Attacks and Preventions in Wireless Sensor Network

Sampada A. Khorgade, Namrata D. Ghuse
Department of Computer Science and Engineering, P.R. Pote (Patil) College of Engineering Amravati, India
sampadakhorgade111@gmail.com, 8421725251

Abstract— Wireless sensor networks have become a growing area of research and become more practicable solution to many challenging applications. Wireless Sensor Network is emerging technology with their limited energy and communication capabilities.WSN provides security and is particularly challenging and its mechanisms are also being the greatest concern to deploy sensor network and monitoring the real world application. The problem of security is due to the wireless nature of the sensor networks. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a dangerous environment where they are not physically protected. The inclusion of wireless communication technology also incurs various types of security threats.

Keywords— WSN, Attacks, Prevention, Architecture, Confidentiality, Authenticity, Security.

INTRODUCTION

Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in the system taken the measurement of physical parameters such as temperature, pressure or relative humidity. Wireless Sensor Network is a promising platform for a variety of application areas such as environmental monitoring, battlefield surveillance, and homeland security domains and many researchers willing to work on various problems related to this domain. In many applications without providing the security to WSN would result in disastrous consequences. Security allows Wireless Sensor Networks used to maintain data integrity and availability of all messages in the presence of resourceful adversaries. The main objective of confidentiality and authenticity is expected in sensor networks to safe guard the information traveling among the nodes of the network. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. In this paper an overview on various WSN attacks are mentioned and summary on the attacks and possible preventive measures. In this it addresses the security concerns in wireless sensor networks.

I. RELATED WORK

A. WSN Architecture

In a typical WSN we see following network components [3] –

- Gateway or Access points :-

  Communication between Host application and field devices is possible because of these access points.

- Network manager :-

  Configuration of the network, scheduling communication between devices and management of the routing tables these are done by Network Manager.

- Security manager :-

  The Security Manager is responsible for the storage, and management of keys.

Each sensor network node has typically several parts:- a radio transceiver with an internal to external connection, a microcontroller etc. Base stations are more distinguished components of the WSN with much more computational, energy and communication resources and acts as a gateway between sensor nodes and the end user as they forward data from the WSN to a server. Many techniques are used to connect to the outside world including mobile phone networks, satellite phones, radio modems, high power Wi-Fi links etc. Figure shows the architecture of WSN.

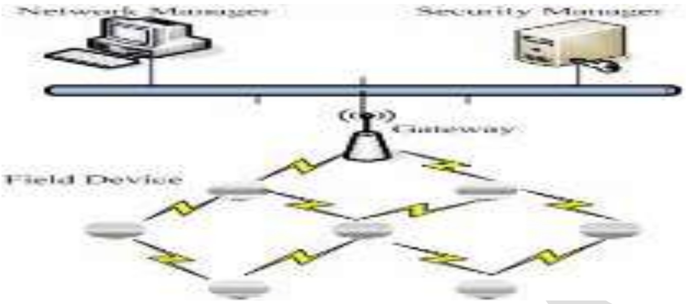

Fig 1. Architecture of WSN.

B. Types of Attacks:-

1. Denial of Service (DoS):

A Denial of Service attack in sensor networks is any event that diminishes the network's capacity to perform its desired function. The simplest DoS attack brings the resources available to the victim node by transmitting additional unwanted packets and prevent correct sensor network users from tapping resources to which these nodes are inserted [4]-[5].This occurs by the unintentional failure of sensor nodes and malicious action. Denial of Service (DoS) attack is means that not only to destroy a sensor network, but also for any event that reduce a sensor network's capability to provide a service [4].In WSNs, various types of Denial of Service attacks might be performed in different layers. At physical layer -the Denial of Service attacks could be jamming and tampering, at link layer-collision, exhaustion, unfairness at network layer -neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding.

- **DoS prevention:**

In [4] Wood and Stankovic explained different Denial of Service (DoS) attacks that can cause problems to different layers of sensor networks. The simplest DoS attack tries to drain the resources required to the victim sensor node, by forwarding additional unwanted packets and thereby prevents legitimate sensor network users from accessing network resources to which they are authorized.

2. Wormholes Attacks:

In the network one of its node i.e. sender sends a message to another rnode i.e. receiver, then the receiving node attempts to send the message to its neighbors. The neighboring node thinks the message was sent from the sender node so they attempt to send the message to the starting node, but it does not arrives as it is far. Wormhole attacks are difficult to encounter because routing information supplied by a node is difficult to verify. Wormhole attack is a noticeable threat to wireless sensor networks; because this kind of attack does not require a sensor in the network rather it could be performed even at the starting phase when the sensors start to discover neighboring information [6].

- **Wormhole attack prevention:**

The mechanism to overcome the wormhole attack include DAWWSEN [7] a proactive routing protocol which is based on the construction of a hierarchical tree where root node and leaf node is present where the base station is the root node, and the sensor nodes are the leaf nodes of the tree. Advantage of DAWWSEN is it does not require any geographical information about the sensor nodes.

3. The Sybil attack:

In Sybil attack a single malicious node will appear to be a set of nodes i.e. the attacker can appear in multiple places at a time, by creating fake identities of nodes located at the edge of the communication range will send the false information to a node in the network. The false information can be the position of nodes, signal strengths, pretending nodes that do not exists [8].Insider attack can prevent by public key cryptography but it is too expensive to be used in a networks. And the outsider attack can be prevented by authentication and encryption techniques by launching a Sybil attack on the sensor network. In WSN the routing protocols in network has a unique identity. The figure demonstrates Sybil attack where an attacker node 'AD' is present with multiple identities. 'AD' appears as node 'F' for 'A', 'C' for 'B' and 'A' as 'D' so when 'A' wants to communicates with 'F'it sends the message to 'AD'.

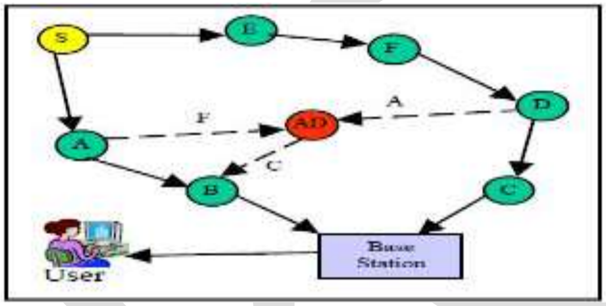

Fig 2. Sybil Attack

- **Sybil prevention:**

For preventing against the Sybil attack the mechanism is to utilize the identity certificates [9].Unique information is assigned to each sensor node before any deployment. The server then creates an identity certificate binding the nodes identity to the assigned unique information and downloads the information into the node. To securely demonstrate its identity, a node first shows its identity certificate, and then proves that it possesses the associated unique information. This process requires the exchange of several messages. This way the Sybil attack gets prevented.

4. HELLO flood attacks:

An attacker sends or replays a routing protocol's HELLO packets from one node to another. This attack uses HELLO packets as a weapon to convince the sensors in WSN. This attack can be caused by a node which sends a Hello packet with very high power, so that a large number of nodes in the network can able to choose its parent [6]. All messages now need to be routed multi-hop to this parent. The figure demonstrates how the attacker node 'AD' broadcast hello packets to convince nodes in the network as neighbor of 'AD'. Though some nodes like I, H, F are far away from 'AD' they link 'AD' as their neighbor and try to forward packets, through it which results in wastage of energy and data loss.

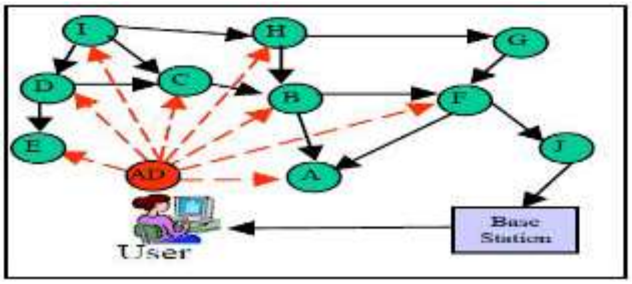

Figure 3. HELLO flood attack

- **Hello flood attack prevention:**

To avoid Hello flood attack requires checking of bidirectional link, so that the nodes ensure that they can reach their parent within one hop. To prevent the hello flood attack cryptographic technique is employed [9]. This technique uses two sensors as same secret key. During the communication the new encryption key is generated. This ensures that only reachable nodes can decrypt and checks the message and thereby prevents the adversary from attacking the sensor network. The disadvantage of this technique is that any attacker can spoof its identity and then starts attacks.

5. Sinkhole attacks

Sinkhole attacks are difficult to encounter because routing information supplied by a node is difficult to identify. As an example, a laptop-class adversary has a strong power radio transmitter that allows it to provide a high-quality route by transmitting with enough power to reach a wide area of the network. In this case a compromised sensor node tries to influence the information to it from each and every neighboring node. In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. In fact, this attack can affect even the nodes those are considerably far from the base stations. Figure shows the conceptual view of a black hole or sinkhole attack.

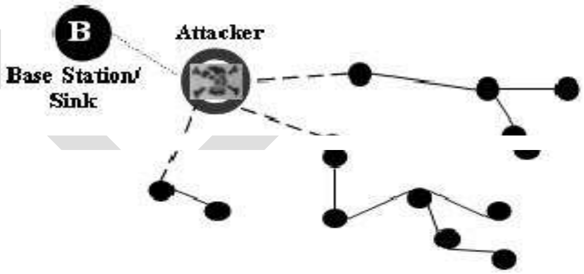

Fig 4. Sinkhole attack

- **Sinkhole prevention:**

One class of protocols resistant to these attacks is geographic routing protocols. These attacks are difficult to resist. Geographic protocols construct a topology on demand using only localized interactions and information and without initiation from the base station [11].

6. Passive Information Gathering Attack:

The information if it is not encrypted intruder with an appropriately powerful receiver and well-designed antenna can easily pick off. Strong encryption technique is needed to minimize the threats of Passive Information. Interception of the messages which contains the physical locations of sensor nodes allows an attacker to locate the nodes and destroys it. [12] - [13].

- **Passive information gathering prevention***:*

To minimize the threats of passive information gathering, strong encryption techniques need to be used.

CONCLUSION

All of the previously mentioned security threats, the Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, serve one common purpose that is to compromise the integrity of the network they attack. Although some solutions have already been proposed, there is no single solution to protect against every threat. In our paper we mainly focus on the security threats in WSN. We have presented the summery of the WSNs threats affecting different layers along with their defense mechanism. We conclude that the defense mechanism presented just gives guidelines about the WSN security threats; the exact solution depends on the type of application the WSN is deployed for.

REFERENCES:

[1] Jamal N. Al-Karaki& Ahmed E. Kamal, (2004) "Routing Techniques in Sensor Networks: A survey", IEEE communications, Volume 11, No. 6, Dec. 2004, pp. 6-28.

[2] M. Tubaishat, S. Madria, (2003) "Sensor Networks : An Overview ", IEEE Potentials, April/May 2003

[3] International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 8 (2014).

[4] A.D. Wood and J.A. Stankovic, (2002) "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, 2002, pp. 54–62.

[5] David R. Raymond and Scott F. Midkiff, (2008) "Denial-of- Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. no. 1, 2008, pp. 74-81.

[6] ZawTun and AungHtein Maw,(2008),"Worm hole Attack Detection in Wireless Sensor networks", proceedings of world Academy of Science, Engineering and Technology Volume 36, December 2008, ISSN 2070-3740.

[7] Rouba El Kaissi, AymanKayssi, Ali Chehab and ZaherDawy, (2005)''DAWWSEN: A Defense Mechanism against Wormhole attack In Wireless Sensor Network", Proceedings of the Second International Conference on Innovations in Information Technology (IIT‟05).

[8] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks", Commun.ACM,47(6):53-57.

[9] J. R. Douceur, (2002) "The Sybil Attack," in 1stInternational Workshop on Peer-to-Peer Systems (IPTPS'02).

[10] ZoranS.Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International Journal of Communication, Issue 1, Volume 2, 2008

[11] M. Zorzi and R. R. Rao, (2003) "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," IEEE Transactions on Mobile Computing, vol. 2, no. 4, pp. 337-348, 2003.

[12] Al-Sakib khan Pathan et.al, (2006)"Security in wireless sensor networks: Issues&challenges" in feb.20 22, 2006,ICACT2006,ISBN 89-5519-129-4 pp(1043-1048)

[13] C. Karlof and D. Wagner, (2003). "Secure routing in wireless sensor networks: Attacks and counter measures,"AdHoc Networks Journal, vol.1,no.2–3,pp.293–315, September22, 2006, ICACT2006, ISBN 89-5519-129-4 pp(1043-1048).