AN OVERVIEW OF VARIOUS ATTACKS AND DEFENSIVE MEASURES IN WIRELESS SENSOR NETWORK

[1]V.Thilagavathi, [2]Dr. N. Nagadeepa
[1]Research Scholar (Part-Time)
Bharathiar University/Coimbatore/Tamil Nadu, India
[2]Karur Velalar College Of Arts And Science For Women
Kuppam(Po)/ Karur / India

Abstract

Today the WSN, playing a significant role in home security, habitat monitoring, battlefield-monitoring system, chemical industries, has a major security problem. Due to the deployment of WSN in open access environment and its resource constrained features such as limited bandwidth, limited computational ability, poor memory, low energy etc, WSN is vulnerable to various attacks such as Sybil attack, node clone attack, packet modification attack, node-dropping attack etc. In recent years, numerous data security protocols, such as symmetric encryption, key authentication, Key pre-distribution scheme, have proposed for securing the data transmitted between sensors and base station. This paper gives an overview of various adversary attacks in the various layers of WSN and defense mechanism used to avoid the mismanagement of sensors data.

Keywords: Wireless sensor network, adversary attacks, defense mechanism, Key management.

I. INTRODUCTION

Wireless sensor network comprises a large number of autonomous sensors, gateway node and base sensed data between the sensors, user and base station. WSN used in real-time application such as habitat monitoring system, battlefield, chemical industries, home security system etc [1]. In WSN, sensor collects and processes environmental data. It transmits to another sensors and base station. The sensor that deployed in open access, harsh and remote unattended environment, is self-configuring and resource constrained by low battery power, low bandwidth, poor memory and limited computational capability [2][3]. Sensors use a small event-driven OS called TinyOS. It consumes 4KB memory out of 8KB. The remaining 4KB used for the security purposes.

In WSN, data security is a big problem due to the salient features of sensors. During data transmission, adversary node captures and misuses this valuable information. However, due to resource constrained and deployment of a sensor in an adversarial environment, WSN is highly vulnerable to various attacks such as clone attack, packet modification attack, packet dropping, packet misrouting, etc [4][5].

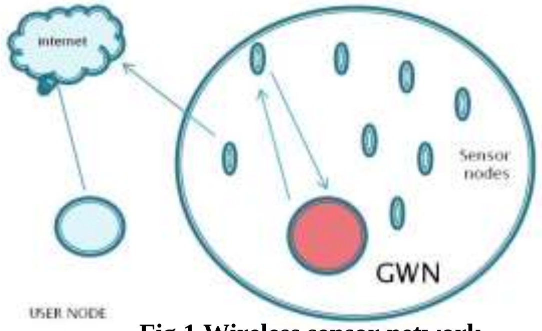

Fig.1 Wireless sensor network

For some application like military applications, WSN lacks in security because of the wireless communication used by sensors. In wireless communication, the eavesdropper can monitor the broadcast medium, intercepts and injects the malicious packets through the broadcast medium. Due to the deployment of a sensor in open access insecure environment, the adversary physically abducts the sensor, changes the cryptographic material through trans-analysis and deploy as an authorized node. WSN is also vulnerable to resource consumption attack. In this attack, the intruder node sends a packet repeatedly to drain the energy and waste the bandwidth.

A. Various attacks on WSN

WSN is vulnerable to various attacks due to the deployment of sensors in the hostile environment. This section discusses some of the attacks. The adversary can launch an attack at a various level such as a router, communication and at various layers of the wireless sensor network.

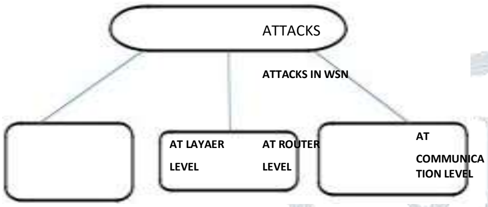

Fig.2. Attack at various level of WSN

a. Physical layer attacks

The Main function of the physical layer is the selection of frequency, carrier frequency generation, detection of the signal, etc. The radio-based wireless medium used in WSN causes following types of attacks

- **Radio jamming attack**

Radio jamming attack is the physical layer attack that compromises the network communication. The attacker frequently jams the spectrum band by introducing intermittent radio interferences for degrading the conditions of the channel. This attack changes one bit in a packet so that receiver never accepts and can drop the packet. Spread Spectrum communication and Bluetooth are the most commonly used techniques to counteract the radio jamming attack.

- **Tampering attack**

In tampering attack, the adversary physically captures the legitimate node, destroy or modify that node in order to get the control of that node and make it as an entry point to launch the attacks. To protect the device from the tampering attack, tamper-proof materials are used or the information stored in that node deleted when the attacks found.

b. Link Layer attack

The major function of link layer is the detection data frame, multiplexing of data streams, medium access control, error control, etc. Link layer suffers from the following attack.

- **Collision attack**

In this attack, the attacker attempts to disrupt the transmission of data packets using illegal activities. Due to these interferences, packets retransmitted in MAC protocol. Furthermore, the attacker uses handshaking techniques for draining the energy and misusing the bandwidth of sensors. This mismanagement of resources of WSN called resource exhaustion attack [7].

c. Network layer attack

- **Black hole attack**

In this attack, the adversary acts as a forwarder of data packets by attracting the neighbor nodes to transmit data packets through the adversary node. Furthermore, the adversary discards all the data packets so that the data packets never transmitted to the destination.

- **Selective forwarding attack**

In Attack, The adversary dropped only the selected packets that match the predefined parameters, not all the packets like black hole attack [8].

- **Sinkhole attack**

In this attack, a malicious node attacks all the traffic listens to the route request from the sensor and provides the false route information for a route-requesting sensor. The sinkhole attack is very hard to detect because it is difficult to verify the routing information provided by the malicious node [8].

- **Wormhole attack**

In this attack, the compromised node establishes a low latency broadband channel with another node situated in the distinct location. Then the compromised node receives a packet, transmits it through a secret channel and reply to a node in distance location.

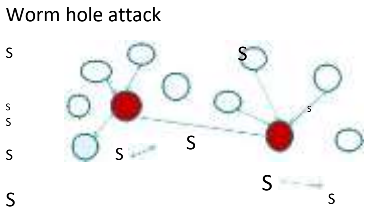

Fig. 3 Wormhole attack

These spatial changes in the network collapse the network topology. This dangerous attack can damage the network protocol and services provided by the network. Furthermore, wormhole attacks are difficult to detect because they use a private low latency broadband channel that is invisible to the sensor [8][9]. To defend against the wormhole attack, Intrusion detection techniques preferred. In this technique, IDS agent that installed in sensors runs independently. This agent sends an alarm message to all the sensors whenever a malicious node found.

- **Sybil attack**

In this attack, the compromised node illegitimately steals the multiple identities of a legitimate node by injecting the false data packets, creates a duplicate identity of a legitimate node for reducing the efficiency and capabilities of fault-tolerant techniques like distributed storage, routing protocol [9].

- **Rushing attack**.

In this attack, the attacker provides a route discovery procedure for route requesting node. Then the attacker forwards all the route request messages its neighbor nodes without following the protocol rules. So that attacker becomes a part of the route between the source and destination node during the entire data transmission.

- **Replaying attack**

Packet replaying attack is an important threat to network communication that intercepts the messages and replays that message into the network with some delay. This delayed messages, create a problem in WSN and the routing protocol becomes failed.

d. Transport layer attacks

- **Flooding attack**

In hello flood attack, the compromised node broadcasts a hello message to all deployed sensors and pretends like a node that occurs very closest to a base station. After receiving the HELLO message, the sensor transmits the secret information through a malicious node.

- **De-synchronization attack**

In this attack, the adversary disrupts the communication between two legitimate nodes by sending the fake data packets repeatedly. The adversary uses the sequence numbers as in real packets, for the fake data packets to make the false node as a legitimate node.

e. Attacks on data aggregation

Data aggregation used to combine various sensor data for avoiding the redundant information, reducing the size of packets and number of transmission. This feature attracts the attacker for launching the attacks [10].

f. Denial of service attack

In WSN, the denial service attacks occur in various layers protocol stack. The attacker can modify the packets before transmitted them to the receiver. Furthermore, this attack modifies one or more bits in the data packets by introducing the radio interference. This modification of data bit causes a denial of a service error.

g. False report

The important application of sensors is to detect a specific event in the surroundings and send their notifications to a base station Due to this; sensors waste much of their energy. To overcome this problem, data fusion node, compromised by other sensors, prepares and sends a final report to the base station. However, if the fake node becomes a data fusion node then it mismanages the data fusion procedure. Finally, the malicious node sends the fake report to a base station. Furthermore, injection of a fake report cannot identify by authentication.

h. Node replication

In this attack, the attacker creates a large number of replicas of the malicious node at different places in WSN. This attack supports the attacker from avoiding the misbehavior detection by injecting the false data. To prevent this attack, distributed detection of node replication protocol used. In this protocol, each sensor knows its location and passes their location identity to a witness node. If the witnessed node finds significant differences in the location information, then it concludes that malicious node found.

III. DEFENSE MECHANISMS

To defend against various attacks in WSN, a large number of defense mechanism and protocols used. This section presents different defense mechanism used in the security of wireless sensor network. To defend against the physical attack, tamper-resistant hardware used that protects the content of memory used in the sensor from the intruder.

A.Symmetric and public key cryptography

Public key cryptography provides a confidentiality, integrity, and authenticity. Due to the resource-constrained features of WSN, public key cryptography algorithms such as RSA (Rivest et al. 1983) and ECC (elliptic curve cryptography)(Menezes et al. 1996) are very hard to implement. Symmetric cryptography is a most commonly used technique in WSN. However, the key distribution between sender and receiver is the major problem in secure data communication.

B. Key management

Symmetric cryptography needs a reliable and secure establishment of the shared key among neighboring sensor nodes. For example, Peer Intermediaries for Key Establishment (PIKE) protocol uses trusted intermediate nodes to establish secret shared keys between the source and the destination node. This protocol uses N*N matrix where each entry in the matrix represents the node's ID. Then every sensor (i,j) in the WSN, shares a pairwise key with (1,j),(2,j), etc.

C. Defense mechanism against Denial of Service attack

Denial of Service attack needs effective measures to prevent this attack throughout wireless sensor network. For example, WSN uses spread spectrum techniques to reduce the damage of the jamming attack.

Furthermore, to prevent collision attack found in the link layer, error-correcting codes preferred. The spoofing and alteration attack found in network layer needs a preventive measure using MAC. To defend against the Path based Denial of Service (PDoS) attack, Sensor uses the hash chain to validate the received data packets.

D. Defense mechanism against Aggregation attack

Simple aggregations such as sum, maximum, minimum, etc creates a major security threat in WSN. Delayed authentication and delayed aggregation techniques defend against the aggregation attack.

E. Defense mechanism against routing attack

The outsider attacks in WSN can prevent using data encryption and authentication using a pair wise key or common key. However, these techniques are inefficient for the insider attack using a compromised node in WSN [11].

The verification of node's ID prevents the Sybil attack. The defensive measures against the sinkhole attack are very difficult because the defensive protocols for this attack establish a route based on the energy measurement that is very difficult to verify. To resist this attack, geographic routing used because this routing technique creates a topology based on localized instructions, not the instructions from the base station [12][13].

IV. CONCLUSION

WSN have many challenging features such as limited bandwidth, storage, processing capability, In WSN, security becomes a major role to maintain efficiency and good performance of the network. WSN used in the much real-time application. Due to the deployment sensor in open access insecure environment and the salient features of the sensor, WSN is highly vulnerable to a variety of attack and WSN security is the challenging task. Many security techniques have preferred especially cryptographic techniques for securing the wireless sensor network. This proposed work attempts to review various security vulnerabilities, attacks found in different layers of WSN and discuss the prominent defensive measures against attacks.

References

[1] IAN F.Akyildiz, Weilian Su, YogeshSankarasaubramaniam, ArdialCayirci, A survey on Sensor Networks, IEEE Communications Magazine, August 2002, pages 102-114.

[2] sljepcevic, S. potkonjak, M., "Power Efficient Organization of Wireless Sensor Networks", Department of Computer Science, University of California, Los Angels, CA 90095-1596.

[3] Walters, J.P., Liang, Z., Shi W. and Chaudhary V., "Wireless Sensor Networks: A Survey", Auerbach Publications, CRC press.

[4] Michael Riecker. Et al," A Survey on Intrusion Detection in Wireless Sensor Networks", Technical Report, SEEMOO-TR-2011.

[5] Bryan Parno et al, "Distributed Detection of Node Replication Attacks in Sensor Networks",IEEE 2005.

[6] Zia, T. A., & Zomaya, A. Y., "A lightweight security framework for wireless sensor networks",J. Wirel. Mobile Networks., UbiquitousComputing.Dependable Appl.(JoWUA), 2, 53-73,2011.

[7] Karlof, C., Sastry, N., and Wagner, D. " TinySec: A link layer security architecture for Wireless Sensor Networks". Proc. of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, 2004.

[8] Alzaid, H., Foo, E., Nieto, J.G. "Secure Data Aggregation in Wireless Sensor Network: A Survey", In Proceedings of the Australian Information Security Conference; Ljiljana, B., Mirka, M., Eds; Australian Computer Society, Inc.: Darlinghurst, Australia, 2008; pp. 93–105.

[9] Jalil Jabari Lotf, Seyed Hossein Hosseininazhad Ghazani, "Security and Common Attacks Against Network Layer In Wireless Sensor Networks", J. Basic. Appl. Sci. Res., 2(2) pp. 1926-1932, 2012.

[10] Yuanyuan Zhang, Wassim Znaidi, C´Edric Lauradoux And Marine Minier," Flooding Attacks Against Network Coding And Countermeasures ", pp. 305-309, IEEE 2011.

[11] Hyojin Kim, Ramachandra Bhargav Chitti, And Jooseok Song," Novel Defense Mechanism Against Data Flooding Attacks In Wireless Ad Hoc Networks", IEEE Transactions On Consumer Electronics, Vol. 56, No. 2, pp. 579-582 May 2010.

[12] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview On Its Security Threats," IJCA Special Issue On "Mobile Ad-Hoc Networks" Manets, pp. 42-45, 2010.

[13] Virendra Pal Singh, Sweta Jain And Jyoti Singhai, "Hello Flood Attack And Its Countermeasures In Wireless Sensor Networks", IJCSI International Journal Of Computer Science Issues, Vol. 7, Issue 3, No 11, pp. 23-27, May 2010.