10th International Conference on Recent Development in Engineering Science, Humanities and Management
The Indian Council of Social Science Research (ICSSR) North West Regional Centre, Punjab University Campus, Chandigarh (India) RDESHM-17
24th December 2017, www.conferenceworld.in ISBN: 978-93-86171-89-4

Review on Security Issues in Wireless Sensor networks

Ravi Arora[1], Mukul Kumar[2]

[1]*Assistant Professor, Department of Computer Science & Engineering*

HMR Institute of Technology & Management

[2]*Department of Computer Science & HMR Institute of Technology & Management*

ABSTRACT

In this current digital era Communication between two points is really sensitive matter. Every single bit of data packet is very precious. In WSN(Wireless Sensor Network) the data transmission between one node to another, sensor to sensor or one device to another device. There are real live example like healthcare system, Smartphone's, Airplane, Military all data managed wireless so monitor the security thread and many security challenges occurs. This paper focus on security attack mechanism in Wireless Sensor Network and monitor and analyze real-time data from Varity of applications.

Keywords: Sensor, Sybil attack , DOS, Wormhole, Black hole, Attack, Holistic, Challenge, symmetric and asymmetric cryptography,

I. INTRODUCTION

Wireless sensor network is an innovative and very vast technology which regularly growing, all kind of important device are binded with the number's of sensors that contain data is collectively sent to the base station through the gateway. This technology used where we can not use wired medium for communication and wired system will be more complex as compare with the wireless like temperature, pressure, speed sensor. Small sensor, ultra sonic sensor, door sensor (open close), car parking sensor etc. All of these sensor are used as for surveillance or monitoring, tracking, analyzing etc. it has limited power capacity, processing capacity, memory and also sensing restriction environment using remotely . They all are connected in the form of master and slave, where more then nodes sends information using its capacity and centralized processing receiving data with in short range so its very important to send data to authorized device[1][2][3][4] if the data reached to unauthorized device then the data can be miss used.

WSN is very useful, the feature provided by sensor network in very cheap cost that can be solution of many real world problems as

self-healing and self-organizing, mobility of deployed nodes, unattended operation, scalability, as well easy use [5] [6].

In this paper we discuss about wireless sensor networks we talk about steganography, cryptography, Security, Wormhole, Black hole, Attack, Holistic, Challenge, symmetric and asymmetric cryptography, other basics of network security.

Security Attacks in WSN[7]

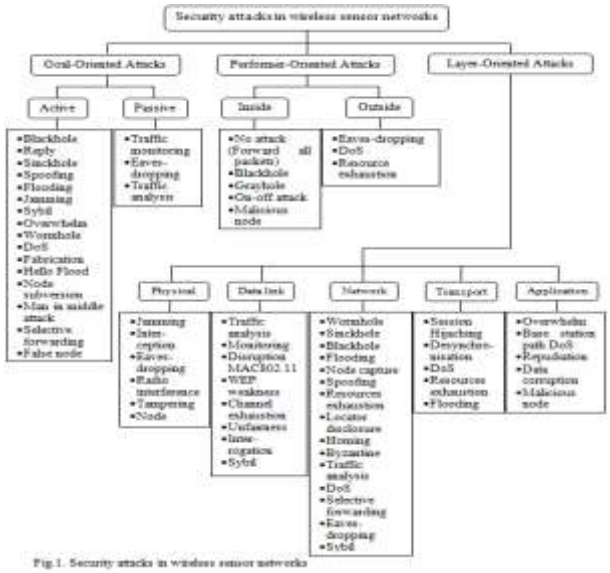

Fig 1. Security attacks in wireless sensor networks

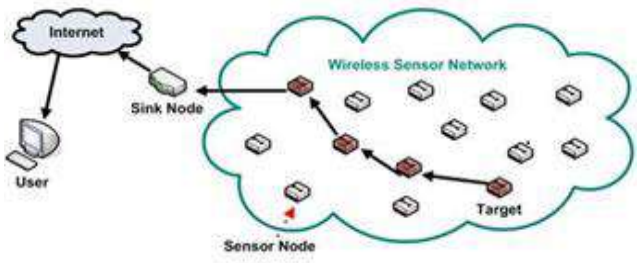

Fig2 Image of Wireless Sensor Network

II. INFORMATION OF SECURITY THREAD AND ISSUES

This is vulnerable to security attacks just because it follow the property of broadcast transmission medium through which where one sender and more then one receiver from that senerio we have two categories of attack active and passive, we discuss these topic in details.

2.1 Active Attacks :-

The mode at which unauthorized access done by attackers that make role of data stream modification in communication channel like monitoring and listening this kind of process id known as Active attack.

2.1.1 Routing Attacks

This attack is performed in network layer so this kind of attack is known as routing attack. There are few different type of attack on routing attack

2.1.2 Selective Forwarding:

Any unwanted node selectively drop certain package. At the end of combining from attacker then gather much traffic. In that scenario the node assumed as forward received massage due to much traffic node get refuse forward packet, neighbors might use another route.

2.1.3 Attack on information transit

This attack is performed in network by changing specific values or parameter and final result is sink according with need. While sending report, attacker can monitor the flow of traffic from this certain changes or modification done on packets so wrong information provide to base station or sink.

2.1.4 Sinkhole/Black hole Attack:

In this kind of attack where malicious node act as black hole that make attack in all traffic in WSN, its also make affect on node that far from the sink.

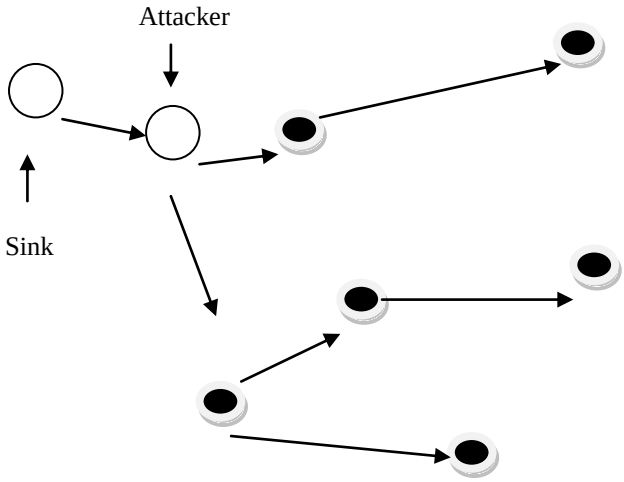

Fig 3 Attack on Sinkhole/Black hole

2.1.5 Wormhole Attack in sensor network:

In this attack where attack find the bits or packet from a network and make record the movement on packet and tunnels those packet from another location .

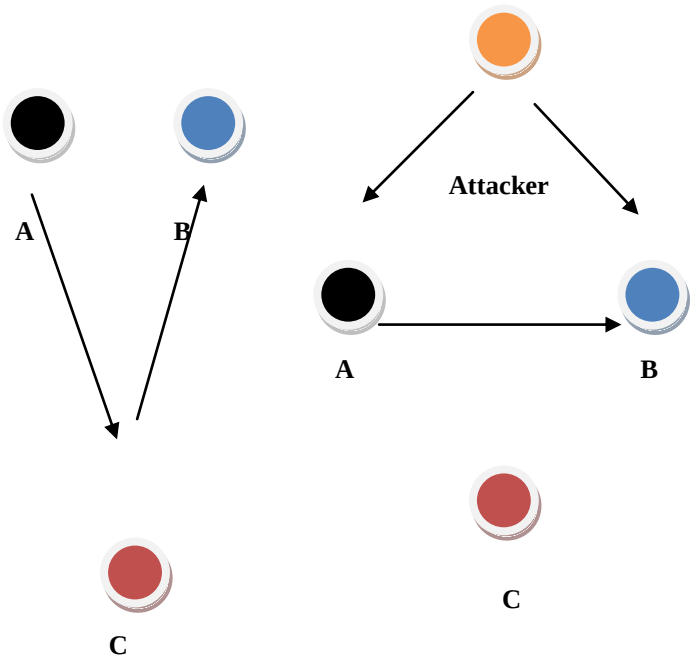

Fig 4 Wormhole Attack

2.1.6 Denial of Service (DOS) attack:

In this attack where attacker going to make network resources unavailable for sometime. In WSN, more then one node having same name sending request to one machine then at a time system unable to reply each and every request, attacker can perform various DOS attack on physical layer it makes jamming of data in data link layer it is collision and exhaustion, at network

layer it is homing, black hole and misdirection, at transport layer it work as de-synchronization.

2.1.7 Node Replication :

In this way of attack where attacker replicate or add the same name of node which have same name and id from existing sensor node from this packet can be corrupted or misguide.

2.1.8 False node:

In this attack where attacker add the false node in a network which contain false information/malicious data that make abstraction in path of routing data packet. Its very dangerous attacks performed in wireless sensor network.

2.2 Passive Attack

In this attack where attacker can monitoring in communication channel from unauthorized access, that kind of monitoring is known as passive attack, this is common attack usually done in sensor network.

2.2.1 Attacking on the basis of Traffic Analysis:

When the massage is transmitted in the presence of certain Encryption Algorithms, it leave the possibility of analysis of communication pattern. Sensor activity can reveal the more information that make adversary that cause harm in sensor network.

2.2.2 Monitoring :

In this kind of attack which is majorly done in sensor network from this privacy of data get affected by snooping that could easy discover in communication channel.

2.2.3 Camouflage Adversaries:

Add external node that hide sensor network, after that it make identical copy of existing node for attack on data packet, from this harm on privacy and misroute the packets.

III.BASIC SECURITY CONCEPT IN NETWORKING

Generally, the major issue in a challenge is directly employing with a size of sensors, Rapidly providing processing power on a data packet, size of memory with respect to tasks performed from the sensor nodes, as limited capacity [8] [9]. Considering secure transmission over sensor network in between sensor, we use several cryptographic techniques symmetric/asymmetric ciphers key. In current Scenario, there are many challenges related to Symmetric/Asymmetric cryptography commonly shown below.

3.1 Asymmetric Cryptography

In Asymmetric Cryptography Public-key cryptosystems heavy to use in WSNs. However, recent works show successful implant be considered as heavy use of WHN Network. It uses public-key cryptography in sensors devices.

In [10], Gura et al. report that both encryption algorithms RSA and elliptic curve explain the possible of cryptography for small devices without running hardware. In particular, Gura et al. demonstrate that ECC point multiplication on small devices which is comparable to RSA public-key operations and an order of magnitude that faster than RSA private-key.

In [11], Watro et al. show that part of the RSA cryptosystem can be successfully applied to the current scenario of wireless sensors.

In [12], Malan et al. demonstrate a working of Diffie-Hellman based on the Elliptic Curve Discrete Logarithm Problem. In this public keys will be generated within 34 seconds, that shared distributed among nodes within sensor network by using 1 kilobyte of SRAM and 34 kilobytes of ROM.

As per result RSA and Diffie-Hellman based on the elliptic curve that is possible for tiny sensor nodes, that help to achieve the good result from small keys that reduce computational time.

3.2. SYMMETRIC CRYPTOGRAPHY

The idea behind the symmetric cryptography is to load secret data within the sensor nodes before they divided data packet in a network. The secret data will be secret from the secret key itself from the help of sensor they derive the real secret key. From this real securely communication establish because they are using secret key encryption/ decryption technique[9]. From this technique, another problem introduces one node can (access to the pre-loaded key) that compromise the entire network. In terms of the solution, they use the pair of keys that overcome inconsistency within the network.

IV.CONCLUSION

Wireless sensor network growing continuously, it makes rapidly incremented graph that deals with digital technology with sensors, as mentioned sensors are small in size with low processing capacity with a certain amount of memory but after all sensors makes life more simple to find solution of variously complicated situation and main advantage in security in every digital application. In WSN there are a lot of different model accordance with the scenario but we required one of the models that can be used in all scenarios and this is next point of research.

REFERENCES

[1] I.F.Akyildiz et al., "A Survey on Sensor Networks", IEEE Commun.Mag.,Vol. 40, No. 8, pp.102-114, Aug. 2002.

[2] HBE-Zigbex. Ubiquitous sensor network. Zigbex Manual [Online]. Available: http://www.hanback.co.kr

[3] 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.

[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, 47(6):53–57, Jun. 2004.

[5] E.Shi and A.Perrig, "Designing Secure Sensor Networks", Wireless Commun. Mag., Vol. 11, No. 6, pp.38-43, Dec 2004.

[6] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", [7]International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[8] Kaplantzis, S., "Security Models for Wireless Sensor Networks", 2006, http://members.iinet.com.au/~souvla/transferfinal-rev.pdf

[9] Y Xiao, VK Rayi, B Sun, X Du, F Hu, M Galloway, "A survey of key management schemes in wireless sensor networks", Computer Communications 30(11-12), 2314–2341, 2007.

[10] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs", Sun Microsystems Laboratories, http://www.research.sun.com/projects/crypto.

[11] Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner, Charles Lynn and Peter Kruus, "TinyPK: Securing Sensor Networks with Public Key Technology", Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks SASN'04, pp. 59-64, Oct.2004

[12] David J. Malan, Matt Welsh, Michael D. Smith, "A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography", Division of Engineering and Applied Sciences, Harvard University, Dec 2007.