International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 10
ISSN: 2454-4248
24 – 26

Security Threats and Challenges for Wireless Sensor Network

K. Vimala
HOD
Department of Computer Science,
Pavai Arts and Science College for women,
Rasipuram, Namakkal

M. Jothimani
M.Phil., Scholar,
Department of Computer Science,
Pavai Arts and Science College for women,
Rasipuram, Namakkal

V. T. Kiruthika
Assistant Professor
Department of Computer Science,
Pavai Arts and Science College for women,
Rasipuram, Namakkal

ABSTRACT: A wireless sensor network is a network of a large number of independently working small sensing units which can communicate wirelessly. The basic plan of a Wireless sensor network (WSN) is to structural distribute self-determining devices using sensors to monitor physical or environmental conditions. Wireless communication technology performance different forms of security threats. WSN need effective security mechanisms because of these networks deployed in untended environments. Due to fixed limitations in wireless sensor networks, security is a crucial issue. The intent of this paper is to investigate the security-related threats and challenges in wireless sensor networks. The threats faced by this WSN are similar but not limited to those observed in a simple network of computers or Internet.We identify thesensorsecuritythreats, review proposed security mechanisms for wireless sensor networks.

Keywords: *wireless sensor network, security threats.*

*****

I. INTRODUCTION

Wireless sensor networks (WSN) are the wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. In the recent years, an efficient design of a Wireless Sensor Network has become a leading area of research. The sensor is a device that responds and detects some type of input from both the physical or environmental conditions, such as pressure, heat, light, etc. The output of a sensor is generally an electrical signal that is transmitted to a controller for further processing. The wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and within a gateway, the data is connected to other networks like wireless Ethernet. Security is an important requirement for many WSN applications, like healthcare, structural, industrial monitoring, military, and smart homes. However, it is difficult to provide security in most of these applications due to many factors. Some of these factors are related to the constrained nature of WSNs, and others are related to environments where sensor nodes are being deployed.

FEASIBILITY OF THE BASIC SECURITY SCHEMES IN WIRELESS SENSOR NETWORKS

Security is broadly used term encompassing the characteristics of authentication, integrity, privacy, non-repudiation, and anti-playback. The more dependency on information provided by networks has been increased; more the risk of secure transmission of information over networks has increased. For secure transmission of various types of information over networks, several cryptographic, steganographic and other techniques are used which are well known. The network security fundamentals and how techniques are meant for wireless sensor networks.

Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to applied directly for wireless networks and in particular for wireless sensor networks. WSN consist of tiny sensors which really suffer from the lack of processing, memory and battery power Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for sensors' longevity. Applying security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks. Moreover some critical questions arise when applying encryption schemes to WSN like, how the keys are generated or disseminated. How the keys are managed, revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for network. As minimal or no human interaction for sensors, is a fundamental feature of wireless sensor networks, it becomes an important issue how the keys could be modified time to time for encryption. Adoption of the pre-loaded keys or embedded keys could not be an efficient solution.

 ISSN: 2454-4248
24 – 26

Steganography

While cryptography aims at hiding the content of a message, steganography aims at hiding the existence of a message. Steganography is the art of covert communication by embedding a message into multimedia data (image, sound, video, etc.).

The main objective of the steganography is to modify from the carrier in a way that is not perceptible and hence it looks just like ordinary. It hides the existence of covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to a steganography and processing multimedia data is a (like audio, video) with the inadequate resources of the sensors is difficult and an open research issue.

Physical Layer Secure Access

Physical layer secure access in the wireless sensor networks could be provided by using a frequency hopping. A dynamic combination of the parameters like hopping set (available frequencies for hopping) dwell time (time interval per hop) and hopping pattern (the sequence in which frequencies from available for hopping set is used) could be used with a little expense of memory, processing and energy resources. Important points in physical layer secure access are the efficient design so that the hopping sequence is modified in less time than is required to discover it and employing for this both the sender and receiver should maintain a synchronized clock. A scheme as a proposed in could also be utilized which introduces secure physical layer access employing singular vectors with the channel synthesized modulation.

THREAT MODEL

It is usually assumed that an attacker may know the security mechanisms that are deployed in sensor network. Attackers may be able to compromise a node or even physically capture node. Most WSN nodes are viewed as non-tamper resistant due to the high cost of deploying tamper resistant sensor nodes. The attacker is capable of the stealing key materials contained within the compromised node. Base stations are regarded as trustworthy in WSN. Most researchers focus on secure routing between sensors and between base stations. Attacks in sensor network can be classified into the following categories.

1. Outsider Vs. insider attacks

Outsider attacks are attacks from nodes which do not belong to a WSN. Insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways.

2. Passive Vs. active attacks

Passive attacks are including eavesdropping on or monitoring packets exchanged with in a WSN. Active attacks involve some modifications of data stream or creation of a false stream.

3. Mote-class Vs. Laptop-class attacks

An adversary attacks WSN by using a few nodes with similar capabilities to the network nodes in mote-class attacks. Mote class attackers can jam the radio link in its immediate vicinity. Laptop-class attack an adversary can use more powerful devices (e.g a laptop) to attack a WSN. These devices have greater transmission range, energy reserves and processing power than the network nodes. A laptop class attacker might be able to eavesdrop on an entire network.

Attacks on WSN can be classified from two different levels of views

1. Attack against security mechanisms

2. Attack against basic mechanisms (like routing mechanisms) In many applications the data obtained by the sensing nodes need to be authentic. A false or malicious node could intercept private information in the absence of proper security or could send false messages to nodes in the network.

Security Improvement Proposal for WSN Network

Due to efficient activities in particular areas where regular wireless network is not capable of handling the communication, wireless sensor network efficiently maintain the communication between different users as well as with the nearest base station. The security threatening issue is one a major drawbacks of this communication system. Malicious or bad intruders are present everywhere and they will remain for ever to gain success of their own by making this types of useful and important network defense less or imperceptible. The engineers and researchers are also working hard to keep the system trustworthy and highly secured for outsiders. Security is one of the greatest challenges in WSN. To ensure confidentiality of the data in sensor networks, various types of the security mechanisms are proposed. Drawbacks like security vulnerabilities are associated with those schemes. In this paper a survey is taken related to the security purpose. Implementation of security for wsn influence a great deal due to their size and energy limitations.To rectify these drawbacks chaotic maps and genetic operations are used. This algorithm is helps in encoding the data. Along that secure encryption transaction algorithm is implemented.

PROTOCOLS

LISP

A Lightweight security protocol for wireless sensor network aims to provide authentication without

 ISSN: 2454-4248
24 – 26

retransmission of keys and also provides scalability in computing. It uses symmetric key system approach.

Tiny Sec

Link layer security architecture for wireless sensor network is a light weight and link layer security protocol. It provides the security services as message Integrity, message authentication and access control at routing level and Reply protection in Adversary. It supports two different security options. They are Authenticated Encryption and Authentication only.

SPINS

(Sensor Protocol for Information via. Negotiation)

Security Protocol for Wireless Sensor Networks. This protocol is used to provide by security services as freshness, Authentication, Confidentiality and Integrity. The Localized Encryption and Authentication Protocol security mechanism provides confidentiality and authentication mechanisms in the sensor networks.

Some important steps should be maintained for an uncompromised security of network is as below.

- Strong cryptographic algorithms should apply for the sharing public key – private key management.
- Routing or transmission of the packets must be managed with secured and efficient routing protocols.
- Assurance of confidentiality, integrity and availability of the network, associates for legitimate stations.
- Trust establishment as well as privacy protection for the whole network.
- Future growing network must can be designed with adaptive defense mechanism to make it utmost reliable.
- Unconditional effort to the curtail percentage of denial of service attack and it mechanism.
- Highly recommendsecurity architecture designing its maintenance and the regular assessment.
- Authentication with mobility access, easy and secure localization and easy method to discovery the neighbour with appropriate security.
- Always updating the present design of an intrusion detection system.

II. CONCLUSION AND FUTURE WORK

Most of attacks against security in a wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by the compromised nodes, a means is required for detecting false reports. However developing such as a detection mechanism and making it efficient represents a great research challenge. Again ensuring the holistic security in wireless sensor network is a major research issue. Many of todayproposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer in the future though security mechanisms become well-established for each individual layeris a combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. Even if the holistic security could be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming days.

REFERENCES

[1]. M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee “Sensor Network Security: More Interesting Than You Think”, In Proc. of the 1st USENIX HotSec, 2006.

[2]. M. Anand, Z. Ives, and I. Lee. “Quantifying Eavesdropping Vulnerability in Sensor Networks”, In Proc. of the 2nd International VLDB Workshop on Data Mgnt. for Sensor Networks (DMSN), 2005

[3]. Stamatios and V. Kartalopoulos, Editors, “Differentiating Data security and Network Security”, IEEE International Conference on Communications, (2008) May 19-23, Beijing.

[4]. S. D. Kanawat and P. S. Parihar, Editors, “Attacks in Wireless Networks”, International Journal of Smart Sensors and Adhoc Networks, (2011) May 18-23.

[5]. Y. X. Lim and T. Schmoyer, Editors, “Wireless Intrusion detection and response”, IEEE Information Assurance Workshop, (2003) June 18-20, Westpoint, Newyork.

[6]. K. Bhatele, A. Sinhal and M. Pathak, Editors, “A Novel Approach to the Design of New Hybrid Security Protocol Architecture”, IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), (2012) August 23-25, Ramanathapuram. International Journal of Future Generation Communication and Networking Vol.7, No.4 (2014) Copyright ⓒ 2014 SERSC 33

[7]. A. H. Lashkari and M. M. S. Danesh, Editors, “A Survey on Wireless Security Protocols WEP, WPA and WPA2/802.11i”, IEEE International Conference on Computer Science and Information Technology, (2009) August 8-11, Beijing.

[8]. G. Selim, H. M. E. Badawy and M. A. Salam, Editors, “New Protocol design for Wireless Networks security”, IEEE International Conference on Computer Science and Information Technology (ICACT), (2006) Feb 20- 22.

[9]. H.-W. Lee, A.-S. K. Pathan and C. S. Hong, Editors, “Security in Wireless Sensor Networks: issues and challenges”, International Conference on Advanced Communication Technology (ICACT), (2006) February 20-22, Phoenix Park.