to replace the programmed chip inside the sensor node to make the sensor node act according to the needs of the intruder or the intruder may totally replace the trusted sensor node with the malicious sensor node.

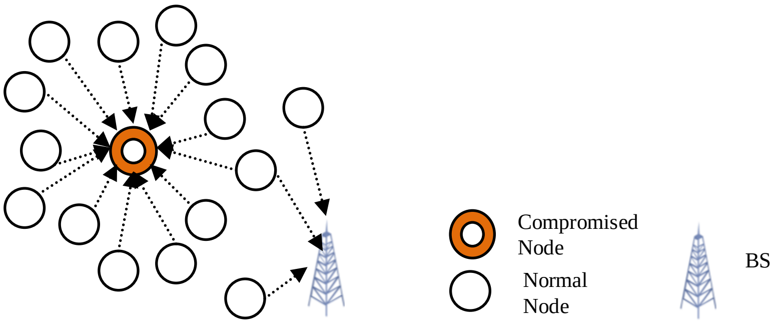

Fig. 3 Compromised node in the Network

Countermeasures: To protect the node against tampering, the nodes should be protected inside the protectors i.e. the tamper proofing technique should be used in the nodes to avoid unauthorized tampering. But in wireless sensor networks, the tamper proofing cannot be to all the nodes due to the increased cost.

B. Attacks in Link layer

The data link layer performs operations like multiplexing of the data streams, Medium Access Control, error control etc. Attackers in this data link layer may try to create collisions, exhausting the resources.

1) Collisions: The attackers or the intruders intentionally create the collision by continuously transmitting the messages. When more number of messages is transmitted over a particular channel continuously, then the packets collide with each other. Thus when two nodes attempt to use the same frequency at the same time, the packets from those two may collide with each other resulting in the packet becoming invalid. The packet may become invalid due to the change in the checksums which are caused due to collisions. Such change in the data makes the receiver to drop the packets as invalid (e.g. mismatching of checksum). Some packets may get lost in the transmission path itself due to collision. Thus retransmissions will be done which leads to further collisions. In some cases, the attacker may concentrate only on specific type of packets like the ACK packet. In such cases the ACK messages will not reach the sender thus sender retransmits the same packet again and again without the knowing about the attacker's tactics. This scenario may lead to costly exponential back off [18]. Countermeasures: TDMA scheme can be used to overcome collisions.

2) Exhaustion of the Resources in the network: If the attacker performs repeated collisions intentionally i.e. if the attacker attempts to generate the useless messages continuously, then the legitimate user packets may get severely lost leading to lots of retransmissions. Retransmissions take place if the acknowledgment packets get dropped. This scenario may lead to the wastage of the power which in turn leads to the degradation of the resources.

Countermeasures: Limitations can be made in the data rate to avoid resource exhaustion.

C. Attacks in Network layer

The network layer is responsible for routing the data from the source node to the destination node. The nodes may be located close to each other or may be located in different networks. The network layer also performs the route selection from the available multiple paths for the transmission of data between the end parties. The network layer also concentrates on saving the power. Thus the network layer utilizes SMECN (Small Minimum Energy Communication Network) and LEACH (Low Energy Adaptive Clustering Hierarchy) protocol for the above purpose [11]. The following are the possible attacks that occur in the network layer.

1) Spoofing attack: Spoofing attack generally refers to the attacking activity where the attacker presents themselves as like trusted or authorized node in the network. The attacker presents their false information to present themselves as like authorized node in the network. This tactics is to perform the malicious activities like stealing of data, spreading of unnecessary noisy data, modification in the data, etc.

In the network layer, the attackers may perform spoofing attack on the routing information. In this attack, the attackers target on the information related to the routing that is transmitted across the network. They may perform illegal activities like changing the routes, generating false error messages to increase the traffic, intentionally increasing the end-to-end delay, creating loops in the network.

Countermeasures: authentication technique can be used. Only the valid routing information need to be accepted by the routers.

2) Selective Forwarding Attack (Greyhole attack): In wireless networks the data is forwarded to the destination through the multiple hops if the destination is far from the source. The data is transmitted based on the belief that each node in the network will forward the packets. But the attackers in the network may resist forwarding some of the packets and may transmit only some kind of packets. The attackers won't explicitly present themselves as an intruder and blocks the forwarding of packets but they try to compromise a node in the network to fool the other nodes as like it is a trusted node. Once the attacker compromises a node in the network, the attacker utilizes that node to perform their attack.

In selective forwarding attack, the attacker forwards the incoming packets selectively. That is not all the packets that are arriving to the attacker are forwarded but only some packets are forwarded while the remaining packets are dropped by the attacker. This attack is similar to the black hole attack. In the black hole attack, the attacker drops all of the incoming packets to it. But in selective forwarding only the selected packets are forwarded and remaining are dropped [19].

Countermeasures: multipath routing technique can be used to avoid the packet loss due to this attack. The activities of the nodes can be monitored and is any of the node shows any misbehaving activities like selective forwarding then timely measure can be taken like eliminating the compromised node from the network.

3) Black hole attack: In black hole attack, the attacker first attempts to place itself in a network and tries to present itself as the node through which shortest path is achieved. Thus majority of the traffic uses this attacker assuming it as the node in the shortest path is achieved [11].

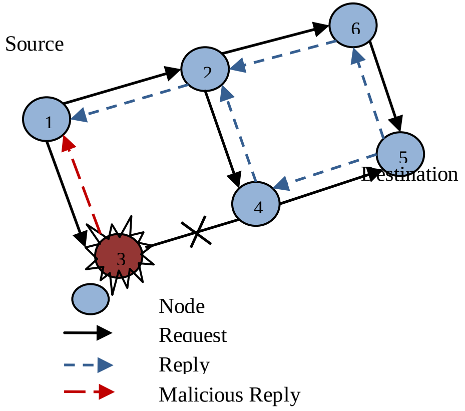

Fig. 4 Black hole attacker not forwarding the packets

The attacker node on receiving the packets from its neighbours, never forward the packets but simply drops it which is shown in the Fig. 4. As like its name “black hole”, this attacker acts like a hole in the network. The packet once gets locked inside this black hole will never get forwarded. Through this attack, the intruder tries to disconnect the communication between the parties [19].

Countermeasures: to prevent the blackhole attackers entering the network, the network should be setup in a secured way thus making difficult for the intruders to participate in the network communication.

4) Sinkhole attack: sinkhole attack, the attacker attempts to compromise a central node which is in the central location which forwards majority of the packets from many nodes. After compromising a node, the attacker uses the compromised node to fool the other nodes in the network. The attacker makes changes in the routing information which makes the other nodes to choose the compromised node for routing. Once the attacker succeeds in attracting the other nodes for forwarding the data, the compromised node can be used to do the intruding activities like the selective forwarding, dropping of packets and so on. In many situations the attackers chooses the place near the base station to place the sinkhole. It is because only then the sinkhole attacker can fool the nodes as like it is the destination base station.

Countermeasures: the attacker finds it very difficult to accomplish this attack if the neighbouring nodes use the unique key to initialize frequency hopping or spread spectrum communication.

5) Wormhole attack: In wormhole attack, the attacker tries to convince the receiving node that its parent node sending the message is the attacker itself. But the actual parent of the message may be somewhere far away from the receiving node [6]. For example consider a case that node ‘A’ wants to broadcast some route request message to its neighbours. The attacker being one of the neighbours of node ‘A’ captures this route request packet and replays the same message as like the packet is directly coming from node ‘A’. Consider node ‘Z’ is far from node ‘A’ that multiple hop is required between them. The attacker’s replayed message is received by node ‘Z’ as node ‘Z’ is one of the neighbours of attacker. Now the node ‘Z’ assumes that the packet from node ‘A’ is received directly from node ‘A’ through single hop. But the message has directly come from attacker not from node ‘A’. In this way the node ‘Z’ assumes the attacker as its parent which is one hop reachable to it. The above example is shown in Fig. 5. This type of attack is referred to as the wormhole attack [11] [10].

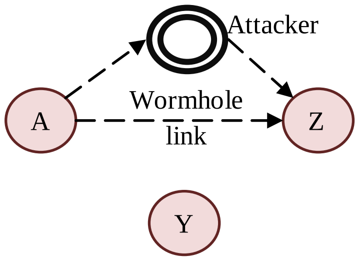

Fig. 5 Attacker convincing it as Parent Node

If the sender and the receiver are one hop distance reachable from the attacker which is in between the end parties, the above scenario happens. But when the sender and the receiver are placed faraway i.e. for example between different networks, a single attacker cannot become an intermediary between source and destination. In such a case at least two wormhole attackers are needed to perform this attack. When the end parties are at different networks, one attacker may reside near the source and the other attacker may reside near the destination and the communication between these two attackers happen via a strong link. Thus the sender’s packets reach the attacker which is near to it and the attacker replays the message to the attacker which is residing near the destination in other network. The attacker on the other end (at receiver side) captures the message from the sender attacker and replays the message to the destination node. Thus through the wormhole attack, the attackers make the end parties to transmit their data in the wormhole link without the knowledge of the sender and the receiver [18]. The wormhole link is shown in the Fig. 6.

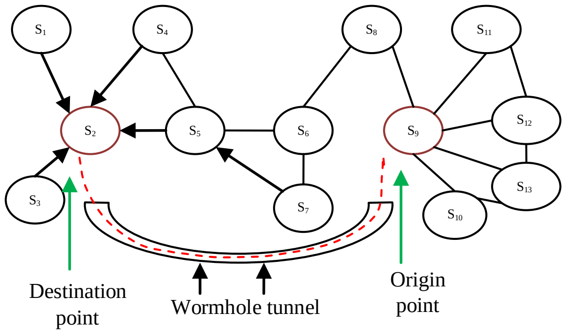

Fig. 6 Attackers creating the wormhole tunnel between source and destination

Countermeasures: Geographic based routing protocols can be used to find the shortest path between the source and destination instead of relying on the neighbour nodes. In geographic based routing protocols, the shortest path is found using the geographic distance.

6) Sybil attack: In this attack, the attacker steals the identity of the other nodes and presents itself as like multiple nodes. This setup is shown in the Fig. 7. By creating multiple fake identities in the network, the attacker tries to degrade the network performance through unnecessary usage of the resources. In distributed applications the work is subdivided and done by multiple nodes. In such situations the Sybil attacker uses multiple IDs to attract the systems that use distributed processing.

Countermeasures: Random key pre distribution technique can be used to overcome this attack. Thus each and every sensor node will have their key apart from their unique ID. Thus both the ID and the key can be used to uniquely identify a node. So even if the attacker steals the legitimate node’s identity, without the key they cannot act like a legitimate node.

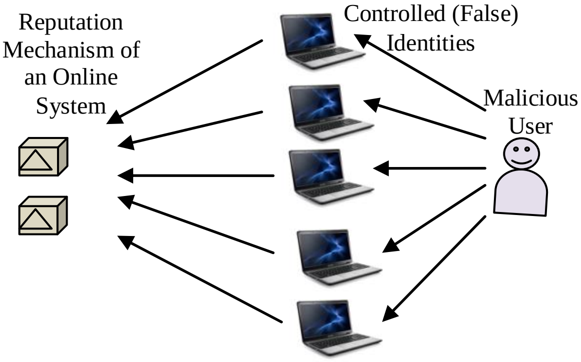
Reputation Mechanism of an Online System
Controlled (False) Identities
Malicious User

Fig. 7 Malicious node with false identities

7) Hello flood attack: protocols in the network utilize the HELLO packet for the neighbour discovery. So when a node transmits its HELLO packet, the neighbour node on the reception of the HELLO packets, comes to know that the sender of the HELLO packet is in its radio range and so the sender node can be used for the packet forwarding. The attacker uses this technique to fool the legitimate users. The attackers intentionally create the HELLO packets and broadcast the packets in the network. Thus the legitimate nodes on receiving this HELLO packet may use the sender of the HELLO packets (attacker) for their data transmission without knowing that the sender is an attacker. This type of attracting the legitimate users using HELLO packets is called Hello flood attack [11]. The attacker uses more power to transmit their HELLO packets only then the HELLO packets will be received my more number of nodes. This technique also creates congestion in the network.

Countermeasures: Authenticated broadcast protocols can be used to prevent this attack.

8) Acknowledgment spoofing: In this attack, the attacker overhears the transmission between the end parties. On hearing the acknowledgment packets, the attacker may capture it and send false data to the nodes. In this way the exact status about the nodes are not transmitted. The attacker changes the Acknowledgment data and transmits false status about the nodes [20].

Countermeasures: To overcome this type of attack, effective encryption techniques need to be employed. Also the authentication mechanisms should also be deployed effectively.

D. Transport layer attacks

Transport layer is responsible for managing the end to end connections. The transport layer also performs the connectivity of the wireless sensor network with the internet [10]. The attacks that can be done in the transport layer in wireless sensor networks are the flooding attack and de-synchronization attack.

1) Flooding attack: In the flooding attack, the attackers repeatedly flood the connection request message to the nodes until the resources will become unavailable and the further request message gets denied. This type of attack is mainly done to disrupt the normal transmissions.

Countermeasures: To overcome this attack, if the number of incoming connection requests packet from a node is limited, this may affect the legitimate nodes sending the requests.

2) De-synchronization attack: In this attack, the attacker tries to spoof the messages to the end host causing the host to request for retransmissions of the missed data. Thus the end hosts will be continuously trying to recover from the errors which were actually never existed. Thus the normal data exchange gets collapsed.

Countermeasures: One possible way to overcome this attack is to authenticate all the packets that are transmitted between the sensor nodes in the network.

E. Application layer attacks

The application layer is responsible for collecting the data, managing the data and processing the data using the application software. The application layer thus helps in presenting the information and in forwarding the request from the application layer to the lower layers. The attack that can occur here is related to the attacks on reliability [11].

Countermeasures: attacks on the reliability can be overcome using the cryptographic techniques.

VI. CONCLUSION

The wireless sensor networks are recently emerging in many fields due to its contribution to the mankind. Wireless sensor networks helps in many fields like early disaster warning using the sensors which monitor various signs in the environment, monitoring the status of the product produced in industry, patients health monitoring, Monitoring of the country borders, forest monitoring etc. Thus sensor networks are deployed in sensitive areas which focus on the real time secured data. Securing the data in WSN is a major role since it carries critical data. Thus the types of threatens that can come into the wireless sensor networks need to be analyzed first for enhancing the security in the wireless sensor environment. Thus this paper focused on the various possible attacks that can occur in the wireless sensor network with respect to the layers and the possible countermeasures that can be taken to prevent such attacks.

REFERENCES

[1] Ju Ren, Yaoxue Zhang, Kuan Zhang, Sherman Shen, "Adaptive and Channel-aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks", IEEE Transactions on Wireless Communications, Issue. 99, February 2016.

[2] Kyung-Ah Shim, "A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks", IEEE Transactions on Communications Surveys and Tutorials, Vol. 18, Issue. 1, pp. 577-601, July 2015.

[3] Jun Wu, Kaoru Ota, Mianxiong Dong, Chunxiao Li, "A Hierarchical Security Framework for Defending against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities", IEEE Early Access Articles, Issue. 99, January 2016.

[4] Vittorio P.Illiano,Emil C.Lupu, "Detecting Malicious Data Injections in Event Detection Wireless Sensor Networks", IEEE Transactions on Network and Service Management, Vol. 12, Issue. 3, pp. 496-510, June 2015.

[5] Mai Abdelhakim, Leonard E. Lightfoot, Jian Ren, Tongtong Li, "Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, Issue. 4, pp. 950-959, February 2014.

[6] Sounak Paul, Bimal Kumar Mishra, "Honeypot based signature generation for defense against polymorphic worm attacks in networks", IEEE International Conference on Advance Computing Conference (IACC), pp. 159-163, February 2013.

[7] Blilat.A, Bouayad.A, El Houda Chaoui.N, Ghazi.M.E, "Wireless sensor network: Security challenges", IEEE Conference on Network Security and Systems, pp 68-72, April 2012.

[8] Martins.D, Guyennet.H, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", IEEE International Conference on Network-Based Information Systems (NBiS), pp 313-320, September 2010.

[9] Jun Zheng, Abbas Jamalipour, "Introduction to Wireless Sensor Networks", IEEE Press eBook Wireless Sensor Networks: A Networking Perspective, pp. 1-18, 2009

[10] Dr.Banta Singh Jangra, Vijeta Kumawat "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 3, September 2012.

[11] Usham Robinchandra Singh, Sudipta Roy, Herojit Mutum, " A Survey on Wireless Sensor Network Security and its Countermeasures: An Overview", International Journal of Engineering Science Invention (IJESI), Volume 2, Issue 9, PP 19-37, September 2013.

[12] Basma M. Mohammad El-Basioni, Sherine M. Abd El-kader, Mahmoud Abdelmonim Fakhreldin, "Smart Home Design using Wireless Sensor Network and Biometric Technologies", International Journal of Application or Innovation in Engineering and Management (IJAIEM), Volume 2, Issue 3, pp 213-229, March 2013.

[13] D.G.Anand, Dr.H.G.Chandrkanth, Dr.M.N.Giriprasad, "Security threats and issues in wireless sensor networks", International Journal of Engineering Research and Applications (IJERA), volume 2, Issue 1, pp 911-916, Jan-Feb 2012

[14] http://www.libelium.com/top_50_iot_sensor_applications_ranking/

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

[16] Prakash Ranganathan, Kendall Nygard , "Time Synchronization in Wireless Sensor Networks: A Survey", International Journal of UbiComp (IJU), volume 1, No 2, pp 92-102, April 2010.

[17] Jaydip Sen, "A Survey on Wireless Sensor Network Security", International Journal of Communication Networks and Information Security(IJCNIS), Volume 1, No 2, pp 55-78, pp 55-78, August 2009.

[18] C.K Marigowda, Manjunath Shingadi, "Security Vulnerability Issues in Wireless Sensor Networks: A Short Survey", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Volume 2, Issue 7, pp 2765-2770, July 2013.

[19] Herve Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey"S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[20] S.Raguvaran, "Spoofing attack: Preventing in Wireless Networks", IEEE International Conference on Communications and Signal Processing (ICCSP), pp. 117-121, April 2014.