ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY ON SECURITY OF WIRELESS SENSOR NETWORKS

Pratima Pandhare
M.Tech student, Dept. of ISE BMS College of Engineering
Bengaluru-India

ABSTRACT

The severe constraints and demanding deployment environments of wireless sensor networks make security for these systems more challenging than for conventional networks. However, several properties of sensor networks may help to solve the challenge of building secure networks. The unique aspects of sensor networks may allow the defences not available in conventional networks. In this paper, the security related issues and challenges in wireless sensor networks have been investigated. The security threats are identified and some of the proposed security mechanisms for wireless sensor networks have been reviewed.

Keywords: Wireless Sensor Networks (WSNs),Security, Threats,Attacks.

INTRODUCTION

Wireless Sensor Networks [WSNs] belong to the class of Ad-hoc networks, consisting of thousands of small devices each with sensing, processing, and communication capabilities to monitor the real world environment. Such sensors are usually low cost devices that perform a specific type of sensing task. Sensors use radio interface to communicate with one another to form a network. WSNs have many important and necessary applications. These applications are divided into many classes like Environmental Military applications, data collection, Security monitoring, sensor node tracking, health application, home application, and hybrid networks. These applications often include monitoring of sensitive information. Security is therefore important in WSNs. However, WSNs suffer from many constraints. These constraints make security in WSNs a challenge. Since these networks are usually deployed in remote places and left as it is; they should be provided with security mechanisms to defend against attacks.

CONSTRAINTS

Sensor nodes in the WSNs are inherently resource constrained. Due to these constraints, it is difficult to employ the conventional security mechanisms in WSNs. Some of the major constraints of a WSN are listed below [7, 8, and 10].

A. Energy constraints

Energy is the biggest constraint for WSNs. In general, energy consumption in sensor nodes can be categorized in three parts [1, 2, 8] (i) energy for the sensor transducer, (ii) energy for communication among sensor nodes, and (iii) energy for microprocessor computation.

B. Memory limitations

A sensor is a tiny device with only a small amount of memory and storage. Memory in a sensor node includes flash memory and RAM. There is usually not enough space to run complicated algorithms after loading the OS and application code [1, 2, 11].

C. Unreliable communication

This is a major threat to sensor security. Normally the packet-based routing of sensor networks is based on connectionless protocols and thus way too unreliable. In certain situation even if the channel is reliable, the communication may not be so. This is due to the broadcast nature of wireless communication, as the packets may collide in transit and may need retransmission [2].

D. Higher latency in communication

In WSN, multi-hop routing, traffic in the network and processing in the intermediate nodes may lead to higher delay in packet transmission. It causes difficulty to achieve synchronisation [2].

E. Unattended operation of networks

As the sensors nodes are placed in remote environment and left unattended. The chances that a sensor faces an attack in such an environment is very high. Management of a WSN from a remote place makes it virtually impossible to detect physical tampering. This makes security in WSNs particularly a difficult task [2, 11].

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

SECURITY REQUIREMENTS IN WSN

Security services in WSNs are required to protect the information and resources from attacks and physical tampering. The security requirements in WSNs include [1, 2, 4, 5 and 10]

A. **Availability:** Sensor nodes may face scarcity of battery power due to excess computation or processing or communication and become unavailable. It may happen that an attacker may overload sensor nodes to make them unavailable.

B. **Authorization:** Authorization ensures that only valid or authorized sensors can be involved in providing information to network.

C. **Privacy:** Privacy prevents attackers from obtaining information that may include any kind of private content.

E. **Confidentiality*:*** Confidentiality ensures that a given message should not make sense to anyone other than the valid recipients. Data confidentiality in networking is most important task in network security.

F. **Integrity:** Integrity facility makes sure that the data is not modified during its transmission.

G. Nonrepudiation: Nonrepudiation indicates that a node cannot deny sending a message that was previously sent by it.

H. **Self-Organization:** As WSN are a kind of adhoc network ,sensor nodes should have the capability of self healing and self organising.

I. **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 of sensors.

J. **Secure Localization:** In WSN each sensor node is required to locate itself in the network accurately and automatically to identify the location of the fault.

K. **Flexibility:** Sensor networks will be used in dynamic battlefield scenarios where environmental conditions, threat, and mission may change rapidly. Changing mission goals may require sensors to be removed from or added to an established sensor node. The sensor network should provide such flexibilty.

SECURITY THREATS AND ATTACKS

A. Security threats

A threat is an event that adversely impact a system through a security breach [6, 7, and 8]. There can be many potential threats to WSNs, for example, power exhaustion, physical tampering, and extinction immediately upon deployment due to the hostile environment. The threats in wireless sensor network can be classified into the following categories:

External versus internal attacks: The external (outsider) attacks are from nodes which do not belong to a WSN. An external attacker has no access to most cryptographic materials in sensor network. The internal (insider) attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways [7, 10, 11].

*Passive versus active attacks***:** Passive attacks are in the nature of eavesdropping on, or monitoring of packets exchanged within a WSN [7]. The active attack is related to doing some changes in the data stream or the creation of a false stream in a WSN.

Mote-class versus laptop-class attacks: In mote-class attacks, an adversary attacks a WSN by using a few nodes with similar capabilities as that of network nodes. In laptop-class attacks, an adversary can use more powerful devices such as laptops [6], etc. and can do much more harm to a network. These types of attackers can jam the radio link in its immediate vicinity.

B. Attacks

Wireless networks are more vulnerable to security attacks than wired networks, due to the broadcast nature of such networks. These attacks are normally due to one or more vulnerabilities at the various layers in the network. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Attacks on the computer system or network can be broadly classified [7, 9] as interruption, interception, modification and fabrication. *Interruption* is an attack on the availability of the network for example physical capturing of the nodes, message corruption, insertion of malicious code etc. *Interception* is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it. Modification is an attack on integrity. *Modification* means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted. *Fabrication* is an attack on authentication. In fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed.

Some of the critical attacks are categorized as follows:

1. **Denial of Service (DoS):** It is produced by the unintentional failure of nodes or malicious action. This attack is a pervasive threat to most networks [6, 7, 10]. Sensor networks being very resource-constraint, they are very vulnerable

to DoS attacks. 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.

2. **Sybil attack***:* It is defined as a malicious device illegitimately taking on multiple identities [10, 11]. In Sybil attack, an adversary can appear to be in multiple places at the same time. In other words, a single node presents multiple identities to other nodes in the sensor network either by fabricating or stealing the identities of legitimate nodes.

3. **Sinkhole (Black hole***):* In sinkhole attacks, a malicious node acts as a black hole to attract all the traffic in the sensor network through a compromised node creating a metaphorical sinkhole with the adversary at the centre [10]. A compromised node is placed at the centre, which looks attractive to surrounding nodes and lures nearly all the traffic destined for a base station from the sensor nodes. Thus, creating a metaphorical sinkhole with the adversary at the centre, from where it can attract the most traffic, possibly closer to the base station so that the malicious node could be perceived as a base station.

4. **Hello flood:** Hello flood attack uses HELLO packets as a weapon to convince its presence to the other sensor nodes sensors in WSN. In this type of attack an attacker with a high radio transmission range (termed as a laptop-class attacker) and high processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN [6,10,11]. The sensors are thus persuaded that the adversary is their neighbour. This assumption would be false. As a consequence, while sending the information to the base station, the victim nodes try to send its data through the attacker as they would have assumed that it is their neighbour and are ultimately spoofed by the attacker.

5. **Wormhole:** Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location [10,11]. In the wormhole attack, an adversary (malicious nodes) eavesdrop the packet and can tunnel messages received in one part of the network over a low latency link and retransmit them in a different part. This generates a false scenario that the original sender is in the neighbourhood of the remote location. The tunnelling procedure forms wormholes in a sensor network. The tunnelling or retransmitting of bits could be done selectively

RELATED WORK AND SOLUTION

In view of resource limitation on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors, it becomes very challenging task to apply security schemes in wireless sensor networks. Researchers have been trying to resolve security issues [9, 11]. Most of the existing security mechanisms require intensive computation and memory. Many security mechanisms require repeated transmission/communication between the sensor nodes which are further drawn in their resources. In this section, we review some of the popular security solutions and combat some of the threats to the sensor networks.

A. Spins

Security protocols for sensor networks [Spins] was proposed in which security building blocks are optimized for resource constrained environments and wireless communication [12, 13]. These protocols are categorised as follows (a) sensor network encryption protocol (SNEP) and b) µTESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness. µTESLA provides authenticated broadcast for severely resource-constrained environment. SNEP uses encryption to achieve confidentiality and message authentication code (MAC) to achieve two-party authentication and data integrity. SNEP provides number of advantages such as low communication overhead, semantic security which prevents eavesdroppers from inferring the message content from the encrypted message, data authentication, replay protection, and message freshness. In a broadcast medium such as sensor network, asymmetric digital signatures are impractical for the authentication, as they require long signatures with high communication overhead. µTesla protocols provide efficient authenticated broadcast and achieves asymmetric cryptography by delaying the disclosure of the symmetric keys. µTesla constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains. µTESLA solves the following inadequacies of TESLA in sensor networks:

- TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. µTESLA uses only symmetric mechanisms.
- Disclosing a key in each packet requires too much energy for sending and receiving. µTESLA discloses the key once per epoch.

  It is expensive to store a one-way key chain in a sensor node. µTESLA restricts the number of authenticated senders

B. *TinySec*

It is link layer security architecture for wireless network and it provides similar services as of SNEP, including

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

authentication, message integrity, confidentiality and replay protection [13]. It is a lightweight, generic security package that can be integrated into sensor network applications. A major difference between TinySec and SNEP is that there are no counters used in TinySec TinySec supports two different security options: authenticated encryption and authentication only. For authenticated encryption, TinySec uses cipher block chaining (CBC) mode and encrypts the data payload and authenticates the packet with a MAC. The MAC is computed over the encrypted data and the packet header. In authentication only mode TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted.

C. Leap

Localized encryption and authentication protocol (LEAP). This protocol is a key management protocol for sensor networks [10, 12, 13]. It is designed to support in-network processing and secure communications in sensor networks. LEAP provides the basic security services such as confidentiality and authentication.

Design of the LEAP protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements. LEAP has the following properties:

- LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighbouring nodes, and a group key that is shared by all the nodes in the network. The protocol used for establishing and updating these keys is communication and energy efficient, and minimizes the involvement of the base station.
- LEAP includes an efficient protocol for inter-node local broadcast authentication based on the use of one-way key chains.
- Key sharing approach of LEAP supports source authentication without precluding in-network processing and passive participation. It restricts the security impact of a node and compromise to the immediate network neighbourhood of the compromised node.

Table I. Represents security solutions for WSN attacks

SECURITY SCHEMES	ATTACKS DETERRED	NETWORK ARCHITECTURE	MAJOR FEATURES
JAM	DoS Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region
Wormhole based	DoS Attack (Jamming)	Hybrid	Use wormholes to avoid jamming
Radio Resource Testing. Random Key Pre-distribution	Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key predistribution, Registration procedure, detecting Sybil entity
Bidirectional Verification, Multi-path, multibase station routing	Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multibase station routing
Tiny Sec	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Focus on providing message authenticity, integrity and confidentiality.

CONCLUSION

Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted a lot of attention in the recent years. The salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads. In this paper, we have introduced some security issues, threats, and attacks in WSNs and some of the solutions. Network

security for WSNs is still a very fruitful research direction to be further explored.

REFERENCES

[1] Yong Wang, Garhan Attebury, and Byrav Ramamurthy "A survey of security issues in wireless sensor networks" 2nd quarter 2006, volume 8, NO. 2 IEEE communication surveys
[2] Jaydip Sen "A survey on wireless sensor networks security International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, August 2009
[3] Yan-Xiao Li, Lian-Qin and Qian-Liang ,"Research On Wireless Sensor Network Security" 2010 International Conference Computational Intelligence and Security
[4] Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI, "Wireless Sensor Networchallenges" IEEE 2012
[5] Abhishek Jain, Kamal Kant and M. R. Tripathy ,"Security Solutions for Wireless Sensor Networks" 2012 Second International Conference on Advanced Computing & Communication Technologies
[6] Md. Abdul Hamid1, Md. Mamun-Or-Rashid2 and Choong Seon Hong3"Defense against Lap-top Class Attacker in Wireless Sensor Network" ICACT2006
[7] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou" Sensor Network Security: A Survey", SECOND QUARTER 2009, VOL. 11, NO. 2 IEEE communication surveys
[8] Adnan Ashraf, Abdul Rauf and B.S.Chowdhry" A Model for Classifying Threats and Framework Association in Wireless Sensor Networks" IEEE 2009
[9] Xiuzhen Chen, Shenghong Li_, Jin Ma and Jianhua Li" ***Quantitative*** Threat Assessment of Denial of Service Attacks on Service Availability"IEEE 2011
[10] Gurudatt Kulkarni, Rupali Shelk, Kiran Gaikwad**"** WIRELESS SENSOR NETWORK SECURITY THREATS" 2nd quarter 2008, volume 12, NO. 2 IEEE communication surveys
[11] Pooja , Manisha, Dr. Yudhvir Singh**"** Security Issues and Sybil Attack in Wireless Sensor Networks"International journal of P2P Trends and Technology-Volume3Issue 1-2013
[12] Rakesh Sharma, Dr. V. A. Athavle, Pinki Sharma"International Journal of Advanced Research in Computer Science and Software Engineering"Volume 3, Issue 5, May 2013
[13] Adrian Perrig, Robert Szewczyk , J.D.Tygar " SPINS: Security Protocols for Sensor Networks" In [ACM Journal of] Wireless Networks, 8:5, September 2002, pp. 521-534