STUDY OF SECURITY ISSUES IN WIRELESS SENSOR NETWORK

MANJU.V.C *

Kerala University, Thiruvananthapuram

Kerala

Email id: MANJU_TVM@YAHOO.COM

Phone no: 09886595205

***Abstract*:** In recent years, the design and implementation of the wireless sensor networks is widely chosen for research as sensor networks enable application that connects the physical world to the virtual world. Wireless platforms are less expensive and are more powerful, with usage in enabling the promise health science to military sensing operations. The wireless sensor networks are prone to more attacks than wired networks. However, the hardware simplicity of these devices makes defense mechanisms designed for traditional networks infeasible. This paper studies the security aspects of wireless sensor networks. A survey with current threats and countermeasures is carried out, in particular, explored the protocol layer attack on sensor networks.

Keywords: Wireless sensor network; security attacks; protocol layer attack;

Introduction

A wireless sensor network (WSN) consists of distributed autonomous sensors to closely monitor physical or environmental conditions (such as temperature, sound, vibration, pressure, motion or pollutants). The applications supported by WSNs vary from monitoring, tracking to controlling.. The Battlefield surveillance used in military operations is the idea behind WSN development. In a typical application, a WSN is scattered in a region where it collects data sensor nodes.

In the era of interconnected world, security of both external and internal data exchange over network nodes is a primary concern. A sensor network constitutes of a wireless ad-hoc network, where each sensor supports a multi-hop routing algorithm (several nodes may forward data packets to the base station). In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source (battery). An attacker can easily intercept, inject or alter the data transmitted between the sensor nodes.

Security attack is a concern for wireless sensor networks because:

→Usage of minimal capacity devices in parts of the systems
→Physical accessibility to sensor and actuator devices
→Wireless communication of the system devices

.In spite of these drawbacks or security attacks, WSN can still function effectively.
These security threats can be handled using structured network security architecture, which includes modifications to traditional security services such as confidentiality, integrity and authenticity to the wireless domain.. Wireless networks are susceptible to which are not adequately addressed through cryptographic methods. One such threat is denial of sleep attack in MAC layer. Denial of sleep attack is targeted on the sensor node's power supply. Due to this attack the network life span can reduce from years to few days.

Necessary Security Requirements

1. Availability

Ensure that the desired network services are available even in the presence of denial of service attacks.

2. Data confidentiality

Confidentiality means restricting data access to authorized personnel. The data should not be leaked across adjacent sensor networks. In many applications, the nodes are used to transfer highly sensitive data. Data encryption using a secret key with access only to authorized users is widely used. .Public key cryptography is

too expensive to be used in the resource constrained sensor networks. Most of the proposed protocols use symmetric key encryption methods.

3. Data authenticity

In a sensor network a hacker/attacker can easily inject messages, so the receiver ensures that the data used in any decision making process originates from the correct source data authentication prevents unauthorized personnel from participating in the network. The authorized nodes should be able to detect messages from unauthorized nodes and reject them. In case of two party communications, the data authentication can be achieved through a purely symmetric mechanism. The sender and the receiver share a secret key to compute a Message Authentication Code (MAC) for all communicated data. When a message with a correct MAC arrives the receiver identifies the sender. .

4.Data integrity

Data integrity ensures that the receiver receives unaltered data in transit by any unauthorized personnel.

5.Data freshness

Data freshness ensures that the recent data is available without any replay of old messages by unauthorized personnel**.**

6.Robustness and survivability

Sensor network should be robust against the various attacks and if an attack succeeds, the impact should be minimized.

7. Self-organization

Nodes should be flexible enough to be self-organizing (autonomous) and self-healing (failure tolerant).

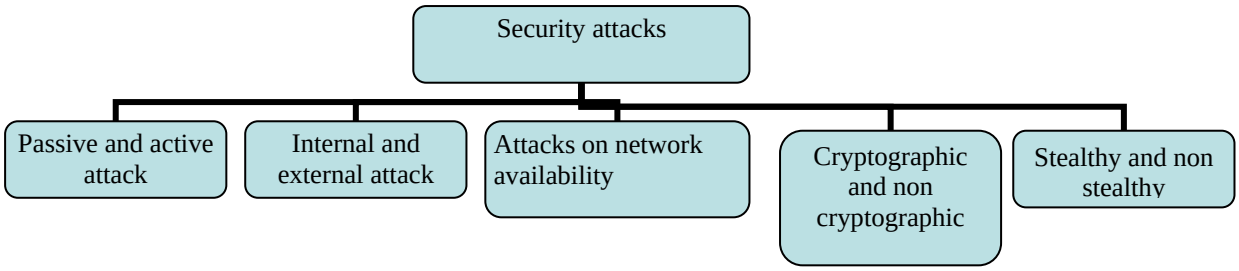
8.Time Synchronization

These protocols should not be manipulated to produce incorrect data.

Attacks on WSN

There are many attacks that have been identified in WSN by the researchers.

These security attacks can be classified on various criteria, such as the domain of the attackers, or the techniques used in attacks. These security attacks in WSN and all other networks can be roughly classified as: passive or active, internal or external, attacks on protocol layer, stealthy or non-stealthy, cryptography or non cryptography related.



1. Passive and active attack

According to the interruption of communication act, attacks are classified as active and passive attack. Passive attack involves data exchange in a network without any interruption in communication. Active attack involves disruption of the normal activity of the network like information interruption, modification or fabrication passive attacks are interception, traffic analysis, and traffic monitoring. Active attacks are jamming, impersonating, and denial of servicing and message replay.

2. Internal attack and external attack

The domain attacks can be classified as internal (insider) or external (outsider) attack.. External attacks are carried out by nodes that are not part of the domain of the network. Internal attacks are from compromised nodes which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows the valuable and secret information

3. Stealthy attacks against service integrity

In a stealthy attack, the goal of the attacker is to make the network accept a false data value. For example, an attacker injects a false data value through that sensor node. In these attacks, keeping the sensor network available for its intended use is essential. DoS attacks against WSNs may permit real-world damage to the health and safety of people.

4. Cryptographic primitive attacks

Most security holes are due to poor implementation of security protocols. For example, authentication protocols and key exchange protocols are often the target of malicious attacks. Cryptographic primitives are considered to be secure; but there were recent collision attacks on hash function (SHA-1) is a concern. Pseudorandom number attacks, digital signature attacks, and hash collision attacks are cryptographic attacks. In Pseudorandom number attacks the packets are made fresh by timestamp or by using the random number (nonce) .The session key is often generated from a random number. In the public key infrastructure the shared secret key can be generated from a random number too. The conventional random number generators in most programming languages are designed for statistical randomness, not to resist prediction by cryptanalysts. In the optimal case, random numbers are generated based on physical sources of randomness that cannot be predicted. The noise from an electronic device or the position of a pointer device is a source of such randomness. However, true random numbers are difficult to generate. When true physical randomness is not available, pseudorandom numbers must be used.

5. Mote class versus laptop class attacks

In mote class attack, WSNs are using few nodes which have similar capabilities to the network nodes. In laptop-class attacks, an attacker can use more powerful devices (e.g., a laptop) to attack a WSN. These devices have greater transmission range, processing power, and energy reserves than the network nodes.

6. Attacks on network availability

Attacks on network availability are often referred to as Denial-of-Service (DoS) attacks. DoS targets any layer of a sensor network.

We reduce the Open System Interconnect model's traditional seven layers to five layers: Physical, Link, Network layer, Transport layer and Presentation layer

- **Physical layer attacks**:

Most wireless communications use the RF spectrum and broadcast medium. Signal wireless broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency. Thus, messages transmitted can be overheard, and fake messages can be injected into the network. Radio signals can be jammed or interfered, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, the generated signal can even overwhelm the targeted signals and disrupt communication. The most common types of jamming attacks in WSN are constant, deceptive, random, or reactive. A constant jamming attack corrupts packets as they are transmitted between WSN nodes. However, this attack requires a significant amount of energy. This attack might not be feasible if the attacker is under similar power constraints as the target network. Instead of transmitting a random signal, a deceptive jammer sends a constant stream of bytes into the network.

- **Link layer attacks**

MAC protocols operate at the link layer, and most require coordination between nodes to arbitrate channel use, making them particularly vulnerable to DoS attacks. Link-layer threats include collisions, interrogation, and packet replay. You can reduce some collisions by using error-correcting codes. However, ECCs adds transmission overhead, consuming additional energy. An interrogation attack exploits the two-way Request-To-Send/Clear To- Send (RTS/CTS) handshake that many MAC protocols use to reduce the hidden-node problem. An attacker can exhaust the nodes resources by repeatedly sending RTS messages to allow CTS responses from a targeted neighbor node. Anti replay protection and strong link-layer authentication can also reduce these attacks. However, a targeted node receiving the bogus RTS messages still consumes energy and network bandwidth.

Another link-layer threat to WSNs is the denial-of-sleep attack, which prevents the radio from going into sleep mode, which is called the denial of sleep attack. MAC protocols are a natural focus for denial-of-sleep attacks. They control the functionality of the transceiver, which consumes more energy than any other component on most wireless-sensor platforms. As a result of differences between the packet structure and timing between WSNMAC protocols, an attacker can determine which MAC protocol is been used by WSN for analyzing network traffic. This information is sufficient to mount an efficient denial-of-sleep attack against most sensor networks employing energy-efficient protocols (such as Sensor MAC (S-MAC), Berkeley MAC (B-MAC), or Timeout MAC(T-MAC))

Denial of Sleep Attack: Medium Access Control (MAC) protocols of state-of-the-art WSN are susceptible to denial-of-sleep attacks which reduces the network life span from years to days. Denial of sleep attack is a specific form of energy consumption of the WSN. The attack imposes large amount of energy consumption on the sensor nodes that the entire charge is consumed by the load levied upon the network and the nodes stop working. In other words, the nodes deny their service. The denial of sleep attack has been mainly noticed in WSN and in wireless such as the PDAs, the laptops and other devices with minimal energy consumption... The low battery of the wireless sensor nodes and consumption of the energy makes the nodes more susceptible to the attacks and hence denial of service through denial of sleep. The power consumption is an important factor in designing wireless sensor network. There are four states exist in wireless sensor module i.e. sending, receiving, idle and standby. In idle state the wireless communication module will monitor the use of wireless channels, to check whether there are any data to receive and close communication model to sleep state. The wireless communication in sending mode takes largest energy consumption while receiving it takes slightly lower than sending state. The minimum energy consumption occurs in sleep state. In sleep mode the transceiver consumes significantly less energy and energy can be saved if the transceiver is kept as much as possible in sleep mode. But denial of sleep attack doesn't allow the sensor node to be in sleep state hence the network life time reduces drastically.

- **Network layer attacks**

The various attacks targeting the network layer have been identified and are studied in research papers. By attacking the routing protocols, attackers can absorb network traffic, inject into the path between the source and destination, and control the network traffic flow. The attackers can create routing loops, introduce severe network congestion, and channel contention into certain areas. There are malicious routing attacks that target the routing discovery or maintenance phase by not following the specifications of the routing protocols. Routing message flooding attacks such as hello flooding, RREQ flooding, acknowledgement flooding, routing table overflow, routing cache poisoning, and routing loop are targeting the route discovery phase. A malicious node advertises routes that change non-existent nodes to the authorized nodes present in the network. This happens in proactive routing algorithms, where routing information is updated periodically. The attacker tries to create enough routes to prevent new routes from being created. The proactive routing algorithms are more vulnerable to table overflow attacks as they attempt to discover routing information before its actual need. An attacker can simply send excessive route advertisements to overflow the receivers routing table. There are attacks that target the route maintenance phase by broadcasting false control messages. More sophisticated and subtle routing attacks have been identified in recent research papers. The black hole (or sinkhole), Byzantine, and the wormhole attacks are the typical examples, which are described below.

Sinkhole/ Black holes attack: The sinkhole attack is an attack in which the attacking node is inserted into the traffic of the network by giving greed to the other nodes that it contains some useful information and allowing its entry.

Wormhole Attack: In wormhole attack, the attacker takes the message from one area and displays in the other area. This makes the adversary eavesdrop upon useful information and display it in another area, thus redirecting the message traffic. The packets of information are tunneled and then displayed.

Sybil attack: The Sybil attack is a case where each node presents more than one identity to the network protocols and affected algorithms include fault-tolerant schemes, distributed storage, and network-topology maintenance. For example, a distributed storage scheme may rely being there with three replicas of the same data to achieve a given level of redundancy. If a compromised node pretends to be two of the three nodes, the algorithms used may conclude that redundancy has been achieved not in reality.

- **Transport layer**

The objectives of Transport layer protocols in WSN include setting up of end-to-end connection, end to- end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection.

SYN flooding attack: The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a –receiver or victim node, but never completes the handshake to fully open up the connection. For two nodes to communicate using TCP, they must first establish a TCP connection

using a three-way handshake. The three messages exchanged during the handshake allow both nodes to learn that the other node is ready to communicate and also agree on initial sequence numbers for the conversation. During the attack, a malicious node sends a large amount of SYN packets to a victim/receiver node, spoofing the return addresses of the SYN packets. The victim after receiving the SYN packets from the attacker, sends them and awaits ACK packet response.. Without receiving the ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed size table while it awaits the acknowledgement of the three-way handshake, all the pending connections would result in overflow of buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection. Session hijacking takes advantage of the fact that most communications are protected (by providing credentials) at session setup, but not later. In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. Thus the attacker impersonates the victim node and continues the session with the target. Hijacking a session over UDP is the same as over TCP, except that UDP attackers do not have to worry about the overhead of managing sequence numbers and other TCP mechanisms. Since UDP is connectionless, edging into a session without being detected is much easier than the TCP

- **Application layer attacks**

The application layer communication is also vulnerable in terms of security when compared with other layers. The application layer contains user data, and supports many protocols such as HTTP, SMTP, TELNET, and FTP, which provide many vulnerabilities and access points for attackers. The application layers attacks are more attractive as they have direct access to the application data

Malicious code attacks: Malicious code, such as viruses, worms, spy wares, and Trojan Horses, can attack both operating systems and the user applications. These malicious programs spread themselves across the network and resulting in computer or network slow down or even damaged.

Repudiation attacks: Repudiation refers to a denial of participation in all or part of the communication.

- **Multi-layer attacks**

Some security attacks can be launched from multiple layers instead of a particular layer. Examples of multilayer attacks are denial of service (DoS), man-in-the middle, and impersonation attacks.Denial of service: Denial of service (DoS) attacks could be launched from several layers and is resulted either by an unintended failure of a node or by unauthorized access of the sensor node. In this case, an intended user is refused of few services. An attacker can employ signal jamming at the physical layer, which disrupts normal communications. At the link layer, malicious nodes can occupy channels through the capture effect taking advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks.

Impersonation attacks: Impersonation attacks are launched by using other node's identity, such as MAC or IP address. Impersonation attacks are the first step for most attacks, and are used to launch More sophisticated attacks.

Man-in-the-middle attacks: An attacker sits between the sender and the receiver and sniffs any information being sent between two ends. In some cases the attacker may impersonate the sender to communicate with the receiver, or impersonate the receiver to reply to the sender.

Conclusion

This paper provides insight on the Wireless Sensor network, its requirement and security concerns with various attacks. Defending denial of sleep attack in MAC layer of resource constrained wireless sensor network with minimum overhead provides significant challenges, and is an ongoing area of research.

References

[1] http://en.wikipedia.org/wiki/Wireless_sensor_network hiqun et al "Link Layer Security Scheme for Wireless Sensor Networks "

[1] Electro/Information Technology, 2007 IEEE International Conference on 17-20 may 2007.

[2] David R. Raymond et al "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols "IEEE Transactions on Vehicular Technology, Vol 58, No.1 January 2009.

[3] James Newsome et al "The Sybil Attack in Sensor Networks: Analysis & Defenses" IPSN'04, April 26–27, 2004, Berkeley, California, USA.

[4] Michael Brownfield et al "Wireless Sensor Network United Denial of Sleep Attack" Proceedings of the 2005 IEEE Workshop on Information Assurance States Military Academy, West Point, NY June 2005.

[5] Rung-Ching Chen et al "An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Networks "JOURNAL OF NETWORKS, VOL. 5, NO. 3 MARCH 2010.

[6] Devesh C. Jinwala et al "Configurable Link Layer Security Architecture for Wireless Sensor Networks" Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.\
[7] Shivangi Raman et al. "Wireless sensor networks: A Survey of Intrusions and their Explored Remedies" International Journal of Engineering Science and Technology Vol. 2(5),
[7] Mingyan Li et al "Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks" IEEE Transactions on Mobile Computing August 2010.
[8] "The feasibility of Launching and Detecting Jamming Attacks in Wireless Networks" MobiHoc'05, May 25–27, 2005, UrbanaChampaign, Illinois,