International Journal of Engineering Research & Management Technology ISSN: 2348-4039
May-2015 Volume 2, Issue-3
Email: editor@ijermt.org www.ijermt.org

ASSESSMENT IN WIRELESS SENSOR NETWORK SECURITY

S.SARADHA
Information and Technology
Sri Krishna Arts and Science College
Bharathiar University, Coimbatore

S.GOMATHI
Information and Technology
Sri Krishna Arts and Science College
Bharathiar University, Coimbatore

ABSTRACT:
Wireless sensor networks have effective security mechanism and interact with some sensitive data. There is a challenge in security issues to find a well balanced situation requirement and deals with some major security issues and wsns have become quit task in the current stage due to many external challenges. Let us survey some security issues, requirements of wireless sensor and so on

INTRODUCTION:

Wireless sensor network securities have low cost solution in real world challenges. here the low cost provider means implement the sensor arrays in variety of conditions and capable of performing military task and it also have lack of data storage and power. There is some major techniques in wsns.To classify the main aspects of wireless sensor network security into four major categories: the obstacles to sensor network security, the requirements of a secure wireless sensor network and attacks, There are variety of attacks are possible in wsns and here classified according to the criteria such as domain of attacks or the techniques used in attacks. Attacks in wsns has been roughly classified into following criteria passive or active &main attacks of the wsns there is the high end technologies &better solutions so attackers need more time for these types of technology so currently certain terms.

LITERATURE SURVEY

1. Bin Xiao, Bo Yu, and Chuanshan Gao. Chemas, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006; A wireless sensor network is a special network and here many constraints compared with classical computer network. The author has survey the hurdles (difficulties) of sensor security, principles of security & attacks. The hurdles have some constraints deploy some security. Wireless sensor network have compressing both the usual &unique requirements.
2. Hralambos Mouratidis, Paolo Giorgini, Gordon Manson, Using Security Attack scenarios to Analyse Security During Information System Design, in the 6th International Conference on Enterprise Information Systems, 2004.here it's developing for business opportunities work level & classify the different types of attacks i.e passive attack or active attack based on this type attack the attacker hack the message from the sender to receiver.
3. Hemanta Kumar Kalita and AvijitKar "Wireless sensor network security modal", International Journal of Next-Generation Networks, 2009.The growth of networks have been increased & here message passing also been increased at the same time hacker also increased and they used some of main attacks to hack the message .

TINY SURVEY OF WIRELESS SENSOR NETWORK SECURITY

A. Hurdles of Sensor Security

A wireless sensor network have used many constraints so it is very difficult to deploy directly so from the existing security only it's possible to deploy the security .In hurdles it's very use full for the constraints.
• Limited Memory storage

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type (TelosB) has a 16-bit, 8 MHz RISC CPU with only 10K RAM etc….

• Limitation of Power

Power energy is largest constraint in wireless sensor .If once the sensor nodes are implement in a sensor network it is not possible to replace because it's very expensive .Here can add some code for the security & protocol.

B. Unreliable Communication

Unreliable communication is another threat to sensor security. It fully depends upon the network communication.

• Unreliable Transfer

In unreliable transfer packet is based upon the sensor network it is connectionless network. Sometimes while sending the packet there may be error because of damage of packets or congested nodes or traffic etc..Ex Cryptographic key

• Conflicts

The channel may be reliable but communication may still unreliable .Due to broadcast nature the packet meet in midway of transfer and conflict will occur so transfer may get fail.

C. Principles of Security

1. Confidentially: confident information is disclosed only to the authorised person.
2. Integrity: Information can be changed only in authorized manner.
3. Availability: service not denied to authorised user.

V. Attacks

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways.

Passive and active attacks

Attacks can be classified into two major categories, according the interruption of communication act, namely passive attacks and active attacks

A. Passive attack:

Passive attack said that data exchange in network without interrupting and communication. Examples of passive attacks are traffic analysis, and traffic monitoring and two types of passive attacks are

=>Release of message contents

=>Traffic analysis

Release of message content

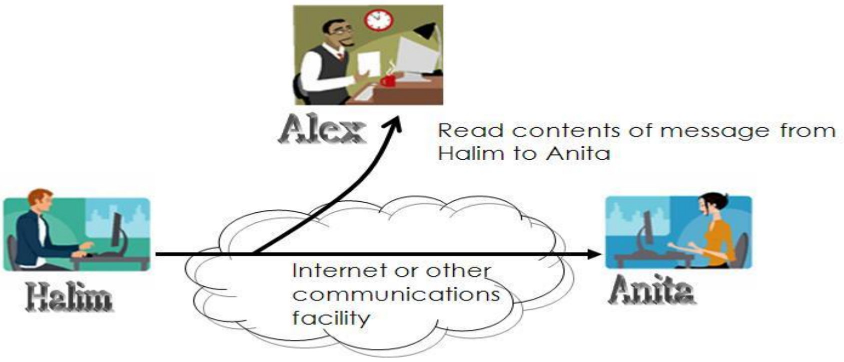

Fig.1 Release of message content

In the release of message contents just hacker silently read the message but he/she does not make any changes in the data capture EXAMPLE : conversion of telephone, sending electronic mail message, and transferred file may contain some sensitive or confidential information .

Traffic analysis:

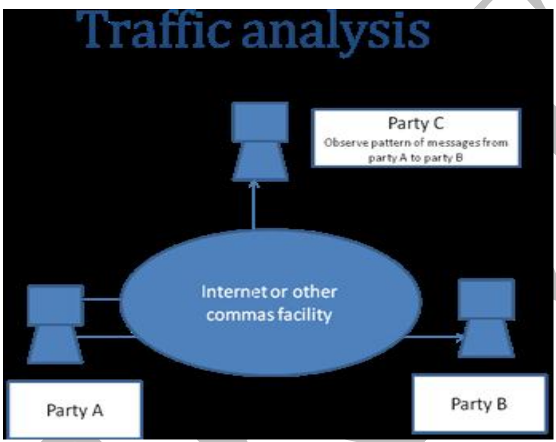

Fig.2 Traffic analysis

The data is always travel from one place to another place that time data monitoring can be do by the hacker capture data in the traffic analysis so in network traffic message may get leaked here to prevent we are using encryption and decryption methods

B. Active attacks

Active attacks involve some modifications of the data and alter system resources in active attacks there are four types of attacks i.e

=>Masquerade

=>Replay

=>Modification of message

=>denial of service

MASQUERADE:

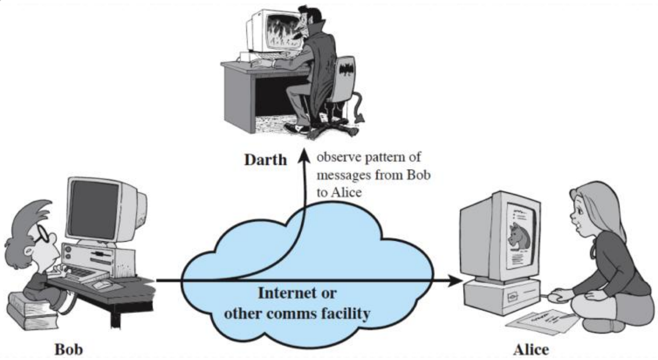

Fig. 3 Masquerade attack

A masquerade takes place when one entity pretends to be a different entity. This attack usually includes one of the others forms of active attacks

Replay:

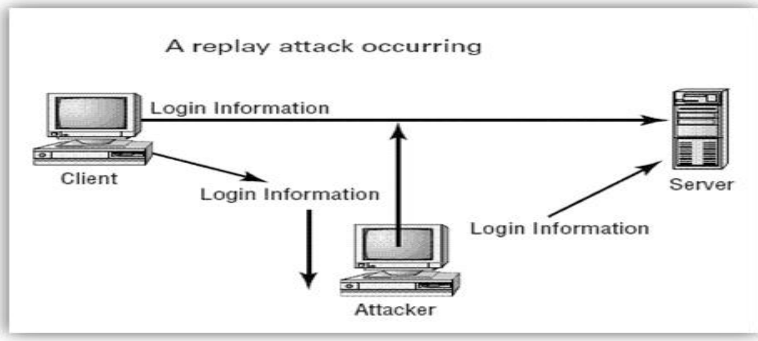

Fig. 4 Replay attack

In replay attack capture the data and retransmit the data that means a client send data to the server that time attacker will capture the information and he will say that he is a original person(client)

Modification of message:

Fig.5 modification of message

In this active attacks message can be modify that means the hacker can capture the data and canadd, edit or delete message and sent to the end user

Denial of service

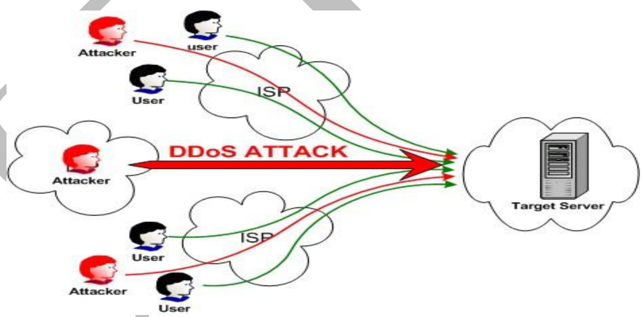

Fig. 6 Denial of service

Denial-of service attack (DoS attack) or distributed denial-of service attack (DDoS attack) is an preventing normal use of system resources. Hacker will send all data so network may overload and it will get down.

LIST OF MAIN ATTACKS AND THEIR EXPLANATION

A. MAC LAYER ATTACK:

Disrupts the cooperation of protocols with one another and thereby, controls the radio channel as a whole.

B. DISRUPTION ON BACK-OFF MECHANISM AND DCF (DISTRIBUTED COORDINATED FUNCTION):

Selfish nodes will disrupt the working modes of MAC protocols.

C. MORTIFYING THE SYSTEM:

Includes or removes bits from the present transmission in order to activate DoS attacks later on.

D. DISRUPTION OF NETWORK VECTOR OF ALLOCATION:

Prevents RTS and CTS signals from being transmitted / received to the current transmissions.

E. NETWORK CONGESTION:

It is also an attack which will prevent the allocation of resources by occupying them indefinitely.

CONCLUSIONS:

A wireless sensor network is growing network in further security exceptions is high in network application. Here key based management become strong and as per the attacks increased security also been increased and there may been attractive option in variety of new areas

REFERENCES:

1. Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004.
2. Avancha, S. et al. "Wireless Sensor Networks," Kluwer Academic/Springer Verlag Publishers, 2003 .
3. A.K.S Pathan,;Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006.
4. Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at.
5. Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534.
6. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ―A survey on sensor networks‖, IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002
7. Pathan, A.S.K.; Hyung-Woo Lee; ChoongSeon Hong, ―Security in wireless sensor networks: issues and challenges‖ Advanced Communication Technology (ICACT)
8. C. Karlof and D. Wagner, ―Secure routing in wireless sensor networks: Attacks and counter measures, ‖AdHoc Networks Journal, vol. 1, no. 2–3, pp. 293–315, September 2003
9. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, vol. 40, no. 8, (2002) August, pp. 102-114.
10. M. Sharifnejad, M. Shari, M. Ghiasabadi and S. Beheshti, "A Survey on Wireless Sensor Networks Security", SETIT, (2007).