DEVELOPING A WIRELESS BASED SECURITY MECHANISM AND SECURITY PROTOCOLS TO ENHANCE DATA SECURITY

Gautam Anand

Student, Sanskriti School, Chanakyapuri

ABSTRACT

Wireless sensor network provides an infrastructure that comprises of densely distributed sensors sensing the environmental changes, processing detected signals and communicating with other sensors. The sensors self-configure themselves to operate and adapt to the changing environment without human intervention. Due to the unique characteristics and unattended operating environment of sensor, they become attractive targets for the attacker for lancing attacks like unauthorized access, tampering and physical assault. Hence, designing of security protocol for providing integrity, authenticity, confidentiality, privacy, etc. becomes mandatory. The paper discusses the necessity of security services and security protocols for the secure communication and transmission of data in a wireless sensor network.

1. INTRODUCTION

WSN, comprising of a large number of low-cost, independent sensors contains a low-speed microcontroller, radio transceiver, battery and high resourced base station. WSN has no fixed infrastructure where every sensor is self-configuring, self-healing, and adapting to a different environment [1]. In the distributed nature of WSN, the lightweight sensors are deployed in a hostile environment for sensing the physical parameters of the environment such as pressure, temperature, humidity, pollutants etc. The sensors are used in real-time applications like home security system, environmental monitoring, chemical industrial monitoring system and battlefield surveillance [2]. The sensor senses the ecological conditions, processes that information and communicates with other sensors and base station through radio frequency technologies. Fig 1 represents the structure of heterogeneous wireless sensor network.

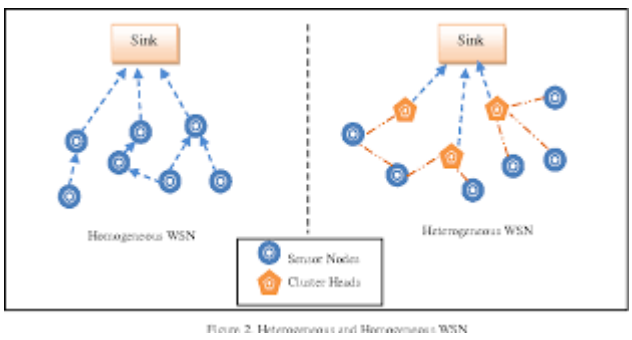

Fig 1 heterogeneous wireless sensor network

Due to the deployment of sensors in remote, unattended areas, the adversaries can easily launch various attacks like physical attacks, tampering attack, node clone attack etc. Furthermore, the sensor is resource-constrained. Hence, it is tough to differentiate security breaches and node failure. Network security provides security mechanisms, policies and services to protect the network from unauthorized access. Most of the security mechanisms offer confidentiality, integrity and availability. WSN demands a security mechanism to protect the sensor and data packets from malicious attacks. Designing of security protocol for WSN is a difficult task due to the following reasons.

1. In WSN, the sensor deploys in open access insecure environment. The sensor uses a radio spectrum for transmitting the data packets between sensors and base station. However, any malicious sensor with same frequency band eavesdrops the classified material transmitted through a wireless channel.

2. Most of the security protocols used in WSN never consider the security mechanism at the design level. Due to this problem, the adversaries launch attacks on data transmission by identifying the security black hole in those protocols.

3. Due to the constrained features of the sensor, it is a difficult task to use strong security algorithms. WSN mostly prefers symmetric cryptographic algorithms.

4. Due to the deployment of the sensor in a hostile area without any fixed infrastructure, it is hard to perform continuous surveillance [3][4].

2. NEEDS FOR SECURITY SERVICES

2.1. Confidentiality

Confidentiality ensures that the secret information can be accessed only by an authorized user. During the data transmission through WSN, confidentiality ensures that data must transmit through the network only by an authorized node. In a wireless network, assurance of confidentiality is very hard to provide because of the wireless communication medium used for the data transmission. The wireless communication uses a wide spectrum that can be eavesdropped by the malicious node using a proper radio transceiver. Furthermore, the attacker monitors the traffic flow, steals the source and destination addresses from the packet headers transmitted through the communication channel and launch attacks. Furthermore, adversary eavesdrops the management packets containing the routing information, obtains the topological information, extracts the identities of cluster head, base station and destroys the entire network. Encryption of data packets is the major technique used to defend against the eavesdropping of data packets.

2.2. Privacy: Privacy, an important security issue, ensures that the attacker never discloses the personal information. In WSN, the adversary node continuously monitoring the traffic flow, gets the identities of source and destination addresses and discloses the information transmitted between nodes.

2.3. Integrity assures that data packets in transit are never modified by the attacker. This security service is the main security service because the receiver has to receive that what the sender transmitted exactly. In order to ensure the integrity of data packets, security protocols use Message Integrity Code (MAC) and digital signature. Packet modification is the prime attack against integrity [5][6].

2.4. Authenticity

Authenticity provides an assurance that the sender receives the data packet only from the legitimate sender. It does not allow the sender to receive false data packets. Security protocol uses the Message Authentication Code (MAC) to avoid receiving false data packets. To calculate MAC, security protocols use the asymmetric key shared by both sender and receiver. Furthermore, the digital signature provides authentication to data packets. Packet injection and Main-in-middle attacks are the major attacks against authenticity [5][6].

2.5. Data Freshness The information transmitted through the wireless network must be fresh and valid in a limited time interval. When the sender transmits a data packet, they must receive that data packet within the time limit. Otherwise, that data packet becomes invalid. Packet replaying is the main attack on freshness [5][6].

2.6. Availability ensures that the network provides the expected services as before designed. Due to the adversary attacks, the functionality of network degrades. Thus, network availability service compromised by an adversary. Selective forwarding, radio jamming, multipath routing and Denial of Task Service (DoS) are the important threats against network availability service

2.7. Non-repudiation ensures that sender as well as a receiver should not deny sending and receiving of messages. Whenever the message is sent, the receiver ensures that the message is sent by the legitimate sender. Similarly, when the message received, the sender ensures that the message received by the legitimate receiver. Non-repudiation protects the data packets from cheating parties. To design a non-repudiation protocol trusted third party (TTP) is used.

Fig 2 represents the CIA model.

3. SECURITY PROTOCOLS USED IN WIRELESS SENSOR NETWORK

3.1. Intrusion Detection Due to the security breaches exists in the design of the network; the attacker breaks the security of wireless network and launch attacks either from inside or outside the network. Furthermore, the adversary eavesdrops the traffic flow and disclose the secret messages transmitted through the system. The intrusion detection techniques these malicious attacks using anomalies [7][8].

3.2. Security Protocols for Sensor Networks (SPINS) The Security protocols for Sensor networks provide two contributions such as Secure Network Encryption Protocol (SNEP) and a micro version of the Timed, Efficient, Streaming, Loss-tolerant Authentication (μTESLA) to provide a counteract against malicious attack.

3.2.1. Secure Network Encryption Protocol (SNEP)

SNMP is the low communication overhead protocol that assures confidentiality, data freshness and data authentication. This protocol ensures authentication and protection against replay attack through encryption technique and Message Authentication Code (MAC). Furthermore, SNEP offers semantic security in that the contract prevents eavesdropping of data packets using encryption. Moreover, this protocol assures the two-party authentication and integrity using MAC [9][10].

3.2.2. μTESLA- μTESLA is the extension of TESLA that authenticates the packets using asymmetric cryptography. In this protocol, the sender encrypts the messages using a secret key and sends it to the receiver with a delayed disclosure of crucial key. The receiver buffers those messages and waits for the secret key from the sender because disclosure of secret key is delayed by the sender. Once key received, receiver authenticates the data packets [9][10].

3.2.4. TinyMCE TinySec is a lightweight security protocol that provides two types of security services such as authenticated encryption, where data packets encrypted and authenticated using MAC and authentication that validates the messages through MAC. TinySec uses a cipher block chaining technique for encryption [11].

3.2.5 ZigBee uses the IEEE 802.15.4 standard that provides access control, confidentiality, integrity and protection against replay attacks. It uses asymmetric encryption with 128 bits' key for securing the data payload. When the sensor issues a request to deploy in the network, ZigBee authenticates that sensor. Furthermore, it distributes the key among sensors in the system and configures the security mechanism to provide end-to-end security between sensors.

3.2.6. LEAP

LEAP, a key management protocol, uses different types of keying mechanisms securing different data packets. This protocol prefers four types of keys, such as individual keys, cluster keys, group keys, and pairwise shared keys. Every sensor has a personal key that is shared with the base station to provide confidentially and calculate MAC. The base station uses the shared key to transmit the encrypted messages to all the sensors used in the network. The

pairwise key is a shared key used by the sensor to communicate with immediate neighbour [12].

3.2.7. PIKE PIKE (Peer Intermediaries for Key Establishment) protocol employs a peer sensor node as a trusted intermediate node for establishing a secret key between two sensor nodes [13]. To create a secret key between two sensor nodes, a trusted intermediate node that shares a pairwise key between both sensors, must be present.

4.CONCLUSION

The miniaturization of computing technology leads to the development of a small and inexpensive sensor that interacts with the physical environment very carefully. Furthermore, the wireless sensor network can be applied in many real-time applications such as healthcare, industrial, environmental, military, biomedical and intelligent parking solutions. This paper provides a general overview of security requirements and security protocols used to establish a secure data communication in a wireless sensor network.