IJETCR Open Access

ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 3; Issue 2; Page No. 72-75

Wireless Sensor Network Security: A Survey

[1]Abhishek Chaudhary, [2] Nalin Chaudhary, [3] Aasiya Khatoon

[1]Assistant Professor (C.S.E), Bhagwant University, Ajmer, Rajasthan, India

abhishek02mar@rediffmail.com

[2]M.Tech Scholar (C.S.E), Bhagwant University, Ajmer, Rajasthan, India

nalin23jan1990@gmail.com

[3]M.Tech Scholar (C.S.E), Bhagwant University, Ajmer, Rajasthan, India

ashi.shiekh@gmail.com

ABSTRACT

As wireless sensor networks continue to grow, so does the need for effective security mechanisms. A wireless Sensor network consists of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed. Due to the reason that the sensor nodes are highly distributed, there is a need of security in the network. Due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional net-work/computer security. There is currently enormous research potential in the field of wireless sensor network security. We survey the major issues in wireless sensor network security, and present the constraint and the requirements in the sensor security. This paper focuses on the various current attacks on wireless sensor network, and finally prevention from attacks.

Keywords: Introduction, Constraint to security, Attacks, Prevention from Attacks.

INTRODUCTION:

Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges [1]. Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. But sensor networks also introduce several resource constraints due to their lack of data storage and power. Both of these represent major constraint to the implementation of traditional computer security techniques in a wireless sensor network. The unreliable communication channel and unattended operation make the security defenses even harder. Many researchers have begun to address the challenges of maximizing the processing capabilities and energy reserves of wireless sensor nodes while also securing them against attackers. All aspects of the wireless sensor network are being examined including secure and efficient routing, data aggregation, group formation, and so on.

In addition to those traditional security issues, we observe that many general-purpose sensor network techniques assumed that all nodes are cooperative and trustworthy. This is not possible for most of the case, whereas most of real-world wireless sensor networking applications, which require a certain amount of trust in the application in order to maintain proper network functionality. Researchers therefore began focusing on building a sensor trust model to solve the problems beyond the capability of cryptographic security. In addition, there are many attacks designed to exploit the unreliable communication channels and unattended operation of wireless sensor networks.

We classify the main aspects of wireless sensor network security into four major categories: the constraint to sensor network security, the requirements of a secure wireless sensor network, attacks, and defensive measures.

I. CONSTRAINT TO SENSOR NETWORK SECURITY

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks.

1. Very Limited Resources- All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

Corresponding author: Abhishek Chaudhary

- **Limited Memory and Storage Space**-
- **Power Limitatio**n-

2. Unreliable Communication- Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

- **Unreliable Transfer**
- **Conflicts**
- **Latency**

3. Unattended Operation- Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes:

- **Exposure to Physical Attacks**
- **Managed Remotely**
- **No Central Management Point**

III. SECURITY REQUIREMENTS

In this section we discuss different types of security requirements for wireless sensor networks. Any compromise on these requirements can cause a huge destruction in the network.

1. Data authentication: - Authentication is very necessary to verify that the data which are sent by correct sensors or not so that forge data is not received by false sender. Data authentication can be achieved by using a secret key by both the sender and receiver so that the receiver is sure that the data are send by correct source or not. Authentication of a sensor node ensures that he is a legitimate sensor and has the right to send data as well as the sent message by that node has the right contents [2]. In asymmetric cryptographic communication digital signatures are used to check the authentication of any message or user while in symmetric key MAC, are used for authentication purpose.

2. Data confidentiality: - Data should be protected from intruders. Data confidentiality is a property of data, usually resulting from legislative measures, which prevents it from unauthorized disclosure. Confidentiality of the network means that data transfer between sender and receiver will be totally secure and no third person can access it (neither read nor write).

3. Data integrity: - As a process, data integrity verifies that data has remained unaltered in transit from creation to reception. Wireless sensor networks are mostly used for security purposes therefore data integrity is very important in such networks. Data integrity ensures that data packets received at destination is exactly the same transferred by the sender and no one in the middle alters that packet WSNs mostly works on broadcasting therefore it is more vulnerable to such security attacks. As a state or condition, Data Integrity is a measure of the validity and fidelity of a data object.

4. Data availability: - Data should be available as and when required. To make data available it should be replicated. In order to ensure the availability of network resources. The sensor nodes may survive for more time if it save its energy or properly utilize it. When there is no activity in the network or the situation is normal as accordingly then sensor nodes may go in sleep mode to save their energy and utilize it in emergency scenario. In normal situation only few nodes are in active mode of operation. Whenever there is an attack the base station is responsible to activate all sensor nodes in sleeping mode.

5. Secure localization: -To locate the accurate position of the sensor node. Accurate location of a sensor node is very important for data forwarding as well as trust management. There are 2 main types of localization Range based and range free based [2], [3]. Range based approach is normally used in wireless sensor networks. In real time applications a lack of smart tracking allows an attacker to send incorrect location using false signal. So the data may be sending to intruders.

6. Data freshness: - Data freshness implies that the data is recent, and it ensures that no adversary replayed old messages. Data Freshness means the time when that packet was sent is recent or not. For security and avoidance of self destruction data freshness is very important in wireless sensor networks. Because an attacker can send an expire packet to waste the network resources and also cause self destruction.

IV. ATTACKS ON WSN

Security of WSNs is the main issue. The data obtained by sensor node should be kept confidential so that the data received by sensor nodes should be safe and unchanged. The malicious node may de send false data to the network. It may intercept the private information. The different types of attack are:

1. Denial of service: - It prevents legitimate network users from accessing services or resources to which they are entitled. This attack may have target a particular user or entire network. If the target is particular user an entity may suppress all messages directed to a particular destination and in another case is disruption of an entire network either by overloading the network with messages or by disabling the performance to degrade performance. Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action [3], [4], [5]. The simplest denial of service attack tries to exhaust the resources available to the victim node by sending

extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. Denial of service attack is meant not only for the adversary's attempt to disrupt or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of denial of service attacks in different layers might be performed. At physical layer the denial of service attacks could be jamming and tampering. At link layer exhaustion, collision, unfairness. At network layer neglect and homing, misdirection, greed, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent denial of service attacks include payment for network resources, strong authentication and identification of traffic.

2. Selective Forwarding attack: - In the selective forwarding attack the sensor node doesn't forward many of the data or packet which they received. In this the nodes forwards only the selected data and ignore the rest of the data which cause the loss of lots of data.

3. Malicious node: - It is caused due to the insertion of false data.

4. Passive attack: - In the passive attack an unauthorized user listen or monitor the communication between two nodes**.** A passive attack attempts to learn or make use of information from the system but does not affect system resources. In this the victim are not able to know about the passive attack because in this the third party or the attacker doesn't change the data. Attacker only observes the data without changing it. Here the requirement of confidentiality gets violated [4], [5]. Detection of passive attack is very difficult since the operation of the network itself doesn't affect. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for attacker to get information from the data overhead.

5. Sinkhole attack: - Also known as black holes occurring at the network layer [7]. It builds a covenant node that seems to be very attractive in the sense that it promotes zero-cost routes to neighboring nodes with respect to the routing algorithm. This results maximum traffic to flow towards these fake nodes. Nodes adjoining to these harmful nodes collide for immense bandwidth, thus resulting into resource contention and message destruction.

6. Sybil attack: - This again is a network layer attack. In this, an awful node presents more than one character in a network. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks [6]. The Sybil attack is efficient enough to stroke other fault tolerant schemes such as disparity, multi path routing, routing algorithms, data aggregation, voting, fair resource allocation, and topology maintenance and misbehavior detection. The fake node implies various identities to other nodes in the network and thus occurs to be in more than one place at a time. In this way, it disturbs the geographical routing protocols. It can collide the routing algorithms by constructing many routes from only one node.

8.Hello flood attack: -In this an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN so that a large number of nodes even far away in the network choose it as the parent. Hello Flood Attack is introduced in .This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission (termed as a laptop-class attacker in) range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbour. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

Table 1: Sensor network layer and attacks

LAYER	ATTACK
Physical Layer	DOS-Jamming, Tampering Sybil
Data-Link Layer	DOS-Collision, Exhaustion, Unfairness Interrogation
Network Layer	DOS-Neglect and Greed, Homing, Misdirection(Spoofing), Black Holes, Flooding Sybil Wormhole Attack
Transport Layer	DOS- Flooding, De-synchronization

V. PREVENTION FROM ATTACK

1. DOS prevention: - Denial of service can be prevented by strong authentication, identification of traffic and pushback. In this the larger data are divided into several small data and every data contain the hash of the next message so that the attacker are not able to hijack the ongoing transmission because it is not easy to construct a message that matches the hash contained in the previous message.

2. Passive attack prevention: -To prevent from passive attack strong encrypt.

3. Selective Forwarding prevention: - To prevent form **selective forwarding attack** multipath routing are used. In the multipath routing the data or packet are send through the path whose nodes are prevented from selective forwarding attack. Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow.

4. Sinkhole attack prevention: -To prevent from the **Sinkhole attack** is to use geographical routing protocol. Geographic protocols construct a topology on demand using only localized interactions and information and without initiation from the base station.

5. Sybil attack prevention: - To prevent from **Sybil attack** unique identity are given to every node in a network. The setup server, before deployment, assigns each sensor node some unique information. The server then creates an identity certificate binding this node's identity to the assigned unique information, and downloads this information into the node. To securely demonstrate its identity, a node first presents its identity certificate, and then proves that it possesses or matches the associated unique information. This process requires the exchange of several messages. Merkle hash tree can be used as basic means of computing identity certificates [3], [4].

6. Malicious node prevention: - This attack basically should be checked in the Routing layer itself.

8. Hello flood attack: - The **Hello flood attacks are** prevented by checking the bidirectional of a link, so that the nodes ensure that they can reach their parent within one hop.

VI. CONCLUSION

In this paper we have described the four main aspects of wireless sensor network security: constraints, requirements, attacks, and preventions. Then we discussed about the security in sensor networks, security issues and various DoS attacks on different layers. Security is an important requirement and complicates enough to set up in different domains of WSN. Our aim is to provide both a general overview of the rather broad area of wireless sensor network security.

REFRENCES:

1. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002
2. Pardeep Kumar and Hoon-Jae Lee," Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey, Sensors, vol 12, Page(s): 55-91, doi: 10.3390/s120100055, 2012
3. Kalpana Sharma and M K Ghose," Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on Mobile Ad-hoc Networks ,MANETs, Sikkim, India, 2010
4. Al-Sakib Khan Pathan , Hyung-Woo Lee and Choong Seon Hong," Security in Wireless Sensor Networks: Issues and Challenges", Advanced Communication Technology, ICACT 8th International Conference, Kyung Hee Univ., Seoul, Volume: 2, Page(s): 6 pp. – 1048, Feb. 2006
5. V.Manjula1 and Dr.C.Chellappan ,"REPLICATION ATTACK MITIGATIONS FOR STATIC AND MOBILE WSN", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2,Pages: 122-133, 2011
6. Pooja , Manisha, Dr. Yudhvir Singh, "Security Issues and Sybil Attack in Wireless Sensor Networks", International Journal of P2P Network Trends and Technology, vol. 3, issue 1, pp. 7-13, 2013
7. C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proc. of the 1st IEEE Int. Workshop on Sensor Network Protocols and Applications (SNPA'03), pp. 113-127, May 2003