ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Survey on Wireless Sensor Network Security

S. Mohan[1], S. Grace Diana[2]. S. Ramya[3]

M.E – Digital electronics and Communication Engineering, Nehru institute of technology, Coimbatore, Tamilnadu, India[1]

M.E – Communication Systems, SNS College of technology, Tamilnadu, India[2]

M.E – Software Engineering, SNS College of technology, Tamilnadu, India[3]

ABSTRACT: The significant advances of hardware manufacturing technology have boosted the deployment of Wireless Sensor Networks (WSNs).The WSN are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. In this article we present a survey of security issues in WSNs.

I. INTRODUCTION

A wireless sensor network (WSN) is composed of large number of sensor nodes with limited power, computation, storage and communication capabilities. Wireless sensor network (WSNs) consists of hundreds or even thousands of nodes each with power unit, a sensing unit, a processing unit and communication capabilities to monitor the real-world environment. Sensors are inexpensive, low-power devices which have limited resources. They are small in size, and have wireless Communication capability within a short- range radio transceiver, a small micro-controller, and a power supply.. In recent years, major advances have been made in the development of low-power micro sensor nodes. The emergence of such sensor nodes has allowed practitioners to visualize networking a large set of nodes scattered over a wide area of interest into a wireless sensor networks (WSNs) for Large- scale event monitoring and data collection and filtering. Wireless sensor networks (WSN) are widely used in different fields. Most sensor network applications aim at monitoring or detection of phenomena likes office building environment control, wildlife habitat monitoring, and forest fire detection. WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. Energy awareness is critical, especially in situations where it is not possible to replace sensor node batteries so it is essential design issue in wireless sensor networks. Security is a well-established field for general-purpose computing where security mechanisms address computing services (e.g. authentication, intrusion detection, etc.) and Provide secure transaction. Since the battery life confines the lifetime of a sensor node, power consumption is normally set as the first priority in developing security solutions. Sensor networks are deployed in a hostile environment, security becomes extremely important as these networks are prone to different types of malicious attacks.

This chapter present a survey of the security issues in WSNs. These papers outline the constraints of WSN, security requirements in the networks and various possible attacks.

II. RELATED WORK

Though there are varieties of challenges in sensor network we have focused on different security issues. Though the security is very important issue in WSN, due to various resource limitations and the feature of the WSNs, the security design for such network is significantly challenging. However, the nodes in WSNs have severe resource constraints due to their lack of processing power, limited memory and energy. Therefore traditional security techniques with large overhead of computation and communication are infeasible in WSNs. providing security in sensor is more difficult due limitations of the sensor nodes. Security in sensor network is complicated by the constrained capabilities of sensor node hardware and

- Sensor nodes use wireless communication, which is particularly easy to eavesdrop on. Similarly, an attacker can easily inject malicious messages into the wireless network.
- The use of radio transmission, along with the constraints of small size, low cost, and limited energy, make WSNs more susceptible to denial-of-service attacks. Security also needs to scale to large-scale deployments.
- Most current standard security protocols were designed for two-party settings and do not scale to a large number of participants.

2.1 Constraints in Wireless Sensor Network

In order to optimize the security algorithm for WSNs, it is necessary to be aware about the constraints of the sensor nodes. Some of the major constraints of a WSN are listed below. *Energy constraints:* Energy is the biggest constraint for a WSN. In general, energy consumption in sensor nodes can be categorized in three parts: (i) energy for the sensor transducer, (ii) energy for communication among sensor nodes, and (iii) energy for microprocessor computation. *Memory limitations:* A sensor is a tiny device with only a small amount of memory and storage space. Memory is a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate results of computations

Unreliable communication: It is another serious threat to sensor security. Normally the packet-based routing of sensor networks is based on connectionless protocols and thus inherently unreliable. Packets may get damaged due to channel errors or may get dropped at highly congested nodes.

Higher latency in communication: In a WSN, multi-hop routing, network congestion and processing in the intermediate nodes may lead to higher latency in packet transmission. This makes synchronization very difficult to achieve.

2.2 Security Requirements

A WSN is a special type of network. It shares some commonalities with a typical computer network, but also exhibits many characteristics which are unique to it. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehaviour of nodes. The most important security requirements in WSN are listed below

Data confidentiality *:* The security mechanism prevent the overall content or a field in a message. In a WSN, the issue of confidentiality should address the following requirements (i) a sensor node should not allow its readings to be accessed by its neighbours unless they are authorized to do so, (ii) key distribution mechanism should be extremely robust, (iii) public information such as sensor identities, and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks.

Data integrity *:* The mechanism should ensure that no message can be altered by an entity as it traverses from the sender to the recipient.

Availability *:* This requirements ensures that the services of a WSN should be available always even in presence of an internal or external attacks such as a denial of service attack (DoS).

Self-organization*:* Each node in a WSN should be self- organizing and self-healing. This feature of a WSN also posses a great challenge to security. The dynamic nature of a WSN makes it sometimes impossible to deploy any pre-installed shared key mechanism among the nodes and the base station. It is desirable that the nodes in a WSN self-organize among themselves not only for multi-hop routing but also to carryout key management and developing trust relations.

Secure localization : In many situations, it becomes necessary to accurately and automatically locate each sensor node in a WSN. For example, a WSN designed to locate faults would require accurate locations of sensor nodes identifying the faults. A sensor computes its location by listening to the beacon information sent by each locator which includes the locator's location information.

Time synchronization : Most of the applications in sensor networks require time synchronization. Any security mechanism for WSN should also be time-synchronized. A collaborative WSN may require synchronization among a group of sensors.

Authentication : It ensures that the communication from one node to another node is proper, that is, a malicious node cannot mask as a trusted network.

Nonrepudiation : It denotes that a node cannot deny sending a message it has previously sent.

Data Freshness :It implies that the data is recent and ensures that no adversary can replay old messages Moreover, as new sensors are deployed and old sensors fail, we suggest that forward and backward secrecy should also be considered:

- *Forward secrecy:* a sensor should not be able to read any future messages after it leaves the network.
- *Backward secrecy:* a joining sensor should not be able to read any previously transmitted message.

2.3 Types of Attacks

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways: Denial of service attacks, Sybil attacks, Traffic analysis, Physical attacks and so on.

The Sybil Attacks : The Sybil attack is defined as a "malicious device illegitimately taking on multiple identities" . It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems . In addition to that, the Sybil attack is also effective against routing algorithms, data aggregation, voting and fair resource allocation.

Denial of Service Attacks : A Type of standard of Denial of service attacks on wireless sensor networks is jamming a node or set of nodes. The jamming of a network can come in two forms: constant jamming, and intermittent jamming.. Denial of service Attacks can also be made on the link layer itself. One possibility is that an attacker may simply intentionally violate the communication protocol and continually transmit messages in an attempt to generate collisions. Such collisions would require the retransmission of any packet affected by the collision. Using this technique it would be possible for an attacker to simply deplete a sensor node's power supply by forcing too many retransmissions.

Physical Attacks :It destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker .

Traffic Analysis Attacks : Wireless sensor networks are typically composed of many low-power sensors communicating with a few relatively robust and powerful base stations. It is not unusual, therefore, for data to be gathered by the individual nodes where it is ultimately routed to the base station. Often, for an opponent to effectively render the network useless, the attacker can simply disable the base station.

2.4 Security Issues

Intrusion Detection : The problem of intrusion detection is very important in the case of WSNs. Traditional approaches which do an anomaly analysis of the network at a few concentration points, are expensive in terms of network's memory and energy consumption. So there is a need for decentralized intrusion detection. Intrusion detection in WSNs is still largely open to research. Key research issues are 1. Due to the constraints in WSNs, intrusion detection has many aspects that are not of concern in other network types. 2. The problem of intrusion detection needs to be well defined in WSNs. 3. It is very difficult to integrate intrusion detection techniques into a uniform hardware platform due to cost and implementation constraints.

Secure Location Discovery : As mentioned earlier, sensor locations play a critical role in many sensor network applications, such as environment monitoring and target tracking. Without protection, an attacker may easily mislead the location estimation at sensor nodes and interrupt the normal operation of sensor networks. Moreover, an attacker may compromise a beacon node and distribute malicious location references by lying about the location or manipulating the beacon signals. In either case, non-beacon nodes will determine their locations incorrectly.

Secure Localization : In a WSN, sensors can be randomly distributed in order to collect data from a site. Knowledge of the position of the sensing nodes in a WSN is an essential part of many sensor network operations and applications. Sensors reporting monitored data need to also report the location where the information is sensed, and hence, sensors need to be aware of their position. In addition, many network protocols such as routing require location information in order to provide the specific protocol service. Localization systems can be divided into three distinct components as Distance/angle estimation, Position computation and Localization algorithm.

Secure Routing :Secure routing is vital to the acceptance and use of sensor networks for many applications, but many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. WSNs use multi-hop routing and wireless communication to transfer data, thus incur more routing attacks. Security attributes are the mechanisms that allow the routing protocols to defend against the possible threats in the whole network. These attributes consist of identity verification, topology structure restriction, base station decentralization and multi-path transmission. There are a lot of approaches to ease routing security 1.Most current proposals are suitable for static WSNs. Designing secure routing algorithms for mobile WSNs is complex and current secure routing algorithms will meet issues when they are applied in mobile environments. 2. Undetected node compromise issues, the current cryptography mechanisms, such as authentication, identification, etc. may detect and defend against node compromise in some extent. However, most compromise activities cannot be detected immediately 3. Currently most proposals only consider security metrics and only a few of them evaluate other metrics. More metrics, such as QoS (quality of service) need to be considered in addition of security. 4. Though some secure routing algorithms are proposed based on hierarchical sensor networks, most of these studies did not show the different effects such as energy consummations, security, etc. due to different cluster size. Though these algorithms may ease secure routing issues, they bring complex cluster management issues and costs. 5. Routing maintenance: During the lifetime of a sensor network, the network topology changes frequently, and routing error messages are normally produced.

III. CONCLUSION

Security concerns a potential block in deployment of sensor networks. WSNs are still under development, and many protocols designed so far for WSNs have not taken security into consideration. On the other hand, the salient features of WSNs make it very challenging to design strong security protocols. In this article, we summarize typical attacks on sensor networks and surveyed the literatures on several important security issues relevant to the sensor networks, including key management, secure routing, and secure location discovery and intrusion detection.

REFERENCES

[1] Hiren Kumar Deva Sarma, Avijit Kar, "Security Threats in Wireless Sensor Networks", IEEE 2006.

[2] E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 6, Dec. 2004 pp. 38–43.

[3] Raymond D.R. Midkiff.S.F, "Denial of Service in Wireless Sensor Network: Attacks and Defenses", IEEE Pervasive Computing, Vol:7, Issue 1, PP: 74 – 81, March 2008.

[4] I. F. Akyildiz W. Su, Y. Sankarasubramaniam, "A Survey on Sensor Networks," IEEE Commun.Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[5] E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 6, pp. 38–43, Dec. 2004.

[6] Xiaojiang Du; Hsiano-Hwa Chen; " Security in wireless sensor networks", Wireless Communications, IEEE, Vol: 15, Issue 4, pp: 60 –66, Aug 2008.

[7] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks" , IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006

[8] M. Kim, E. Jeong, Y. C. Bang, S. Hwang, and B. Kim, "Multipath energy- aware routing protocol in wireless sensor networks," in Proc. IEEE INSS, Kanazawa, Japan, 2008, pp. 127–130.

[9] Y. Challal, A. Ouadjaout, N. Lasla, M. Bagaa, and A. Hadjidj, "Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1380– 1397, Jul. 2011.

[10] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Netw., vol. 1, no. 2, pp. 293–315, sep 2000.