Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

An Assessment on Attacks on Routing Protocols in Wireless Sensor Networks

Ms. Sheffy Jindal [1]
M. Tech Student,
Computer Science,
Mody University Of Science and Technology,
Lakshmangarh, Rajasthan

Mr. Pinaki Ghosh [2]
Assistant Professor,
Computer Science,
Mody University Of Science and Technology,
Lakshmangarh, Rajasthan

***Abstract*— Now-a-days Wireless Sensor Networks (WSN) has become an emerging technology which has wide variety of applications such as fire detection, traffic observing, nuclear reactor regulator, seismic detection etc. But there are variety of attacks wireless sensor networks are susceptible of that interrupt the normal working of the network. Wireless sensor network's security is undermined because the sensor nodes are positioned randomly in an open environment with limited memory and power constraints and unescorted nature. In this paper various attacks the network can be attacked by and a tabular representation showing attacks' name, its effect and severity are discussed.**

Keywords*— Wireless Sensor Network, Security, Attacks.

I. INTRODUCTION

Wireless Sensor Networks have become worldwide attention seeker in last few years. WSN comprised of huge number of sensor nodes arranged randomly in an area. These sensor nodes' size is small and have computational capability for carrying out simple computations [1]. These nodes are inexpensive as compared to the traditional sensor nodes. These nodes sense and collect the statistics from the environment neighboring in which they are deployed. Then after sensing, the nodes transmit the information gathered to sink node which aggregates the whole information received from the nodes and convey it to another network. The sensor nodes can monitor environmental and corporeal conditions such as pressure, sound vibrations, humidity and temperature. Because of these types of features of the sensor nodes they are broadly used in the applications of wireless sensor network like military, medicine, industries, disaster assistance operations, traffic surveillance, environmental monitoring, agriculture monitoring, infrastructure monitoring [1, 2]. So the node in WSN plays two characters basically: collect the data and forward that data to the sink.

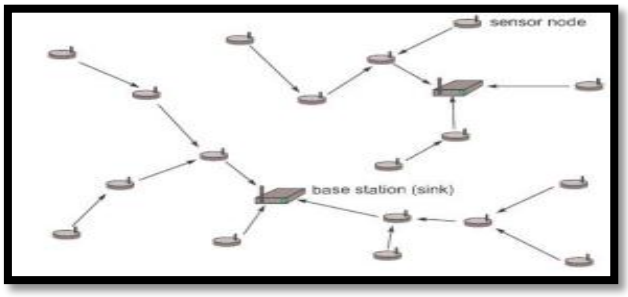

Figure 1: A Wireless Sensor Network

Typically, a sensor node comprised of five components: power unit (battery), memory, transceiver (transmitter/receiver), processor, and sensing unit. Some more components can be further added in the sensor node: location discovery system that permits the node to find the position of the node, a power initiator or generator that is used for recharging battery of the node and increasing its lifespan, and a mobilizer that allows the nodes to move. Sensing unit basically consists of two subunits: (i) analog to-digital converter (ADC) and (ii) a sensor. When an event is occurred the node sense the data (analog signal) and convert it into digital signal by the ADC unit. The transceiver unit is possible for connection between node and the network. The fuel of the sensor node is power unit (battery). That's why it is the most substantial constituent of a sensor node.

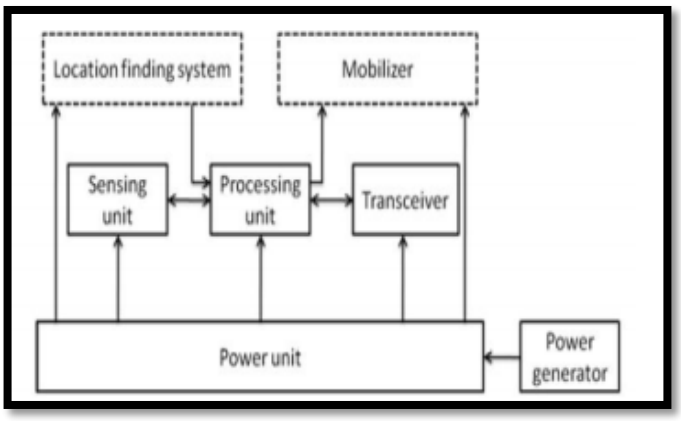

Figure 2: Components of a sensor node

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

As majority of sensor nodes are arranged in an unfriendly environment, so they are susceptible to numerous types of attacks that are initiated by some mischievous nodes in the network. These attacker nodes amend the behaviour of the network from normal to defective. These malicious nodes are created by tampering node's hardware or software or both and allowing it to transmit false information, or drop the required information. Hence, the most critical issue in wireless sensor network is security.

This paper majorly pays towards the security attacks. The paper is designed in the given manner: Section 2 deliberates about the kinds of wireless sensor networks. Section 3 deliberates about the security in wireless sensor network. Section 4 deliberates about the security goals in wireless sensor network. Section 5 deliberates about categories of security attacks in wireless sensor networks. Section 6 gives their detailed explanation of the attacks. Section 7 concludes the paper and a table containing effects and severity of attacks.

II.TYPES OF WIRELESS SENSOR NETWORKS

1) *Terrestrial WSNs [3]*: In these networks nodes are arranged in the area given either in an unplanned manner (sensor nodes are arbitrarily thrown into the target area by simply throwing it from a plane) or in pre-planned manner (sensor nodes' positions are planned and placed according to the grid placement). Since battery is insufficient and it cannot be recharged, an elective power source such as solar cells can be delivered for terrestrial sensor nodes.
2) *Underground WSNs [4]:* In these type of networks sensor nodes are buried under the earth or in a mine or cave that senses the underground conditions. Sink nodes are placed above the ground that forward the information gathered from sensor nodes to the sink. These networks are more inflated as compared to the terrestrial sensor networks as selection of proper nodes is completed which assure reliable communication through rock, water, soil and other minerals.
3) *Underwater WSNs [4]:* In these networks location of sensor nodes is underwater. In this autonomous vehicles gather the data from the sensor nodes which are also located underwater. Inadequate deployment of nodes is completed in this network. Limited bandwidth, signal vanishing issue and long transmission delay are the main problems that can be faced while doing communication in this network.
4) *Multimedia WSNs [5]*: In these networks cameras and the microphones are furnished with low costing sensor nodes. These nodes are arranged in a preplanned manner that guarantees coverage. Demand of high bandwidth, quality of service provision, consumption of high energy, cross layer design and data processing and compression techniques are the main issues in these networks.

III. SECURITY IN WIRELESS SENSOR NETWORKS

Security is the most substantial aspect of any system. Traditional WSNs are affected because of several types of attacks. These attacks are categorized as:

1. Attacks on confidentiality and authentication
2. Silent attacks on integrity
3. Attacks on availability

For preventing confidentiality and authentication attacks cryptographic techniques are used. In silent or passive attacks, the attacker confronts a sensor node and forages erroneous data. Attacks on availability of network are called denial of service (DoS) attacks. With the successful promotion of DoS attacks the functioning of WSNs can be degraded badly. DoS attacks on various stratums of networks are discussed below [6]:

A. *DoS attacks on the physical layer*: Physical layer is intended with selection of frequency, signal detection, inflection and data encryption. DoS attack on this layer can be injected using the most corporate way called Jamming.
B. *DoS attacks on the link layer:* Link layer is unveiled to multiplexing of discovery of data frame, data streams, error control and medium access control. The attacks on this layer results in resource exhaustion, collision and iniquitousness in the apportionment of frames.
C. *DoS attacks on the network layer:* Various attacks to which network layer is open to are selective forwarding, spoofed (fooled) routing information, sinkhole, wormhole, Sybil, hello flood and acknowledgment flooding.
D. *DoS attacks on the transport layer:* In this, Transport layer is open to de-synchronization attack and flooding.
E. *DoS attacks on the application layer:* Application layer is open to buffer overflow and logical errors.

.

IV. SECURITY GOALS IN WIRELESS SENSOR NETWORKS

A wireless sensor network has some unique features of its own which marks it dissimilar from traditional network but it has some features that are common with traditional network. Therefore, this section covers both the traditional network goals and the goals suited solely for the wireless sensor network. The security goals or services can be categorized into two types: Primary and Secondary goals.

A. Primary Goals

1) Data Confidentiality: Confidentiality can be understood as to limit the means of information access to only the authorized users and to prevent access from the users who are unauthorized [8]. Data confidentiality is the most substantial issue of any network. Sensor nodes carry some sensitive data which must be kept hidden from the attackers or malicious nodes. If the sensor nodes are not capable that they can keep the data confidential, then any node in its neighbor can tamper the data and transmit false information. This can cause serious problems, especially in military applications and traffic surveillance.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

2) *Data Authentication:* Data authentication is basically the capability of a receiver to validate data it has received from the correct sender [8]. In a wireless sensor network, the entire packet stream can be manipulated by attacker by addition of false packets to it. So, a receiver need to be able to recognize if the data received is from the correct source or not. Data authentication can be done securely by using symmetric key cryptography or asymmetric key cryptography where the sender and the receiver share a secret key or encryption and decryption of data can be done using public and private keys respectively.
3) *Data Availability:* Data availability determines if the network's services are available in case of failure or when attackers are present in the network. The availability of resources and other services can be threaten because of even a solitary point failure. So, data availability is very substantial goal and is liable for almost all the operations of the network.
4) *Data Integrity:* The attacker nodes in network can manipulate the data in the packets by adding some false packets to it [9]. Data integrity ensure that the data received is not changed in transfer. It confirms that the data is not transformed and is reliable.

B. Secondary Goals

1) *Data Freshness:* Data freshness decides that no longstanding packets have been reiterated and data received is recent. To guarantee the freshness of the message is also of same importance as much as ensuring data confidentiality and integrity is. There are two sorts of data freshness: Weak freshness and strong freshness. Weak freshness offers partial organization of messages but it does not offer any information about delay. Strong freshness offers total ordering of the messages and also the delay estimation [4]. Weak freshness is used in the sensor measurements while strong freshness is employed in the network for time synchronization.
2) *Self-Organization:* The sensor nodes in WSN are randomly deployed. They have no fixed infrastructure. That's why these sensor nodes have a capability called self-organizing which allows them to organize dynamically according to environment and the situation. Self-organizing capability is important because it helps in key management, multi-hop routing and building trustworthy relations with neighbors. If a sensor network lacks self-organizing capability then it results in severe damage from attacks.
3) *Time Synchronization:* Almost all sensor network applications rely on some of the form of time synchronization. While packet voyages between two sensors, sensors have the ability to figure out the end-to-end interval of the packet. Group synchronization for tracking applications may be required for a more collaborative sensor network [8].
4) *Secure Localization:* For recognition of nodes or for accessing whether the nodes belong to the network or not, WSN uses geological based information. Attacker may explore the headers of packets and data of the protocol layer for investigating position of the nodes. That is why secure localization is other most important objective that has to be satisfied during the implementation of security protocols [8].
5) *Robustness and Survivability*: Wireless sensor network must be robust in front of various security attacks and its impact should be reduced if an attack conquers. The convention of one node should not destroy the security of whole network [9].

V. ATTACKS IN WIRELESS SENSOR NETWORKS

A passive attack is about listening and monitoring of the data stream but it doesn't involve any modification of the data. No direct harm to the network is caused as passive attacks cannot modify the data. Attacks against privacy are passive attacks.

A. Attacks against privacy

The availability of huge amount of data through remote access is allowed by sensor networks. Due to this feature privacy problem arises because the attacker nodes can access the information easily without being physically available in the network [7]. These attacks are classified into three categories as follows:

1) *Eavesdropping:* In eavesdropping, the attacker node simply overhears the data stream and gain knowledge about communication content. When control information is transferred by network traffic about the configuration of sensor network which has details about the network, eavesdropping acts effectively against the privacy protection here.
2) *Camouflage:* Attacker nodes hide themselves in the given network by showing themselves as normal sensor nodes. So they falsify the other sensor nodes and attract the data packets from them. After receiving these data packets, either the attacker node drop the packets or misroute them.
3) *Traffic Analysis:* Attacker nodes evaluate the traffic of the network to determine which nodes are highly active. Once highly active nodes are revealed, the attacker nodes can harm those nodes because of which the whole network will get harmed.

B. Active Attacks

An active attack includes listening, monitoring and also modification of data by the malicious nodes residing inside or outside of the network. Active attacks can directly harm the network as they can manipulate the data. There are many types of active attacks. In this paper we are going to focus on the routing attacks seen in the network

.

VI. ROUTING ATTACKS IN WIRELESS SENSOR NETWORKS

The attacks on the network layer are known as routing attacks. These attacks occur while messages are send and received i.e. during the time of routing. Following are the routing attacks:

A. Sybil Attack

Sybil Attack is named after the name of the book *Sybil*, basically a case study of a woman having multiple fake identities. The nodes with these fake identities are called Sybil nodes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

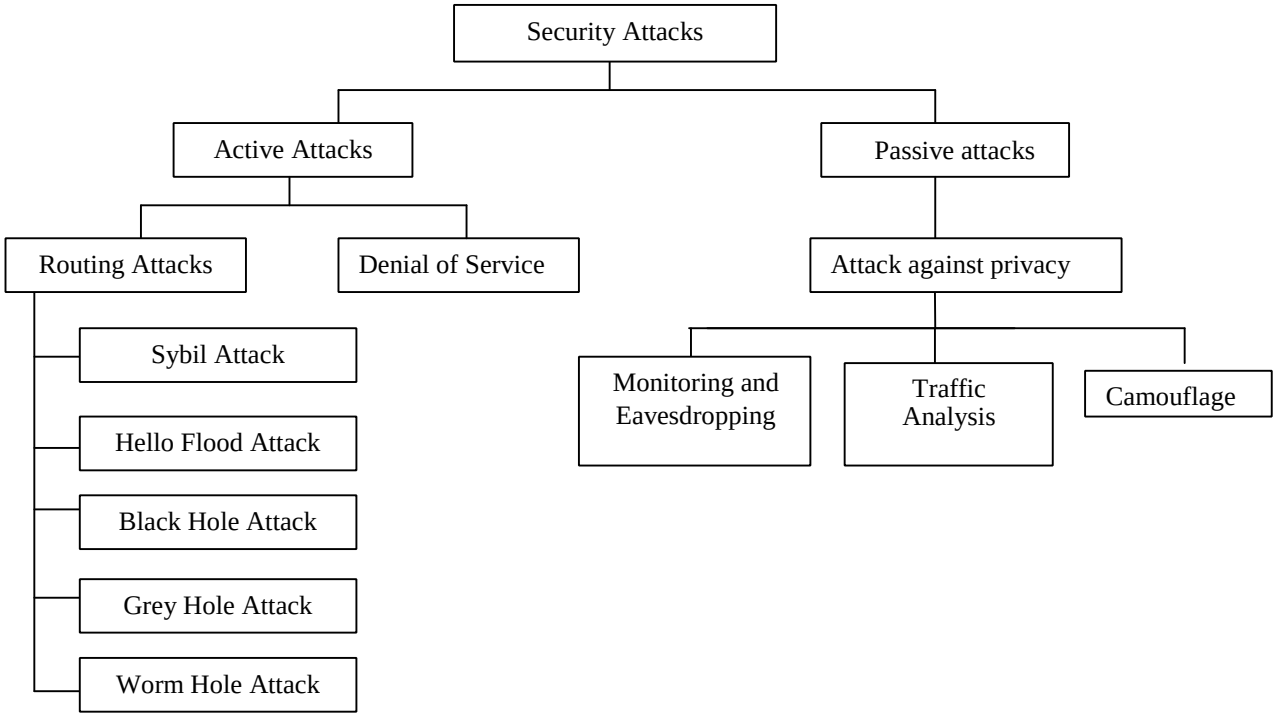

Figure 3: Classification of Attacks on WSN.

Sybil nodes can vote out the honest nodes in the network. Usually, most vulnerable networks to Sybil attacks are peer to peer systems. Examples of vulnerable systems include vehicular Ad hoc Network, Applications in Peer to Peer Systems, Distributed Storage and Routing in a Distributed Peer to Peer System [12], etc.

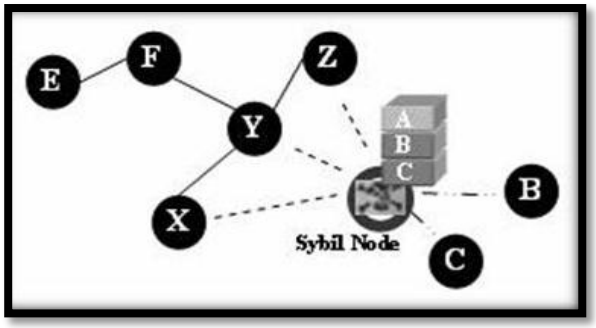

Figure 4: Sybil Attack in Network

B. Hello Flood Attack

Most protocols require nodes to air or we can say broadcast HELLO PACKETS to show their existence to their neighbors and the receiving nodes may undertake that it is within the reach of the sender. This assumption may prove to be false when attacker transmit routing information with an abnormally high transmission power to prove every other node in the network that the attacker node is its neighbor. Such an attack in the network is known as a hello flood attack [11].

C. Black hole Attack

A black hole is an attacker node that basically attracts all the traffic in the network by making advertisement that it has the direct path in the network [13]. This black hole node drops all the packets received by it from the other nodes.

In a black hole attack, attacker node does not send true control messages. To accomplish a black hole attack, malicious node wait for the adjoining nodes to send RREQ messages. When the attacker node receives RREQ message from its adjoining nodes, it then immediately replies a false RREP message providing a route to destination over itself.

Therefore, the requesting node assumes that the route detection process is accomplished and ignore RREP messages from further nodes and start forwarding packets over the attacker node. In this way attacker node attacks in the network and takes over all of the routes in the network. Therefore, all the packets are sent to the attacker node from where they are never forwarded or we can say they are eventually dropped. This is known as a black hole attack which in reality means to swallow all the information [10].

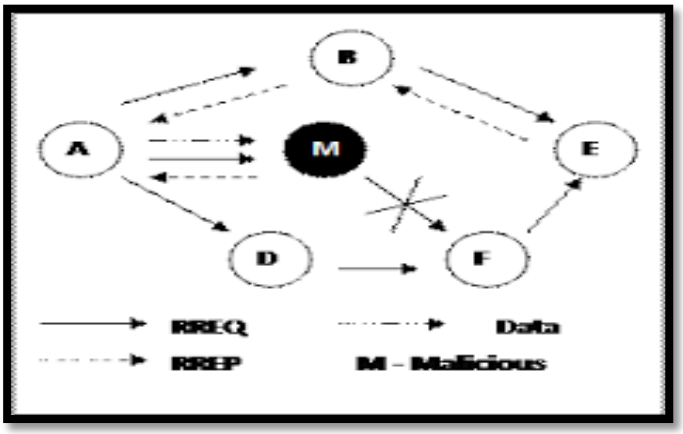

Figure 5: Black Hole Attack in Network

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

D. Grey hole Attack

A grey hole attack is an alternative of black hole attack in which the packets are dropped selectively by the nodes. The two ways in which a packet can be dropped by a node:

- It can drop all the UDP packets while transmit all TCP packets.
- It can drop of the packets or can drop them with some probabilistic distribution.

This attack is challenging to detect because the normal node prevents from behaving usually. A grey hole attack affects only one or two nodes in the network but a black hole attack affects the whole network.

E. Wormhole Attack

This is an attack over the routing protocol in which the packets or individual bits of the packets are captured at one location, tunneled to some other location and then replayed at another location. In this attack the two conspiring nodes generate an illusion that the locations involved are directly connected though they are actually distant.

VII. CONCLUSION

Wireless Sensor Networks are liable to many kinds of attacks due to arrangement of sensor nodes in an unattended atmosphere. In this survey, firstly we have given the security of a network and security goals of the wireless networks. Next, we have categorized the attacks in WSN in two categories i.e. active attacks and passive attacks. Further, we have given the detailed characterization of these types of attacks. This survey also gives the tabular classification of attacks and determines the severity of each attack.

TABLE 1 ATTACKS ON WSN

Attack Name	*Attack Definition*	*Attack Effects*	*Severity*
Eavesdropping	Overhearing the communication channel to gather confidential data.	• Reduces data confidentiality • Extracts vital WSN information • Threatens privacy protection of WSN	Low
Traffic Analysis	Monitoring the network traffic and computing factors that affect the network.	• Degradation of network performance • Increased packet collision • Increased contention • Traffic distortion	Low
Camouflage	Malicious nodes masquerade as normal nodes to attract packets.	• Increased packet loss/corruption • False data to network	Low
Sybil	Impersonation by malicious nodes as numerous bogus identities to attract packets from nodes.	• Packet loss/ corruption • False sensor readings • Modification of routing information	High
Black hole	Attracting all the possible traffic to a compromised node.	• Triggers other attacks like wormhole, eavesdropping • Exhausts all the network resources • Packet dropping/ corruption • Modification of routing information	High
Denial of Service (DoS)	Prevents the user from being able to use the network services. Extends to all the layers of protocol stack.	• Reduces WSN availability • Affects physical layer, network layer, link layer, transport layer and application layer • Prevents access to network services by the user.	High
Wormhole	Tunneling and replaying messages from one location to another via low latency links that connect two nodes of WSN.	• Changes normal message stream • False routes / misdirection • Forged routing • Changes network topology	High
Hello Flood	Transmission of a message by malicious node with an abnormally high transmission power to make the nodes believe that it is their neighbor	• False / misleading routes generated • Route disruption • Packet loss • Confusion	High
Grey hole	Selective dropping of packets by attracting packets to a compromised node.	• Suppresses messages in an area • information fabrication • packet loss • Launch other active attacks	High

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey, Computer Networks", pp. 393422, 2000.
[2] A.S.K. Pathan, H.W. Lee, C.S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges", *Communications, IEEE Transaction* , Feb 2006.
[3] I.F. Akyildiz, W. Su, Y.Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine 40 (8) (2002) 104–112
[4] I.F. Akyildiz, E.P. Stuntebeck, "Wireless underground sensor networks: research challenges", Ad-Hoc Networks 4 (2006) 669–686
[5] Kriti Jain, Upasana Bahuguna, "Survey on Wireless Sensor Network", IJSTM, Vol. 3 Issue 2, pp. 83-90, Sept 2012
[6] Jaydip Sen, Security and Privacy Challenges in Cognitive Wireless Sensor Networks, Dec 2012
[7] G. Padmavathi, D. Shanmugapriya,"A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", *International Journal of Computer Science and Information Security*, vol. 4, 2009.
[8] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Sean Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. ICACT 2006, Volume 1, 20-22, pp. 1043-1048, Feb. 2006.
[9] HBE-Zigbex. Ubiquitous sensor network. Zigbex Manual [Online]. Available: http://www.hanback.co.kr
[10] Dr. G. Padmavathi, Mrs. 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.
[11] V. P. Singh, S. Jain and J. Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", *International Journal of Computer Science*, vol. 7, no. 11, may 2010
[12] W. Chang and J. Wu , "A Survey of Sybil Attacks in Networks", *Sensor Networks for Sustainable Development*, M. Ilyas (ed), CRC Press.
[13] M. Al-Shurman, S.M. Yoo, S. Park, "Black Hole Attack in Mobile Ad Hoc Networks", *42nd Annual ACM Southeast Regional Conference (ACM-SE'42)*, 2004.