Journal of Theoretical and Applied Information Technology
15th April 2012. Vol. 38 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REVIEW ON SECURITY PROTOCOLS IN WIRELESS SENSOR NETWORKS

P.S RAMESH[1], F. EMILY MANOZ PRIYA[2], B.SANTHI[3]

[1] Sr.Asstt Prof.Dept of Information Technology, SASTRA University, Thanjavur, India
[2] P.G Student, Dept of Computer Science and Engineering, SASTRA University, Thanjavur, India
[3] Prof. Dept of Information and Communication Technology, SASTRA University, Thanjavur, India.

E-mail: ramesh@cse.sastra.edu[1], sweetemblika@gmail.com[2], shanthi@cse.sastra.edu[3]

Abstract

Security in Wireless Sensor Network plays an important role in the node communication. The significant growth is existed for developing the wireless sensor network applications. The key features of Wireless sensor networks are low power, low-memory, low-energy and having bulky scaled nodes. Due to this various facts the existing security algorithms are not appropriate for current applications. This causes the research to propose the novel security mechanisms which contains minimum resource consumption and maximum security. Many papers have been developed in this field. This paper is to isolate the security issues in layer level, key management and routing framework.

Keywords- *Wireless Sensor Network, Security, Routing, Key Management*

1. INTRODUCTION

In wireless sensor network the sensor nodes are densely deployed to sense and collect data. Wireless sensor network has severe resource constraints which does not enclose predefined infra structure. Self-organizing and Self-configuring are the special features of this network. This increases the wide range of applications especially in the fields of environment and military. Several authors are analyzing the security challenges for Wireless sensor network. In [1], Wireless sensor network physical attacks are discussed. Designing a secure wireless sensor network is expecting several security properties. Wireless sensor network [9] is vulnerable to various attacks. Attackers may physically capture the nodes and then they try to attack the entire sensor network. Adversaries may concern nodes and abandon the data or modify the data to mislead the decision.

2. SECURITY PROTOCOLS

Wireless network are more vulnerable to security attacks than wired network. The sensor nodes are low power devices with limited computational and communication resources. The network is more exposed to attacks because they are deployed in untrusted location area. Asymmetric digital signatures for authentication are impractical because it requires high communication strategy with high power. Deployment of security mechanisms creates additional overhead like having consumed energy, increases latency. Due to this the lifetime of the network is directly decreases.

2.1 Security

The security in wireless sensor network is essential and their main objective is to maintain the data freshness, self organization, time synchronization, protected localization, cost efficiency, self healing . Challenges in Security for wireless sensors are to retain the security against standard resources, untrusted communication and unattended operation [2] [6]. The constraints for node in sensor network are to have high energy, storage, memory and processing speed. The wireless networks are unreal, having collision and latency and lack of physical infrastructure and remotely managed. The common attacks like interruption, interception, modification, fabrication are frequently occurs in the networks. Security threats in sensor network are most importantly focused on [9] authentication, availability and certifications. In this, they perform the attacks like modification, forgery, deletion and replay attack.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The security mechanism is splitted into two levels. They are High and Low levels. In the high level security mechanisms, they have the fields like secured data aggregation, secured ID, secured group, Secured Base Communication (SBC) and Mass Communication (MC).
In low level security mechanisms, they contains fields like key establishment, secured authentication, privacy, robust to communication, Denial of service (DoS), secured routing and resistance to node capture.

2.2 Existing Security Protocols

In the real time environment, there are a number of security protocols existed. The important protocols are described here.

SNEP (Secure Network Encryption Protocol)

SNEP provides a number of distinctive advantages which thwart the hackers from hacking the messages from the users. This protocol [4] [7] are having the following properties: Semantic security, data authentication, replay protection, week freshness, low communication overhead.

µTESLA (Micro version of Timed, Efficient, Streaming, Loss-Tolerant, Authentication protocol)

µTESLA is a security protocol provides authenticated broadcast for several resources within the constrained environment [7]. It uses only symmetric mechanisms. They restrict the number of authenticated senders and they disclose the key ones per epoch. They are having the following phases:

- Sender set up
- Sending authenticated plots
- Bootstrapping new techniques
- Authenticating plots

SPINS (Security Protocol for Sensor Network)

It contains secured building blocks [7] by two primitives which are SNEP and **µ**TESLA .They have shared secret key between each node and base station. In this type of protocol trust between the node to node interactions are extended from node to base station. SPINS provides data reliability through authentication.

3. SECURITY REQUIREMENTS

The basic requirements for security issues [3], [6],[9] are Authentication, Data integrity, Confidentiality, Data security. Authentication is the process of scrutiny the trusted feature of a data. Authentication can be in the form of both at the user level and data level. Data integrity provides the guarantees for the quality of data. Confidentiality refers to limiting information access and disclosure to authorized users
and preventing access by or disclosure to unauthorized ones. It is related to the broader concept of data privacy. It is divided into two phases: strong and weak [2]. Strong confidentiality provides the partial order of the information or messages. Weak confidentiality provides the entire order of information or message.
Data security is to protect the data from adversaries. The security levels are as shown in the figure 1.

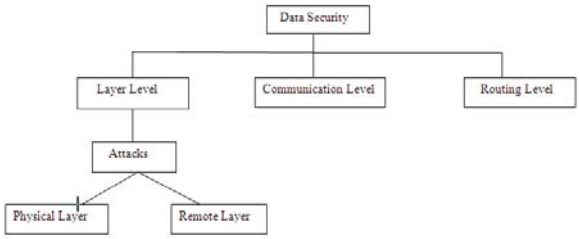

Figure 1: Levels of Data security

To ensure the success of any system with wireless sensor network, security mechanisms are prime factor. In general, all the common security attacks are defined by [5]. This paper lists the types of attacks along with its counter measures. Analysis of security requirements lead to avoid security violations. Most of the applications deployed in wireless sensor network is unattended. Probability of risk is more than the protected area network.

3.1 Layer Level

Layer level attacks are more common attacks in the field of sensor security [4]. The following attacks are generally achieved by the adversaries

- Physical attacks
- Remote attacks

3.1.1 Physical Attacks

Physical attacks are incarcerating the nodes in wireless sensor network. They intend to include the malicious node as intermediate node into the routing information [1]. They may also modify or misguide the traffic through the routing information and change the MAC protocol to launch the Denial of service (DoS) attacks. They

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

exhaust the sensor nodes by using their resources and make them unavailable when it is required.
The Hash-Chain protocol [8] is used to resist the physical attacks but they have some problem in scalability.
Secure Identity Reporting Protocol [9] is the protocol that can refuse physical attacks. This can also defuse other attacks and suitable for large RFID systems. Even though they refuse the physical attacks they still have a drawback in robustness. Hence this study focuses on need for an efficient protocol which overcomes the above drawbacks.

3.1.2 Remote Attacks

Any malicious attacks that object any system other than the system the attacker is currently logged on to. Remote attacks via networks are not dissuaded by introduction of safeguards that progress the risk that an attacker will be detected. The below table shows the layers with their appropriate protocols and attacks.

OSI Layers	Protocols	Attacks
Physical Layer	Frequency Hopping	Tampering, Jamming
Data Link Layer	TinySec, LMAC	Collision, Exhaustion, unfairness
Network Layer	LEACH, Location-Based key management and authenticatio n schemes	Selective Forwarding, Sinkhole and Wormhole attacks, Hello flood, Sybil attacks
Transport Layer	DSR Protocols	Flooding, Desynchronizatio n attacks.
Applicatio n Layer	LEAP	Compromising the whole sensor network.

Table 1: OSI layers with their attacks and protocols

3.2 Communication Level

Most of the wireless sensor network cryptographic protocols are based on symmetric key concept. Public key cryptography is expensive in terms of computation. These algorithms are not suitable for wireless sensor network, because of its limited memory power and resources.

The security requirements are combined with two issues.

- Key distribution
- Key management

3.2.1 Key distribution

Key distribution contains key maintenance and shared key pools. They have the issues like key pre-distribution, shared key discovery, path-key establishment and etc.
Generally, the key distribution protocols are not adopted properly in the wireless sensor network because of the restricted resources and small tamper resistance. Basically these types of protocols require large number of nodes and efficient resources.

3.2.2 Key management

Key management plays a vital role in wireless networks. So far, number of protocol is existed. One such protocol, LEAP protocol uses four keys: individual key, pair wise shared key, group key and cluster key.
Communication patterns are as follows:

- Node to base station communication
- Base station to node communication
- Base station to all nodes
- Node to node communication

Hence Base station is the major part and it should be trusted enough to process the communication in overall network. Each node shares the master key with base station and remaining keys are derived from this master key. In network communication security is compromised due to the following issues:

- Insertion of malicious code
- Interception of message to know the location
- Observe the application specific content
- They may inject false message along with original message
- Offer sleep deprivation torture

Key Infrastructure

The main intend of the key infrastructure is to defend the network against outside attackers. A public key infrastructure is a type of key management system that utilize the hierarchical certificates for providing authentication and public keys for encryption.

3.3 Routing Level

Many authors have been proposed routing protocols for wireless sensor network but they are limited with security objectives. Those

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

existing protocols are energy efficient but they are lack in security concern.

This section describes the routing security in wireless sensor network. In [5] security properties for sensor networks are analyzed. Routing protocols are related with network layer. Hence the network layer attacks are listed with its counter measures. Attacks are generally classified into active, passive, inside, outside, mode-class, laptop-class, and secrecy. Attackers are commonly divided as

- Mote-Class attackers
- Laptop-Class attackers

Attacks are splitted into outside and inside attacks. Adversaries may perform the process like attract or repel traffic flows. They may increase the latency and disable the entire network.

Protocol	Attacks	Measures
Tinyos	Spoofing, Wormhole	Authenticated routing updates
Directed diffusion	Flooding	Authenticate the exchanged packets
GEAR/GPSR	Sybil	Creating routing logs

Table 2: Protocol with its attacks and measures

4. LIMITATIONS IN EXISTING SECURITY PROTOCOLS

The existing security protocols having the following limitations in the security aspects

1. Overload in communication
2. Low computational power
3. High Resource consumption
4. Lack of integrity
5. Lack of confidentiality

5. CONCLUSION

This paper deals the general overview about wireless sensor network protocols. They give general security requirements and the security on wireless sensor network which is based on resource restricted design and deployment characteristics.

This work briefly described the existing security protocols. In turn it gives detail about different types of attacks and adversaries along with the counter measures. Security levels are ably described with appropriate tabulation.

REFERENCES

[1] Alexander Becher, Zinaida Benenson and Maximillian Domseif,"Tampering with modes: Real-World Physical Attacks on Wireless sensor networks", RWTH Aachen, Dept of computer science, 52056 Aachen, Germany,

[2] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, "SPINS: Security Protocols for sensor networks", Dept of Electrical Engineering and computer science, University of California, Berkeley.March 01.

[3] Akyildiz.I.F, W. Su, Y. Sankarasubramanian, E.Cayirci,"Wireless sensor networks: a survey" Georgia Institute of Technology, Atlanta, USA, Dec 01.

[4] Chris Karl of, Naveen Sastry, David Wagner, "A Link Layer Security Architecture for WSN",Feb 04.

[5] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: attacks and counter measures", University of California Berkeley, CA94720, USA, Ad Hoc networks 1(2003)293-31,Oct 01.

[6] JinatRehana," Security of wireless sensor networks",Helsinki University of technology,April 09.

[7] Lianos Tobarra, Diego Cazorla and Fernando Cuartero, "Formal analysis of sensor network encryption protocol", University of Castilla-La Mancha Escuela Polit'encica superior de Albacete. Spain-0271,Jan 08.

[8] Zhaoyu Liu and Dichao Peng, "A secure RFID identity protocol for physical attack resistance", Dept of software and information systems, University of north Carolina at charlotte,charlotte,USA,July 06.

[9] Emily Manoz Priya, Ramesh,Santhi," Secured transfer of messages against malicious attacks using efficient algorithm" IJCES, Volume1 Issue2, November 2011.