International Journal of Scientific & Engineering Research Volume 9, Issue 4, April-2018
ISSN 2229-5518

Security in Wireless Sensor Network For Attacks and Goals

[1]E.Asha, [2]N.Savitha

Abstract— Wireless sensor networks consist of many inexpensive wireless nodes, each having sensing capability with some computational and communication power. The development of large scale wireless sensor networks are consist of much low power, low cost and small size sensor nodes. Security is critical for many sensor network applications, such as military target tracking and security monitoring. Wireless sensor networks are result of developments in micro electro mechanical system and wireless networks. That traditional security measures are not enough to overcome these weakness. These small sensor nodes are susceptible to many kinds of attacks. Attacks can also be classified into outside and inside attacks. Wireless sensor networks are one of the most exciting and challenging research domains of our time. The energy efficient security protocol proposed in symmetric cryptography. It is extremely important to build a secure channel in a WSN.

Keywords— wireless sensor network, inexpensive wireless nodes, low power and small size sensor node, communication power, military target tracking, security monitoring.

1 Introduction

In the near future, the wireless sensor networks are expected to consist of thousands of inexpensive wireless nodes, each having sensing capability with some computational and communication power. Providing security in sensor networks is not an easy task. Since sensor nodes are severely energy constrained and it is infeasible to replace the batteries of thousands of sensor nodes, the key challenge in sensor networks is to maximize the lifetime of sensor nodes. Another key issue in wireless sensor networks is to have secure communication between sensor nodes and base station. Advancements in micro electro mechanical system and wireless network have made possible the advent of tiny sensor nodes called smart dust.

2 Literature Review

Researchers have addressed many areas in sensor network security. SPINS leaves some questions like security of compromised nodes, DOS issues, network traffic analysis issues. Furthermore, this protocol assumes the static network topology ignoring the ad hoc and mobile nature of sensor nodes. This protocol does not specify any security measures in case of any passive attacks on node where an adversary is intercepting the communication. Sensor nodes are assumed to be immobile and also they do not have a specific architecture when deployed over a specific geographic area. However, these nodes organize themselves into clusters, based on self- organizing clustering technique. Sensor nodes are battery powered and their lifetime is limited. Therefore, cluster heads are dynamically chosen initially. To agree on a key for communication, two nodes find one common key within their subsets and use that key as their shared key. These base station of sensor communication, where it can detect and remove an aberrant node if it is compromised. This idea later converges to pseudo random generation of keys which is energy efficient as compare to previous key management schemes.

3 Security Attacks On Wireless Sensor Networks

A large-scale sensor network consists of thousands of sensor nodes and may be dispersed over a wide area. Typical sensor nodes are small with limited communication and computing capabilities, and are powered by batteries. These small sensor nodes are susceptible to many kinds of attacks. Attacks can also be classified into outside and inside attacks. It is impractical to monitor and protect each individual sensor from physical or logical attack.

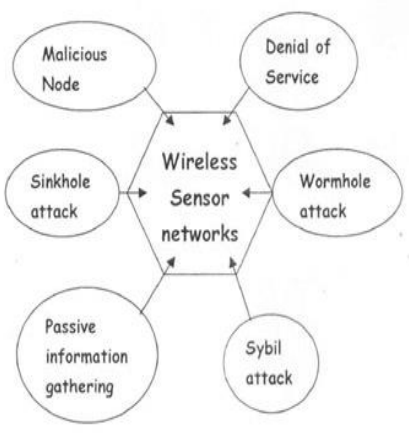

Fig.1 security attacks on wireless sensor networks

- [1]E.Asha, Second year MCA, Er.Perumal Manimekalai College of Engineering, Hosur. PH-8904426923. E-mail: ashaellappan1997@gmail.com
- [2]N.Savitha, Second year MCA, Er.Perumal Manimekalai College of Engineering, Hosur. PH-8111046424. E-mail: savithanarayanan02@gmail.com

4 Techniques For Typical Attacks

4.1 Jamming

Spread-spectrum, lower duty cycle.

4.2 Tampering

Tamper-proofing, effective key management schemes.

4.3 Collusion

Error correcting code.

4.4 Exhaustion

Rate limitation.

4.5 Manipulating Routing information

Authentication, encryption.

4.6 Sybil attack

Authentication.

4.7 Flooding

Limiting connection numbers, client puzzles.

4.8 Clone attack

Unique pair wise keys.

5 WSN Security Goals

5.1 Data confidentiality

It is the ability to hide message from a passive attacker and is the most important issue in network security. Sensor nodes may communicate highly sensitive data, such as key distribution, so it is extremely important to build a secure channel in a WSN.

5.2 Data availability

Availability is a importance for maintaining an operational networks. It is ability of a node to utilize the resources and the network is available for the message to move on.

5.3 Self organization

WSN is typically an ad-hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations.

5.4 Time synchronization

time synchronization for execution. A more collaborative sensor networks may require group synchronization for tracking Many WSN applications demands and form of applications.

5.5 Secure localization

Sensors may get displaced while deploying them or after a time interval or even after sum critical displacement incident. The utility of a WSN will really on its ability to accurately and automatically locate each sensor in the network.

6 General Security Requirements In Wireless Sensor Networks

Because of the nature of wireless communications, 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 is a challenge to provide security in WSNs. The ultimate security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. To provide secure communications for the WSN, all messages have to be encrypted and authenticated. Security attacks on information flow can be widespread.

7 Security Goals

It is the ability to hide message from a passive attacker and is the most important issue in network security. Sensor nodes may communicate highly sensitive data, such as key distribution, so it is extremely important to build a secure channel in a WSN. Moreover, sensor identities and public keys should also be encrypted to some extent to protect against traffic analysis attack.

Fig.2 security goals

.

7.1 Confidentiality

Data confidentiality is preserving the information hideaway from adversaries. The great way to keep the data invisible is to encrypt data with a secret key [1],[4]. The authorized can import data.

7.2 Data integrity

The adversaries have tried to change or modify the data. Therefore, data integrity makes sure the recipient who received message has not modified by unauthorized through transmission.

7.3 Availability

Availability is of importance for maintaining an operational network. It is the ability of a node to utilize the resources and the network is availability for the message to move on.

8 Security Benchmarks For WSN

1. Encryption
2. Data partitioning
3. Secure data aggregation
4. Cryptography
5. Shared keys

8.1 Encryption

In fact, most of wireless sensor network hold in an open area or dangers location, thus it susceptible to the network attacks.

8.2 Data partitioning

The technique of partitioning is to separate the data in networks into some or several parts. In wireless sensor networks gives a solution to make sure the attacker cannot catch the information by using the data partitioning.

8.3 Secure data aggregation

Transmit data in wireless sensor network increased than before. As results, the most issue in network is data traffic. So, the cost is rising. To reduce the high cost and network traffic, wireless sensor node aggregates measurements before transferring to the base station.

8.4 cryptography

Symmetric key cryptography is a key that used in cryptography solution in wireless sensor networks. Symmetric key is suitable and rapid to implement. A cryptography method is used to prohibit some of the security attacks.

8.5 Shared key

A better deal of the concentration in wireless sensor networks is the field of key management. WSN is a single in this feature because size, mobility and power constraints. There are four types of key management, global key, pair wise key node, pair wise key group, and individual key. These keys are solution to prevent attack.

9 Conclusion

Security in wireless sensor network communication is the self organization of sensor nodes, leader election and rout selection towards base station. Security is critical for many sensor networks. The wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, s well unreliable communication and unattended operation. To provide a general overview of the major aspects of wireless sensor network security: challenges, goals, and attacks as well as some of commonly used defenses approaches.

References

[1] Tanveer Zia and Abert zomaya "A security framework for wireless sensor networks"
[2] Naser Alajmi "wireless sensor networks attacts and solutions"
[3] Hasan Cam, Suat Ozdemir, Devasenapathy Muthuavinashippan, and Prashant nair "energy efficient of security protocols for wire less sensor networks"
[4] Aditya Sharma, garima tripath, md sohail khan, kakelli anil kumar " a survey paper on security in protocols of wireless sensor networks"
[5] Dr. deeppa gupta " wireless sensor networks feature trends and latest research chellenges"
[6] Aamir sheikh and siraj pathan "research on wireless sensor networks technology"
[7] Kahina CHELLI " security issues in wireless sensor network: attacks and countermeasures"
[8] Xiaojiang du " security in wireless sensor network"