Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Wireless Sensor Networks: an Overview on Its Different Attacks

Pruthvika S. Kadu

Department of Computer Science & Engineering

IBSS College of Engineering, Amravati, India

Abstract :- Wireless Sensor networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges wireless sensor networks face today is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future. The wireless communication technology also acquires various types of security threats. This paper discusses a wide variety of attacks in WSN.

Keywords: Wireless Sensor Network(WSN), Security goals, WSN attacks, Denial of Service, Sybil Attack

I. INTRODUCTION

Basically, sensor networks are application dependent. Sensor networks are primarily designed for real-time collection and analysis of low level data in hostile environments. For this reason they are well suited to a substantial amount of monitoring and surveillance applications. Popular wireless sensor network applications include wildlife monitoring, bushfire response, military command, intelligent communications, industrial quality control, observation of critical infrastructures, smart buildings, distributed robotics, traffic monitoring, examining human heart rates etc. Majority of the sensor network are deployed in hostile environments with active intelligent opposition. Hence security is a crucial issue. Sensor networks provide unique opportunities of interaction between computer systems and their environment. Their deployment can be described at high level as follows: The sensor nodes measure environmental characteristics which are then processed in order to detect events. Upon event detection, some actions are triggered. This very general description applies to extremely security-critical military applications as well as to such benign ones (in terms of security needs) as habitat monitoring.

II. SECURITY GOALS FOR SENSOR NETWORKS

As the sensor networks can also operate in an adhoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of adhoc sensor networks. The security goals are classified as primary and secondary [2]. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self- Organization, Time Synchronization and Secure Localization.

The primary goals are:

1. *Data Confidentiality*

Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. A sensor node should not reveal its data to the neighbors.

2. *Data Authentication*

Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets [3]. Data authentication verifies the identity of the senders and receivers. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys. Due to the wireless nature of the media and the unattended nature of sensor networks, it is extremely challenging to ensure authentication.

3. *Data Integrity*

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed. Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by alterations. The integrity of the network will be in trouble when:

• A malicious node present in the network injects false data.
• Unstable conditions due to wireless channel cause damage or loss of data.[1]

4. Data Availability

Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.

The Secondary goals are:

5. Data Freshness:

Even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message. Informally, data freshness [1] suggests that the data is recent, and it ensures that no old messages have been replayed. To solve this problem a nonce, or another time related counter, can be added into the packet to ensure data freshness.

6. Self-Organization:

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the risky environment may be devastating.

7. Time Synchronization:

Most sensor network applications rely on some form of time synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization [1] for tracking applications.

8. Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals. This Section has discussed about the security goals that are widely available for wireless sensor networks and the next section explains about the attacks that commonly occur on wireless sensor networks.

III. TYPES OF ATTACKS ON WIRELESS SENSOR NETWORK

Why is security necessary in WSN? The reasons are many. First of all Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically safe. Attacks on WSNs can be classified from two different levels of views:-

1. Attack against security mechanisms.
2. Attack against basic mechanisms (like routing mechanisms).

In many applications, the data obtained by the sensing nodes needs to be kept confidential and it has to be authentic [9]. In the absence of security a false or malicious node could intercept private information, or could send false messages to nodes in the network. The major attacks are: Denial of Service (DOS), Worm hole attack, Sinkhole attack, Sybil attack, Selective Forwarding attack, Passive information gathering, Node capturing, False or malicious node, Hello flood attack etc. In this section a brief overview on these attacks are presented.

A. Denial of Service (DoS)

It occurs by the unintentional failure of nodes or malicious action. The simplest DoS 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[4][5]. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service [5]. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization.

B. The Wormhole attack

One node in the network (sender) sends a message to the another node in the network (receiver node)[9].Then the receiving node attempts to send the message to its neighbors. The neighboring nodes think the message was sent from the sender node(which is usually out of range), so they attempt to send the message to the originating node, but it never arrives since it is too far away. Wormhole attack is a significant threat to wireless sensor networks, because, this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover neighboring information [10]. Wormhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

C. The Sybil attack

In this attack, a single node i.e. a malicious node will appear to be a set of nodes and will send incorrect information to a node in the network. The incorrect information can be a variety of things [9], including position of nodes, signal

strengths, making up nodes that do not exist. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. However, an insider cannot be prevented from participating in the network, but he should only be able to do so using the identities of the nodes he has compromised. Public key cryptography can prevent such an insider attack, but it is too expensive to be used in the resource constrained sensor networks.

D. Selective Forwarding attack

It is a situation when certain nodes do not forward many of the messages they receive. The sensor networks depend on repeated forwarding by broadcast for messages to propagate throughout the network.

E. Sinkhole attacks

In a sinkhole attack, the adversary's aim is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center [6]. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. As an example, a laptop-class adversary has a strong power radio transmitter that allows it to provide a high-quality route by transmitting with enough power to reach a wide area of the network [6].

F. Passive Information Gathering

An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them [7] [8]. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields.

G. Node Capturing

A particular sensor might be captured, and information stored on it might be obtained by an adversary [7][8].

H. False or Malicious Node

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network [8].

I. Hello flood attacks

The Hello flood attacks can be caused by a node which broadcasts a Hello packet with very high power, so that a large number of nodes even far away in the network choose it as the parent [9]. All messages now need to be routed multi-hop to this parent, which increases delay.

IV. CONCLUSION

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. This paper summarized the different attacks on Wireless Sensor network.

REFERENCES

[1] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002

[2] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006.

[3] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006.

[4] A.D. Wood and J.A. Stankovic, (2002) "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, 2002, pp. 54–62.

[5] David R. Raymond and Scott F. Midkiff,(2008) "Denial-of- Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008, pp. 74-81.

[6] E. C. H. Ngai, J. Liu, and M. R. Lyu, (2006)"On the intruder detection for sinkhole attack in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications (ICC ‟06), Istanbul,Turkey..

[7] Al-Sakib khan Pathan et.al,(2006) "Security in wireless sensor networks: Issues and challenges" in feb.20-22,2006,ICACT2006,ISBN 89-5519-129-4 pp(1043-1048)

[8] C. Karlof and D. Wagner, (2003). "Secure routing in wireless sensor networks:Attacks and countermeasures," AdHoc Networks Journal, vol. 1, no. 2–3,pp. 293–315, September

[9] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks", Commun.

[10] ACM,47(6):53-57. Zaw Tun and Aung Htein Maw,(2008)," Worm hole Attack Detection in Wireless Sensor networks", proceedings of world Academy of Science, Engineering and Technology Volume 36, December 2008, ISSN 2070-3740.

