Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Issues in Wireless Sensor Network

Dr. N. Krishna Murthy, Dr. R. Selvam
Assistant Professor, Department of Computer Science, Sri Subramanyaswamy Government Arts College, Thiruvallur District, Tiruttani– 631 209, Tamil Nadu, India

Abstract: Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. WSN consists of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed. Security is an important issue nowadays in almost every network. It has posed numerous unique challenges to researchers. It focuses on the challenges related to the security of Wireless Sensor Network and begins with the concept of WSN. The introductory session begin with brief information on the WSN components and its architecture and then with the major security issues over WSN. It proposes some security mechanisms against these threats in WSN.

Keywords – WSN Architecture, Cryptography and Stenography, Types of WSN, Security in Wireless Sensor Network (WSN), Attacks.

I. INTRODUCTION

Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors. These nodes consist of three main components-sensing, data processing and communication. Two other components are also there called, aggregation and base station. The ways the sensors are deployed can either be in a controlled environment where monitoring and surveillance are critical or in an uncontrolled environment. We explore the security issues and challenges for next generation wireless sensor networks and discuss the crucial parameters that require extensive investigations.

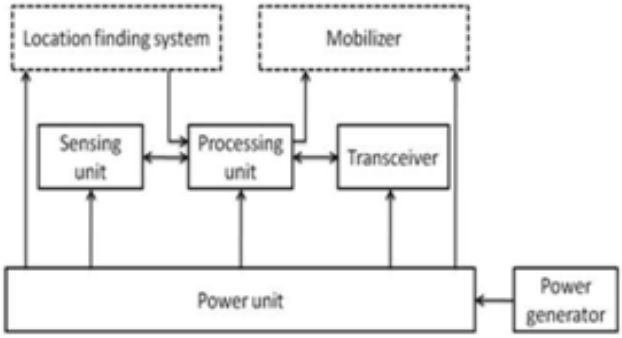

Fig.1 Sensor node components

II. WSN ARCHITECTURE

The WSN components are as follows:

There are several parts of sensor network nodes, each nodes are categorised into a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for.

1 Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.
2 Gateway or Access points – A Gateway enables communication between Host application and field devices.
3 Interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.
4 Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

The network nodes are one or more distinguished components of the WSN with much more computational, energy and communication resources. The main role of a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables. Many techniques are used to connect to the outside world including mobile phone networks, satellite phones, radio modems, high power Wi-Fi links etc.

III. DATA TRANSMISSION

For the secure transmission of information over networks, several cryptographic, steganographic and other techniques are used in Wireless Sensor Networks.

1. *Cryptography:* Cryptographic techniques can be used to prevent against the secrecy and authentication attacks. In silent attacks, the attacker compromises a sensor node and feeds wrong data. The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks.
2. *Steganography:* While cryptography aims at hiding the content of a message, steganography aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.). The main objective of steganography is to modify the carrier in a way that is not perceptible and hence, it looks just like ordinary. It hides the existence of the covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to steganography and processing multimedia data (like audio, video) with the inadequate resources of the sensors is difficult and an open research issue.

IV. TYPES OF SENSOR NETWORKS

1. *Multimedia WSNs:* In Multimedia WSNs, low cost sensor nodes are equipped with cameras and microphones. These nodes are located in a pre-planned manner to guarantee coverage. Issues in these networks are demand of high bandwidth, high energy consumption, quality of service provisioning, data processing and compression techniques, and cross layer design.
2. *Underground WSNs:* In Underground WSNs, sensor nodes are buried underground or in a cave or mine that monitors the underground conditions. Sink nodes are deployed above the ground to forward the gathered information from the sensor nodes to the base station. These are more expensive than the terrestrial sensor networks because proper nodes are to be selected that can assure reliable communication through soil, rock, water and other mineral contents.
3. *Terrestrial WSNs:* In these, nodes are distributed in a given area either in an ad hoc manner or in pre-planned manner. Since battery power is limited and it cannot be recharged, terrestrial sensor nodes must be provided with an optional power source such as solar cells.
4. *Underwater WSNs:* In these, sensor nodes and vehicles are located underwater. Autonomous vehicles are used for gathering the data from the sensor nodes. Sparse deployment of nodes is done in this network. Main problems that come under this while communicating are limited bandwidth, long propagation delay and signal fading issue.

V. SECURITY IN WSN

Security is one of the major aspects of any system. Traditional WSNs are affected by various types of attacks.

1. Attacks on secrecy and authentication
2. Silent attacks on service integrity
3. Attacks on network availability

Attacks on network availability are also known as denial of service (DoS) attacks. If DoS attacks are promoted successfully, it can badly degrade the functioning of WSNs. The following are the DoS attacks on different network layers:

1. *DoS attacks on the physical layer:* Jamming is the most common way of injecting DoS attack on this layer. Physical layer is engaged with frequency selection, carrier frequency generation, signal detection, modulation and data encryption.
2. *DoS attacks on the link layer:* The attacks when elevated on this layer results in collision, resource exhaustion and unfairness in allocation of frames. Link layer is exposed to multiplexing of data streams, data frame detection, medium access control and error control.
3. *DoS attacks on the network layer:* Network layer is exposed to different types of attacks such as spoofed routing information, selective forwarding, sinkhole, Sybil, wormhole, hello flood and acknowledgment flooding.
4. *DoS attacks on the transport layer:* Transport layer is exposed to flooding attack and de-synchronization attack.
5. *DoS attacks on the application layer:* Application layer is exposed to logic errors and buffer overflow.

Security concern in WSN:

1. *Data Confidentiality:* Confidentiality is an acceptance of authorized access to information communicated from an authorised sender to an authorised receiver. A sensor network must not reveal sensor readings to its neighbours. Highly sensitive data is sometimes routed through many nodes before reaching the final node. For secure communication, encryption is used. Data is encrypted with a secret key that only authorized users have. Public sensor information should also be encrypted to some degree to protect against traffic analysis attacks.

2. *Data Integrity:* Data integrity can be provided by Message Authentication Code (MAC). Integrity of data needs to be assured in sensor networks, which strengthens that the received data has not been tampered with and that new data has not been added to the original contents of the packet.
3. *Data Authentication:* Data authenticity is an assurance of the identities of communicating nodes. Nodes taking part in the communication must be capable of recognizing and rejecting the information from illegal nodes. Authentication is required for many administrative tasks.
4. *Robustness and Survivability:* The sensor network should be robust across various security attacks and if an attack conquers, its impact should be reduced. The covenant of a single node must not violate the security of the whole network.
5. *Self Organization:* A typical WSN may have thousands of nodes fulfilling various operations, installed at different locations. Sensor networks are also ad hoc networks, having the same flexibility and extensibility. Sensor networks crave every sensor node to be independent and ductile enough to be self-organizing and self-healing according to different situations.
6. *Time Synchronization:* Most sensor network applications depend upon some form of time synchronization. In order to skimp power, an individual sensor's radio may be turned off for some time. Moreover, sensors may wish to calculate the end-to-end delay of a packet as it travels between two pair wise sensors.
7. *Secure Localization:* WSN makes use of geological based information for recognition of nodes, or for accessing whether the sensors correspond to the network or not. Some attacks work by investigating the location of the nodes. Attacker may probe the headers of the packets and protocol layer data for this purpose. This makes the secure localization an important feature that must be satisfied during our implementation of security protocol.
8. *Data Availability:* Availability is an insurance of the endowment to indulge expected services as they are designed earlier. It guarantees that the network services are feasible even in the subsistence of denial of service attacks. For making data available, security protocol should obsess less energy and storage, which can be targeted by the reuse of code and making sure that there is slight increase in communication due to the functioning of security protocols. Central point scheme should also be avoided as single point failure will be introduced due to this in a network that threatens the availability.
9. *Flexibility:* Sensor networks will be used in vigorous arena scenarios where environmental circumstances, hazards and mission may change frequently. Changing mission goals may desire sensors to be eliminated from or injected to a settled sensor node. Moreover, two or more sensor networks may be merged into one, or a single network may be divided in two. Key establishment protocols must be ductile enough to render keying for all potential scenarios a sensor network may encounter.
10. *Data Freshness:* Data freshness ensures that the data communicated is recent and no previous messages have been replaced by an adversary. Data freshness is classified into two types based on the message ordering; weak and strong freshness. Weak freshness provides only partial message ordering but gives no information related to the delay and latency of the message. Strong freshness on the other hand, gives complete request-response pair and allows the delay estimation. Sensor measurements require weak freshness, while strong freshness is needed for time synchronization within the network. For ensuring the freshness of a packet, a timestamp can be attached to it. Destination node can compare the timestamp with its own time clock and checks whether the packet is valid or not.

Attacks:

Wireless Sensor Networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Basically attacks are broadly classified in two categories i.e. active attacks and passive attacks. This paper points out both of these attacks in details.

Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. Some of the more common attacks against sensor privacy are:

1. *Monitor and Eavesdropping:* By snooping to the data, the adversary could easily discover the communication contents.
2. *Traffic Analysis:* Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.Even when the messages transferred are encrypted; it still leaves a high possibility analysis of the communication patterns.
3. *Camouflage Adversaries:* One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

1. *Routing Attacks in Sensor Networks:* The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the messages.

2. *Attacks on Information in transit:* In a sense or network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to Interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks.
3. *Black hole/Sinkhole Attack:* In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. In fact, this attack can affect even the nodes those are considerably far from the base stations.
4. *Wormholes Attacks:* In the wormhole attack, pair of awful nodes firstly discovers a wormhole at the network layer. A wormhole is a low-latency junction between two sections of a network. The malicious node receives packets in one section of the network and sends them to another section of the network. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location. This may cause congestion and retransmission of packets squandering the energy of innocent nodes.
5. *HELLO flood attacks:* An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN.
6. *Denial of Services:* Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. In wireless sensor networks, several types of DoS attacks in different layers might be performed.
7. *Node Malfunction:* A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader.
8. *Physical Attacks:* Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.
9. *Message Corruption:* Any modification of the content of a message by an attacker compromises its integrity.
10. *False Node:* A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur.
11. *Node Replication Attacks:* Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted.
12. *Passive Information Gathering:* An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.

VI. CONCLUSION

Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. Wireless Sensor Network product in industry will not get acceptance unless there is a full proof security to the network. In this paper discussed the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks and also discussed about various security concern in WSN (confidentiality, integrity, authenticity, availability etc.) Then I discussed about the security in sensor networks, security issues and various DoS attacks on different layers.

REFERENCES

[1] Aashima Singla, Ratika Sachdeva, International Journal of Advanced Research in Computer Science and Software Engineering, Volume3, Issue 4, April 2013.

[2] Vikash Kumar, Anshu Jain and P.N. Barwal – International Journal of Information & Computation Technology, Volume 4, Number 8 (2014), pp. 859-868.

[3] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong – Security in Wireless Sensor Networks: Issues and Challenges – pp 1043-1048.

[4] B. Krishnamashari, D. Estrin and S. Wicker, "Impact of Data Aggregation in Wireless Sensor Networks", Proc. 22nd International Conference Distrib. Comp. Systems, Jul. 2002.

[5] R. Ramen, J. Lopez, S. Gritzalis, "Situation awareness mechanisms for wireless sensor networks ", IEEE Communication Magazine, vol. 46, no. 4, pp. 102-107, Apr. 2008.

[6] Rina Bhattacharya, "A Comparative Study of Physical Attacks on Wireless Sensor Networks", *IJRET*, vol. 2, issue 1, pp. 72-74, Jan 2013

[7] S. Rajasegarar, C. Leckie, and M. Palansiwami, "Anomaly detection in wireless sensor networks", IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp. 34-40.

[8] A.D. Wood, J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, Vol. 35, Issue 10, pp. 54-62, October 2002

[9] I.F. Akyildiz, W. Su, Y.Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", *IEEE Communications Magazine* 40 (8) (2002) 104–112

[10] Shio Kumar Singh, M P Singh, D K Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", *International Journal of Computer Trends and Technology*-, May to June Issue

2011, ISSN: 2231-2803

[11] 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

[12] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", *IJCIT*, vol. 2, issue 1, pp. 62-67, 2011

[13] Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.

[14] Römer and Mattern, The Design Space of Wireless Sensor Networks. IEEE Wireless Communications, 2004.

[15] X. Wang, W. Gu, K. Schosek, S. Chellappan, D. Xuan, "Sensor network configuration under physical attacks", *International Journal of Ad Hoc and Ubiquitous Computing*, Vol 4, Issue 3/4, pp. 174-182, April 2009

