A SURVEY ON ATTACKES AND SECURITY IN WIRELESS SENSOR NETWORK

Meghana S. Kalburgi[1], Neelakka A. Shirol[2], Bhagyashree S. Nyamagoud[3], Veeresh M. Hiremath[4]
[1,2,3]8th Sem B.E, Dept. of ECE, S .G. Balekundri Institute of Technology,
Belagavi, Karnataka, India
[4]Assistant professor, Dept. of ECE, S .G. Balekundri Institute of Technology,
Belagavi, Karnataka, India
Email: meghanakalburgi139@gmail.com[1], neelushirol03@gmail.com[2],
bhagyashreen111@gmail.com[3], vireshblh@gmail.com[4]

Abstract

Nowadays, wireless sensor networks (WSNs) have widespread applications in the areas of medicine, military etc. It is always important to think on the security of this technology.WSN security is having some scientific and technical challenges. 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. WSNs must be secured to keep an attacker from hindering the delivery of sensor information and from forging sensor information as these networks are build for remote surveillance and unauthorised changes in the sensed data may lead to wrong information to the decision makers. Most existing security schemes require intensive computation and memory, which are considered as limitations in WSNs. This paper gives broad overview on all attacks that can harm to any wireless sensor networking environment like, physical attacks that can affect the functioning of different layers of networking, attacks related to privacy, secrecy and authentication related attacks.

KEYWORDS: Wireless sensor network, Attacks, Security, wormhole, sinkhole

I. Introduction

A Wireless Sensor Network (WSN) is generally formed by number of small sensor nodes. Composed of four main components such as processor and memory (microcontroller), Sender and receiver (transceiver), power supply and sensor along with digital to analog converter (A/D converter). The simplified architecture of a sensor node is depicted in Figure. As human organs such as eye and ear have the ability to sense about surrounding environment, sensor nodes are considered similar to them as they gathers the information about surrounding environment, related to temperature, light, pressure, vibrations, velocity and magnetism.

The architecture of the sensor node is as shown in the figure I, a sensor unit is a device that detects and responds to some type of input from the physical environment. The output is generally a signal that is converted to human readable display at the sensor location or transmitted electronically over a network for reading or further processor. The analog to digital converter (ADC) is a system that converts an analog signal. A processor is the one which takes the input from sensor unit and then send it to the receiver. A transceiver is a combination of transmitter / receiver. The power unit gives power supply to the system.

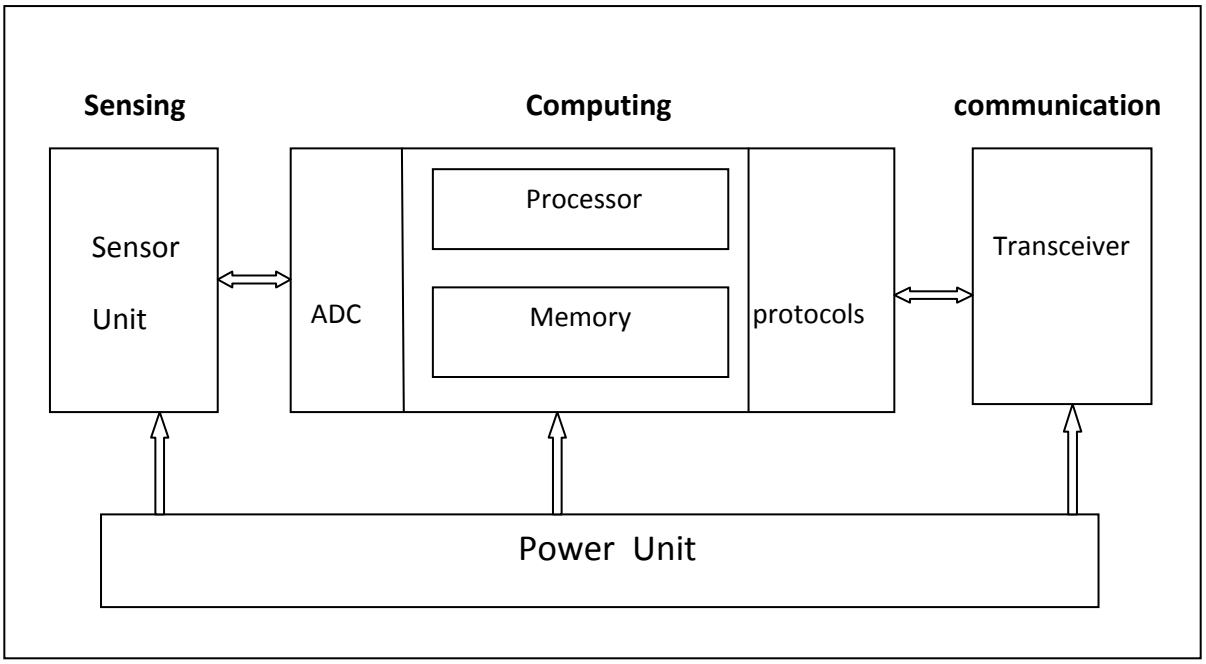

Fig: I Simplified architecture of sensor node

II. ATTACKS IN WIRELESS SENSOR NETWORK

Basically attacks in wireless sensor network can be classified in various ways based on the attacker location, level of damage and attacking devices used [3]. General classification of attacks is given as follows;

A. Outsider verses insider attacks

In outsider attack, Attack is not arranged by network node but external node can be deployed in current network. They are not having access to cryptographic keys or rules as they are not from the network. In insider attack, insider node is compromised due to some weakness in system. Insider attacks can have some partial keys with them and they are having trust of other sensor nodes. Detection of insider attack is more difficult than outsider attack.

B. Passive verses active attacks

Passive attacks are somewhat eavesdropping kind and in this, unauthorised user attack tries to track sense and monitor the communication channel. The active attacks are responsible for major modifications of the data or they can create some false stream of data in a WSN.

C. Physical attack / node capturing attack.

In this, attackers get the full control on all the activities going through sensor node. Attackers capture the node itself by having full physical access, so called physical attack . These attack harm sensors permanently, so the losses cannot be overcome. Tamper proofing is one of the solutions to avoid physical attack but it is irrelevant in WSN.

III. Attacks according to layers of network

These are the attacks that takes place at to affect different layers network such as Physical, Network, Transport and Application layers .This session gives overview of these attacks.

A. Physical Layer Attack

In networking, physical layer has different tasks associated with it. Some of the major task of physical layer includes signal detection, selection of frequency for data transfer, data encryption etc. As WSN is deployed in the remote locations, the attackers have chance to access the physical layer of WSN. Jamming and tampering are some examples of vulnerability of WSN.

a) Jamming:

If the adversaries just have the knowledge about wireless transmission frequency of network then this kind of attack can be done easily by them. The jamming source can be either be a powerfull or less powerfull. Powerfull jamming source is able to create traffic in the entire network, where as less powerfull jamming source is able to disrupt only smaller portion of the network. In this, the attacker tries to transmit radio signal

arbitrarily with the same frequency as that of other sensor nodes in WSN.

B. Link layer attack

Whenever node stops its functioning then this situation is called as node outage. Node outage is harmfull when there is outage of cluster node, at that time protocols should be designed in such way that these will provide some alternate route for transmission of messages.

a) Collision:

Whenever single transmission channel is overloaded by data from different senders at that time there is possibility of collisions. Whenever packets collide there are chances that it can change some data portion and thus destination will not receive data correctly. There can be collision from attacker in some specific packets such as ACK control message. Such kind of collisions can lead to costly exponential back-off in certain media access control (MCA) protocols. Error correcting codes is one of the defense techniques against collision and there are best suited for the collisions that are happening due to environmental errors. Such kind of codes will need additional processing and communicational overhead to overcome the collisions. But, we have to accept the fact that we will not be able to correct more than whatever has been corrupted.

C. Network and routing layer attacks

To improve power efficiency, awareness of location and addressing and to make sensor network more data centric, network and routing layer plays an important role. Major function of network layer is to route messages from one sensor node to another. Attackers can access routing paths to redirect the traffic and provide some wrong information about path to WSN or they can launch Denial-of-service attacks. Some attacks on this layer are as follows:

a) selective forwarding / Black Hole Attack:

In this type of attack, malicious nodes just drops packets that are to be damaged and selectively forwards other non interesting packets.

A black hole attack is one in which, node drops all packets that it receives.

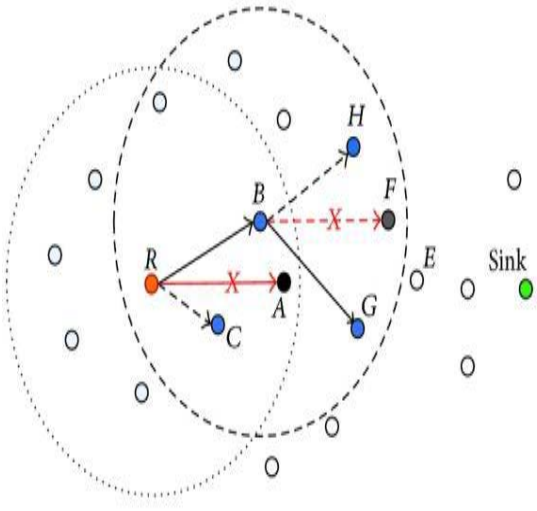

Fig: a) Black hole attack

The black hole ferociousness positions a node in range of the sink and attracts all one traffic to be routed through it by advertising itself as the shortest route. The adversary drops packets coming from specific sources in the network. This violence can allocation apart from pleasurable nodes from the base station and creates a discontinuity in network connectivity.

a) Sybil Attack

Rather than having single identity, if node carries different identities to different nodes. Than it is a Sybil attack. This attack disrupts functioning of geographic routing protocols by being simultaneously at more than one place. In fig () Sybil attack is represented by adversary node AD which carries multiple identities. Here node A looks node AD as node F, node D as node A, so when node A wants to communicate with node F, it sends the message to adversary node AD. To defend from Sybil attack one should verify identity of nodes, but as WSN's have some computational limitations where traditional networks symmetric key and public key algorithm cannot be applied to verify identity in WSN.

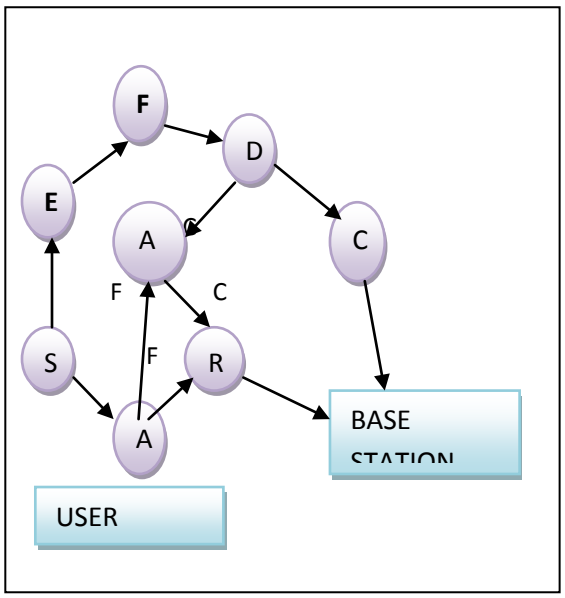

Fig: a) Sybil attack

a) Sinkhole attack

It is a kind of attack in which compromised node looks more attractive and most of the other surrounding nodes try to forward data to this compromised node as next node. This type of attack is also responsible to boost selective forwarding attack as it is going to attract all traffic from large area in network and compromised node can only forward selected packets. In fig() SH denotes sinkhole attack. This sinkhole tries to attract all traffic from near about all the nodes to route through it except nodes N, L and M.

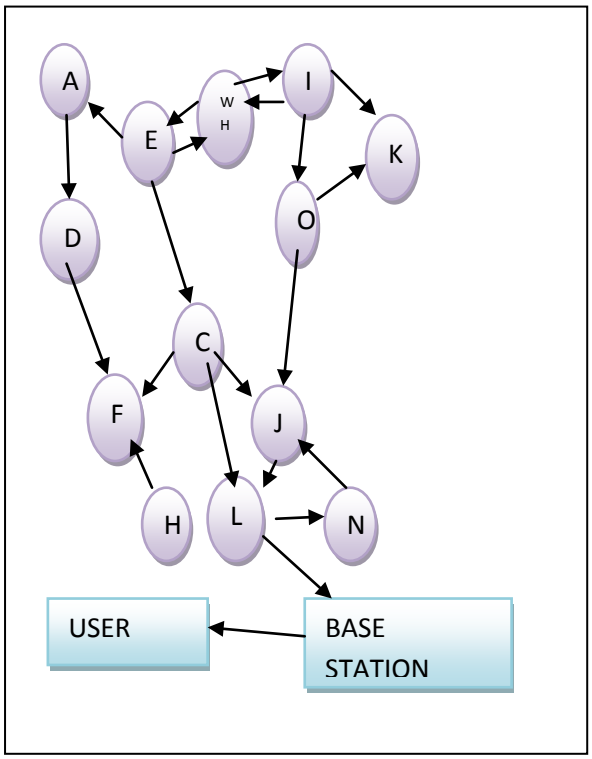

Fig: b) sinkhole attack

b) Worm hole attack

In this, node at one end listens packets and transmits them through the tunnel to node at other end, where the packet are replyed to local area. If these two ends forward messages without any change then it is helpfull to accomplish faster transmission but most of times packets are dropped at end and selective packets are forwarded. As transfer is fast neighbour nodes can fill that these two nodes are neighbour of each other. If any of the tunnel ends is nearer to base station then it can attack a lot of traffic and it can act as sinkhole attack too. Fig() demonstrates a Wormhole attack where WH is adversary node that creates tunnel between nodes E and I. Both sinkhole and wormhole attacks are difficult to detect. When routing protocols route packets based on advertisements on remaining remained or minimum hop count needed to react base station. There some graphic routing protocols that are providing some kind of resilience to these attacks.

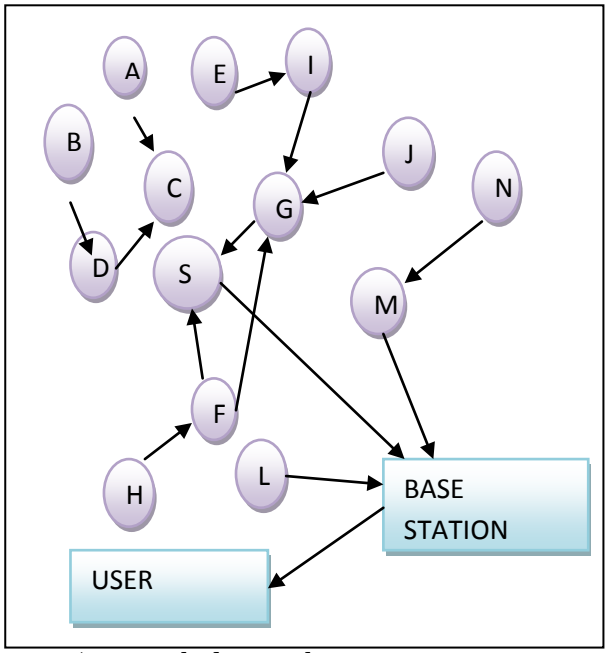

Fig: c) worm hole attack

c) Hello flood attack:

In this attack, attacker sends hello message to all surrounding nodes by using powerfull transmitter due to which all other nodes that are not in radio range think that sender is in radio range. This makes node to send packets to adversary node rather than to base station. Fig() show an adversary node AD which try to show other nodes that it is neighbour of them. There will be wastage of energy and there will be loss of data in this type because

here adversary node will try to pretend other nodes that it is neighbour node, even if that node is far away from those. One partial defence to this attack is to do authentication of such node by some third party.

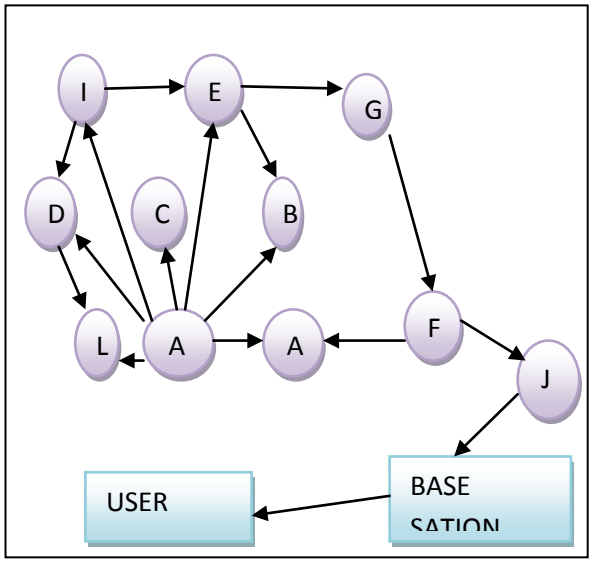

Fig: d) Hello flood attack

D. Transport Layer Attack

Functionally of end-to-end communication between source and destination is generally provided by the transport layer.

Some possible attacks on this layer are discussed below:

a) Flooding

If source node receives many requests repeatedly, then its memory became exhausted through flooding. An attacker requests for new connection continuously till its maximum limit. In this situation sender decline all request including the genuine request of any node in WSN. Thus, attacker can waste resource of WSN and communication between nodes will stop. In this attack many connection establishment requests can be sent by attacker to victim node to use its resources causing flooding attack.

E. Application Layer Attacks

This layer basically collects and manages the data. As information is revealed in this layer it can lead to compromise whole network. Exclusion of node is probable solution in this attack if node gets compromised. LEAP (Localized Encryption and Authentication Protocol) can verify if a node has been compromised or not and if it is compromised then it can revoke that node by some efficient keying mechanism.

IV. Attacks on Secrecy and Authentication

Following are some attacks which can harm cryptographic techniques to explode secrecy of data and authentication of user:

a) Node replication attack

In this attacker tries to have duplicate identity of node by copying identifier of another node. These nodes can distrupt networking by giving wrong information and wrong routes t another node. This can lead to partition the network and it will responsible to communicate false readings of sensor to another nodes. There is always possibility of copying cryptographic keys if attacker gain access to communication channel and these keys can be used by replicate node for communication.

V. Attacks on Privacy

Attackers need not be present to gather information, one remote access is sufficient for them to gather information from multiple sides at single instance. Privacy of sensor node can be disturbed by following types of attacks.

a) Eavesdropping and passive monitoring

It is common attack on data privacy. The adversary could easily understand the contents, if cryptographic mechanism is not used for protecting messages. Most of times, more information is revealed by the packets having control information than information available at location sever.

b) Traffic analysis

Eavesdropping when combined with a traffic analysis, it makes an effective attack on privacy. Due to thorough analysis of traffic for adversary it is possible to understand the roles of nodes. For example unfortunate increase in message communication can make adversaries to understand that there are some events to happen.

VI. Security in Wireless Sensor Network (WSN)

The main security requirements are confidentiality, integrity, availability. WSN's popular due to low cost solution and real world problem solving features. Security is needed to protect the sensitive data during transmission and also for protecting the networks proper functioning.

Security requirements in WSNs are:

- Data confidentiality.
- Data integrity.
- Self organization.
- Data newness.
- Authentication.
- Time synchronisation.
- Secure localization.
- Availability.

Data confidentiality

Data confidentiality protects data so that any unauthorized user cannot read the data and analyze it. Attacker should not know about the frequency of transmission and the content of the data. Data should be received by only the intended receiver. The key distribution should be done in very secret way. The key distribution algorithm should be strong and enough. Secure channel generation is very important. Without permission any near by nodes should not read the content of the nodes.

Data integrity

Data integrity ensures that data is not modified by any unauthorized third party means the data, during transmission from source to destination should not be modified or changed by attacker. Malicious nodes may modify the data. So this tampered data should be transmitted to the actual source. From time to time, data should be verified.

Self- organization

Wireless sensor network is a type of ad-hoc network. Each sensor node is flexible and self organizing. Therefore, applying traditional cryptographic algorithm is difficult. As the sensor nodes behave dynamically, sharing key between nodes is difficult before deployment, if symmetric key is used.

Data newness

In case of symmetric key cryptography, sometimes old data is sent repeatedly, which is termed as replay attack. To overcome this problem, a time specific counter should be added to ensure the freshness of data. With the time specific counter , it is easily detected whether the data is updated or old data is used. If shared key is used. It is mandatory to update data over time.

Data authentication

Authentication ensures that the data is coming from an unauthentic source. It should also ensure that no third party is acting like an authorized user. Receiver should have a scheme to ensure that the received data is coming from the actual user. Data authentication can be done using message authentication code (MAC). MAC is calculated using the message and the shared key.

Data availability

Data availability ensures that the authorized user is not prevented to access service. WSN should always be accessible to legitimate users. To address this problem, one common technique is using extra communication between nodes. Denial-of-service attack results in loss of availability of data.

Time synchronization

The security schemes should be well time synchronized. Time synchronization is a major need in wireless sensor network applications. It needs a critical timing.

Secure localization

Sensor nodes in WSNs should be localized in a secured manner in any environment. If sensor nodes are not secured properly, attacker can deliver false location information and replay messages. Different techniques are there to find the actual location. One of them is id verifiable multi-lateration where the exact location is known from different reference points.

Conclusion

As sensor nodes are deployed in open environment, they are vulnerable to different attacks. So, security of such network is always important aspect. This paper provides

comprehensive survey on attacks and how to provide security in wireless sensor network with respect to different layer of networking. This paper also gives overview on some new attacks that can harm most of trust models in WSN. This survey brings researches and view of all attacks in wireless sensor network while designing any security mechanism at different layer of network.

REFERENCES

1] William stallings, "Cryptography and network security ", Principles and practice. year: 2011.

2] Kamal Soni, Pranjul Mishra, Sonam Various Security Attacks in Wireless Sensor Network: "A Survey" International journal of engineering research and technology (IJERT) ISSN:2278:0181,Vol.3 Issue 4, April -2014

3] Aykut karakaya, Sedatak Akleylek "A survey on security threats and authentication approaches in wireless sensor network" 978-1-5386-3449-3/18/$31.00 2018 IEEE

4] Waleed AI Shehri, "A survey on security in wireless sensor network", International Journal of network security and its applications (IJNSA) Vol.9,No.1, January 2017.

5] Ayman souheil tajeddine, Imad H. Elhajj "Authentication schemes for wireless sensor network", Researchgate, conference paper- April 2014.

6] Rajkumar, Sunita K. R, Dr. H. G. Chandrakanth "A survey on security attacks in wireless sensor network", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue4, July-August 2012.

7] Swapna Naik , Dr. Narendra Shekokar, Rupali Yavale " A Novel Authentication approach in Wireless sensor Network" International Journal of Scientific & Engineering Research, Volume 5, Issue 3, March-2014 ISSN 2229-5518

8] Sunil Gupta, Harsh Kumar Verma and AL Sangal "Authentication Protocol for Wireless Sensor Networks" International Journal of Electronics and Communication Engineering. Vol:4, No:6, 2010

9] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal,Abdul Hanan Abdullah and Kashif Naseer Qureshi Department of Communication, Faculty of Computing, University Technology Malaysia, Skudai, Malaysia, "Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks". International conference on smart sensors and applications (ICSSA) 2015.

10] Manpreet kaur, Amarvir Singh, **"**Detection and mitigation of sinkhole attack in wireless sensor network". 2016 International Conference on Micro-Electronics and Telecommunication Engineering