INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES
© 2004 -14 Society For Science and Nature (SFSN). All Rights Reserved
www.scienceandnature.org

Short Communication

SECURITY ISSUES AND THREATS IN WIRELESS SENSOR NETWORKS AND THEIR REMEDIES

[1]Kour Teajsvit, & [2*]Singh Tejbhan
[1]Chandigarh Group of Colleges,Gharuan, Mohali Chandigarh, Punjab, India
[2*]Mahant Bachittar Singh College of Engineering and Technology, Jammu, India

ABSTRACT

Wireless sensor networks are finding their place in almost every possible sphere of modern life. However, with their high usage also occurs the problem of their security. Various threats like the Sybil attack, wormhole attack, etc are in the picture. Safety from these threats and security issues is one of the main priorities of the researchers. In this paper various security issues and threats are discussed in detail and various counteract methods are also discussed so that these issues and threats are handled.

KEYWORDS: Wireless, Wormhole, Security, Priorities.

INTRODUCTION

In the present scenario, the application of wireless sensor networks is almost becoming endless and stretches to any extent of human imagination. The main of any wireless sensor network is the development of small devices, which could be spread in a given area, are capable of measuring a given parameter, and are able to communicate with other devices. Various parameters that can be sensed by wireless sensors are humidity, temperature, lighting conditions, soil monitor, military applications, presence and absence of particular objects, vehicle motion. A wireless sensor network basically consists of 100 to 1000s of wireless sensor nodes and they are able to receive, process and transmit the required information. Even after the extensive use of wireless sensor network, their security is of major concern because the data flowing through the network is highly susceptible to addition of useless bits to the data packets; eavesdropping etc. therefore the security of data plays a great role in ensuring that the data is properly transmitted through the channel. In this paper, we explore the various security issues that may affect proper transmission of data and various measures and methods are given for counter act.

In section (1), various security issues during data transfer are explained in detail. Section (2) is divided into 5 subsections which explain various security threats and their possible counteract methods.

VARIOUS SECURITY ISSUES OCCURRING DURING DATA TRANSFER IN WSNS

The major security parameters are data authenticity, data confidentiality, data integrity. Each of these parameters and the concerns regarding them are described below:

Data Authenticity

Authentication is used to ensure the authenticity of the user. In case of sensor networks an outside party can easily add unwanted data, so it becomes necessary for the receiver to check the authenticity of the data and make sure that the data has come from the correct source. To achieve data authentication MAC (Message Authentication Code) is used. The sender and receiver share a secret key and calculate a MAC (Message Authentication Code) of all the data that is transferred between the sender and the receiver. In case of WSNs the authentication must be stronger than normal networks because in case of WSNs the data is sent to multiple receivers and the MAC proves to be insufficient here. However there are two methods by which this problem can be solved: SPINS and LEAP. SPINS is Security Protocols for Sensor Networks. There are two protocols in SPINS: SNEP and mTESLA. The advantages of SNEP are data confidentiality, freshness of data and two party data authentication. mTESLA is a fairly new protocol and it performs the function of proper and authenticate broadcast for resource constrained environments.

LEAP (Lightweight Extensible Authentication Protocol) performs the function of mutual authentication and supports regular re authentication for clients.

Data confidentiality

Data confidentiality ensures that the communicated data is accessible only to the intended receiver so that it is not misused or lost. The problem of confidentiality in case of WSNs is that sometimes the sensor nodes can misguide the base stations by adding false data during the transmission of data. Hence, data confidentiality should be properly achieved for secure data communication.

Data integrity

Data integrity ensures that the data is real and is not altered during the communication of data. Data authentication provides data integrity also. So when we ensure data authentication, data integrity is also provided along.

Various security attacks on WSNS

WSNs are prone to various security threats. The main and most severe security threats are as follows:

- Denial of service
- Selective forwarding
- Hello flood attack
- Wormhole attack
- Sinkhole attack
- Sybil attack

Denial of service attack

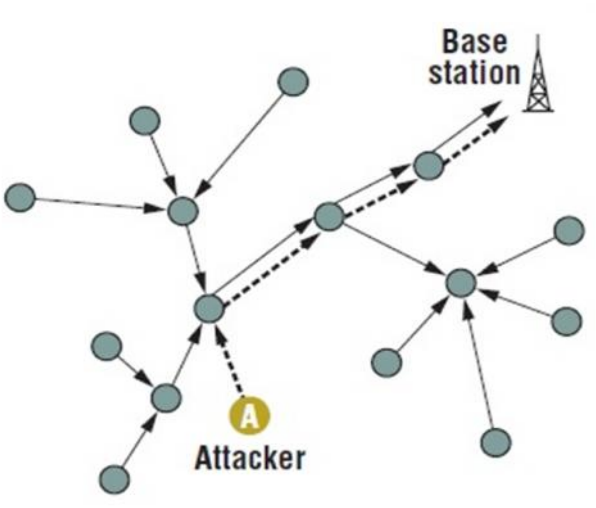

Figure (1)

Denial of service may be caused either because of failure of nodes or false action. In this type of attack extra packets are sent thereby exhausting the resources available to the affected node and thereby prevents the user to access the required information. In wireless sensor networks this type of attack occurs at various layers. At the physical layer, the attack could be tampering and jamming. At the link layer it may be collision, exhaustion and black hole at the network layer. This attack can be prevented by using JAM which in which a mapping protocol finds the jammed area in the wireless sensor network thereby avoiding the faulty area and enabling routing within the network.

Selective forwarding

Figure [2] represents selective forwarding. In a selective forwarding attack, the defected node does not forward selected messages. The result is that these messages are not communicated forward any further. It is also called Gray hole attack. Selective forwarding is of various types. One type of selective forwarding attack may be the case in which the affected/malicious node selectively drops the packet which comes from either a group of nodes or from a particular node. This type of attack acts as a denial of service attack. Selective forwarding attack also behaves as black hole attack. In this case the malicious node does not forward any data packet. One way to deal with selective forwarding attack is the use of multipath routing. The messaged are passed through paths, which are immune to selective forwarding.

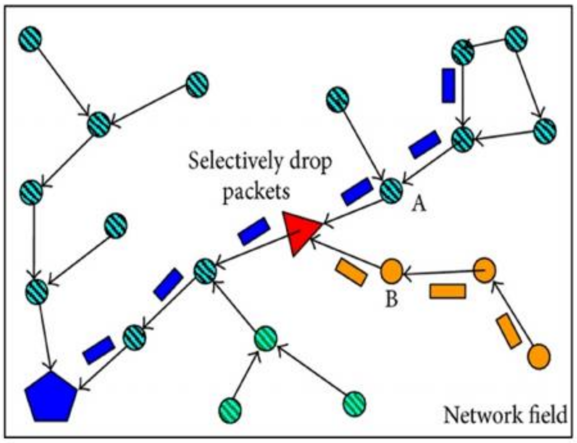

Figure (2)

Hello flood attack:

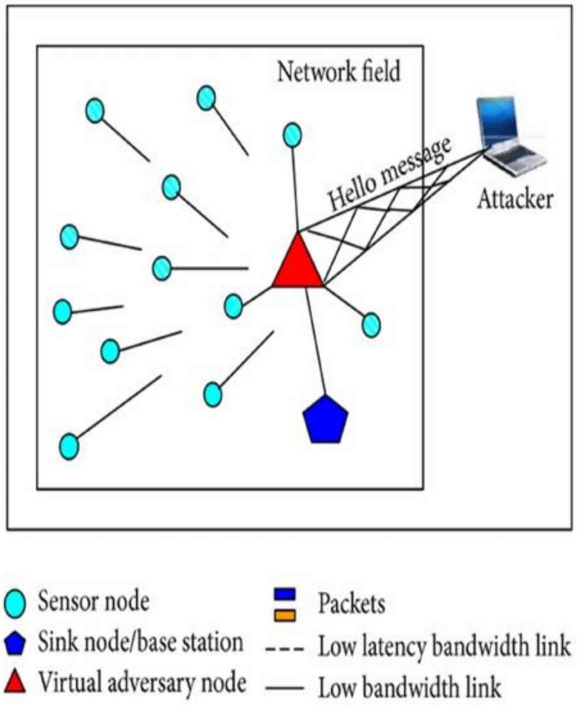

Figure (3)

Figure 3 shows hello flood attack. In hello packet attack as the name suggests, hello packets are used as a weapon. A major cause of this attack is that many protocols in wireless sensor networks need the nodes to broadcast HELLO packets to declare themselves as sensor nodes and the nodes who receive it may consider themselves to be in the normal range of the sender node. It is this consideration by the sensor, which goes wrong when the attacker broadcasts with high transmitting power high enough to influence the sensor node that the adversary is its neighbor. The hello flood attack can be prevented by the properly checking the directionality of the link and by making it sure that they can reach their parent node in single hop.

Wormhole Attack

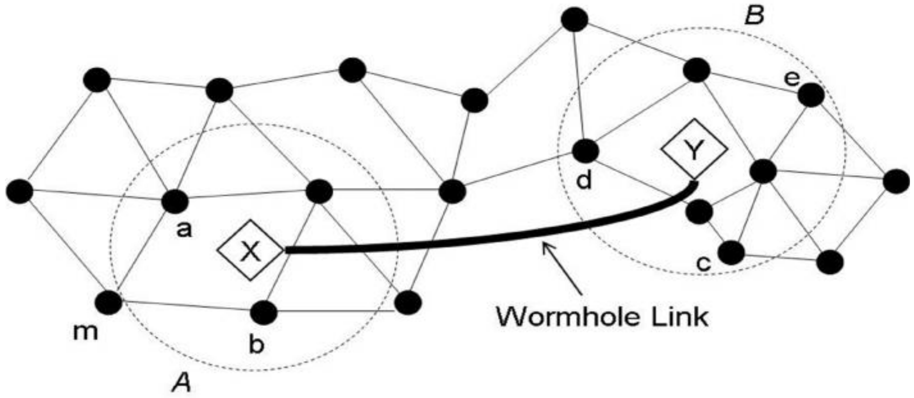

Figure (4)

Figure [4] represents a wormhole attack. In this attack the tunneling of bits takes place from one location in the network to the other location. As we can deduce from the figure in this attack the attacker in the area location B acquires the data from the node in location A. This attacker then convinces its neighboring node that it is in the range of location A even though it is many hops away thus creating a wormhole link as shown in figure [4]. It can be counteracted by using a mechanism called [DAWSEN] It is a routing protocol in which the base station serves as the root node and the sensor nodes serve as internal or leaf nodes thus forming a hierarchical tree like structure. The advantage of this mechanism is that this there is no need of any geographical information of the sensor nodes.

Sybil attack

In a Sybil attack , a single node acts to be more than one node by taking the identity of other nodes. Sybil attack therefore affects the integrity, security and hampers the resource utilization.

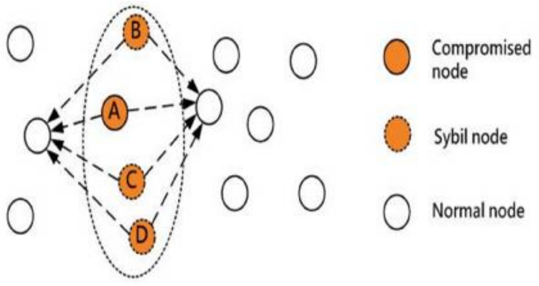

Figure (5)

One way to prevent Sybil attack is the use of identity certificates. In this, the server assigns a unique information to the sensor nodes. The server then gives an identity certificate depending on the unique information assigned to the sensor node and after that it downloads the unique information into the sensor node. The sensor node with the unique information needs to present its identity certificate to prove itself.

CONCLUSION

From the facts described in the paper, we conclude that wireless sensor networks because if their nature of distribution and architecture are prone to various kinds of security threats and issues. There are various techniques to counteract these attacks. These techniques and methods need to be adopted properly and accurately in order to get rid of the unnecessary threats and attacks.

REFERENCES

Han Kyusuk: Kim Kwangio: Shon Taeshik, 2010. Untraceable Mobile Node Authentication WSN. Sensors 10.no.5:4410-4429

A.R Beresford and F.Stajano, Location Privacy in Pervasive Computing, IEEE Pervasive Computing 2(1):46-55,2003

.

A. Perrif, R. Szewczyk,JD. Tygar,V.Wen, and D.E. Culler.Spims:security protocols for sensor networks.Wireless Networking,8(55):521-534,2002.

Jeffery Undercoffer, SasukanthAvancha, Anupam Joshi and John Pinkston. In Sevurity for Sensor Networks.

Chris Karlof David Wagner. In Secure Routing in Wireless Sensr Networks: Attacks and countermeasures.

J.R. Douceur,(2002)"The Sybil Attack" in last International Workshop on peer to peer Systems(IPTPS"02).

Rouba El Kaissi, AymanKayassi,AliChehab and ZaherDawy,(2005)DAWSENN:" A Defense Mechanism against wormhole attack in wireless sensor network",Proceedings of the Second International Confernce on Innovations in Information Technonlgy.