Research Paper Engineering

A Comparative Study of Security Protocols for Wsns

* Ms. Preeti Sharma ** Ms. Simple Nain

* Asst. Professor at KIIT college of Engineering, Gurgaon.

** M.Tech student, VCE, Rohtak.

ABSTRACT

Wireless sensor network is a network comprises of low cost resource constrained sensor nodes that are communicating using wireless medium. Similar to other technologies, in WSNs there are some considerable issues that should be taken into account. One of that issues is security. As the wireless sensor nodes are employed in a remote or hostile environmental area that is prone to attacks frequently, so security is an important and valuable criterion to be considered in WSNs [6]. Many Secured protocols are proposed in wireless sensor networks. This paper is presented to do a comparative study of all these protocols considering all the challenging issues and requirements of security.

Summary: This paper analyzes five popular WSN security protocols: SPINS [6,7], LEAP[8] TINYSEC [6,7], MINYSEC[4,9], and ZIGBEE[10], And SIM[11]. The paper also presents an application characteristics table which helps to select the appropriate security protocols. Rest of the paper is organized as follows. Section 2 describes the general security constraints of WSN. Section 3 defines the security challenges in WSNs. Section 4 provides the major features of selected security protocols. Section 5 analyzes and compares the selected security protocols. Finally, Section 6 concludes the paper.

Keywords: Attack, security, sensor nodes

1. Introduction

The evolution of wireless sensor networks is inspired by military applications such as surveillance in battlefield. But now a days, these networks are employed in many industrial applications such as in process monitoring, control systems, machine life monitoring etc [6]. Wireless sensor networks are constituted of large numbers of resource-constrained and wirelessly communicating computing devices. With Development in computing and communication technology, it becomes possible to integrate sensing capabilities, wireless communication interfaces, and microprocessors into tiny devices that allow integrating computational power in arbitrary environments. The applications of wireless sensor networks include surveillance and environmental monitoring to healthcare and the provisioning of context information for computing applications. Many of these applications directly influence human beings or are of high economic significance. The specific characteristics of wireless sensor networks make them prone to attacks on their communication channels and their hardware [2]. Cryptographic mechanisms can be exploited to protect against some of the possible attacks: eavesdropping on messages is countered by encryption, and the injection of messages by the attacker is restricted by authentication. Unfortunately, direct physical access to the sensor nodes provides a chance to an attacker to manipulate them randomly [1].

In particular, nodes could be compromised and then made to execute malignant code injected by the attacker. Tamper resistance mechanisms applied to the nodes' hardware, concealment, surveillance and other techniques may be used to placate such attacks. However, they cannot be completely prevented and therefore, any communication security scheme being used must be sufficiently effervescent to tolerate a certain amount of compromised nodes. Therefore an important objective is to restrict the impact of a set of compromised nodes on the legitimate operation of the network to a minimum level.

2. CONSTRAINTS IN WSN:

Resource constraints: Sensor nodes have restricted resources, including low computational capability, small memory space, low wireless communication bandwidth, and a non-rechargeable battery.

Small message size: Messages in sensor networks are usually small size as compare to the existing networks.

Addressing Schemes: As a WSN network comprises of large no nodes, it become impossible to exploit a global addressing scheme for deployment of a large number of sensor nodes as overhead of identity maintenance is high.

Sensor location and redundancy of data: Awareness of node locations in sensor network is important since data collection is normally based on location [5].

3. SECURITY CHALLENGES IN WSNs:

There are a number of general security vulnerabilities of sensor networks which can be identified, such as in the transmission of messages, on the routing layer, or concerning physical node capture. Depending on the type of attacks that are anticipated, these vulnerabilities may become security threats. The goal of security services in WSN is to protect the information and resources from attacks and threats. The security requirements in WSN include:

Message Authentication and Integrity: Messages must be protected from any alteration and the receiver of a message must confirm the sender of the message. But integrity does not necessarily imply identification of the sender of the message. A message that hops from one node to another one should not be susceptible to wrong interpretation or eavesdropping by an attacker. On the data link layer, this can be achieved by encrypting and authenticating messages in transit. The necessary keys can be agreed upon when the wireless link is established

3. OVERVIEW OF WSNs SECURITY PROTOCOLS

In WSNs, the following security protocols have been proposed:

3.1 SPIN: Ritu Sharma, Yogesh chaba, YaduvirSingh,& Sahana, A.Mishra,I.S(2010,2011) says that In SPIN (Sensor Protocols for Information via Negotiation), nodes use three types of messages ADV, REQ and DATA to communicate.ADV is used to advertise new data, REQ to request for data and DATA is the actual message itself. The protocol initiates when a SPIN node obtains new data that it is willing to share. This is carried out by broadcasting an ADV message containing meta-data [6,7]. If a neighbor shows interest in the data, it will generate an REQ message for the DATA and the DATA is sent to this neighbor node. The neighbor sensor node then repeats this process to its neighbors as a result of which the entire sensor area will get a copy. It consists of blocks SNEP (Sensor Network Encryption Protocol) and TESLA (Timed Efficient Stream Loss-tolerant Authentication).In addition to integrity, SNEP is used to provide confidentiality through encryption and authentication using a message authentication code (MAC). It helps in minimizing the overhead by adding only 8 bytes per message [1,9]. TESLA completes the authentication process for the initial packet using the digital signature.

3.2 LEAP: S. Zhu, S. Setia, & S. Jajodia (2003) focuses on the goal of LEAP (Localized Encryption and Authentication Protocol), that is to meet the security properties of authentication and confidentiality in a wireless environment where the intruder may eavesdrop, inject packets, and replay messages [8]. LEAP, viewed as a key management protocol for sensor networks, is designed to mitigate the in-network processing, while constraining the impact of a compromised node to the network. In order to support the in-network processing required for most applications of these networks along with security properties, such as security and authentication, use of pair wise symmetric keys is mandatory. LEAP specifies four types of keys: individual keys, pair wise shared keys, cluster keys and group keys.

3.3 TINY SEC: Ritu Sharma, Yogesh chaba, & Yaduvir Singh(2007) says that the commonly found traffic pattern in sensor networks is many-to-one, with many sensor nodes communicating sensor readings or network events over a multihop topology to a central base station. Thus if each node sends a packet to the base station in response; precious energy and bandwidth are wasted[7]. To eliminate these redundant messages, to reduce traffic and save energy, sensor networks exploits in-network processing that includes aggregation and duplicate elimination [6]. With authenticated encryption, TINY SEC encrypts the data payload and authenticates the packet with a MAC. TINY SEC is a research platform that is easily extensible and has been inbuilt into higher level protocols.

3.4 MINI SEC: M. Luk, G. Mezzour, A. Perrig, and V.Gligor, (2007) develop MINI SEC [5] which is a secure network layer protocol that claims to have lower energy consumption than TINY SEC while achieving a level of security which is comparable that of ZIGBEE. A major feature of MINI SEC is that it uses offset codebook (OCB) mode as its block cipher mode of operation, which provides authenticated encryption with only one pass over the message data. Normally there is need of two passes for both secrecy and authentication. Another major advantage of of employing OCB mode is that the cipher text is having the same length as the plaintext, without considering the additional fixed length tag, so in MINI SEC's case, cipher text stealing is not necessary. Another primary characteristic of MINI SEC over the other security suites mentioned here is strong replay protection without the transmission overhead of sending a large counter with each packet.

3.5 ZIGBEE: In ZIGBEE, the concept of a Trust Center is bring into existence. Generally the ZIGBEE coordinator performs this function. This trust center permits other devices to join the network and also distributes the keys. There are three roles played by ZIGBEE:

- As a trust manager, who authenticate the devices that request to join the network.
- As a network manager, perform functions of maintaining and distributing network keys, and
- As a configuration manager, provide end-to-end security between devices [10].

It works out in both Residential Mode and Commercial Mode. The Trust Center running Residential Mode finds use for low security residential applications. Commercial Mode is designed to meet demand of high-security commercial applications. In Residential Mode, the Trust Center will allow devices to join the network, but does not establish keys with the network devices [11]. It therefore cannot periodically update keys making the memory cost to be minimum, as it cannot scale with size of the network. In commercial mode, it built up and maintains keys and freshness counters with every device in the network, allowing centralized control and update of keys. This results in a memory cost that could scale with the size of the network.

3.6 A SM protocol: J. Heo, C.S. Hong (Jan,2006) develop SM (Security Manager), a new method of key agreement has been proposed in [4], in which, when a new device joins a network, the Security Manager (SM) provides static domain parameters at the base station such as the order of the curve and the elliptic curve coefficients. After calculating a public key using the base point and a private key, the

Node sends a public key to the SM. Therefore the SM would have the public key list for all the devices in the network. Authentication is achieved by using either Diffie-Hellman or Elliptic Curve Equation. Confidentiality is achieved by using message authentication protocol. This reflects that SM protocol offers more services than the other existing protocols 3.6 802.15.4

IEEE Standards Association(2003) in New York defines, The 802.15.4 standard [12] provides link layer security services, and performs in modes of operation: unsecured, Access Control List (ACL) mode and secured mode. In unsecured mode, as the name implies, services are not secured. In ACL mode the device maintains a list of devices with which it can communicate. Devices not present in list cannot communicate with the host node. Secured mode offers seven security suites and depending on which four security services access control, data encryption, is frame integrity and sequential freshness are offered [12]. Hence, 802.15.4 standard, if implemented accurately, can serve as a good base for building higher level, fully featured security suites.

4. Conclusion & Future Perspectives

Table1. Comparison of various protocols.

Protocols	Encryption	Freshness	MAC used	Key Agreement	Implicit Authentication	Authentication for user
SPIN	Yes	Yes	Yes	Symmetric Delayed	Yes	No
LEAP	Yes	No	Yes	Pre-delayed	Yes	No
TINY SEC	Yes	No	Yes	Any	Yes	Yes
MINI SEC	Yes	No	Yes	Any	Yes	Yes
ZIGBEE	Yes	Yes	Yes	Trust Centre	Yes	Yes
SM	Yes	No	Yes	-	Yes	Yes

In this paper we compared the performances of all the existing protocol with proposed protocol. SPIN was found to perform better in smaller size networks because of its efficiency and high latency properties. The use of SPIN in large scale networks could potentially exhaust system resources in a much faster pace. This is to further evaluate the effectiveness of these protocols and define their more desirable character-

istics. There is currently no one solution that can be plugged-in to an application to provide all the necessary.

The future perspectives for WSNs security protocols should include following:

1. A major challenge in protocol design in WSNs is to improve reliability of Protocols and to reduce delivery delay time and the number of packet retransmission.
2. To design and implement the protocols for rural environments as well.
3. The future goal of this research is to develop a new authentication protocol, by combining the most desirable traits of what currently exists and implementing some new ideas, which is optimal for implementation in wireless sensor network application security primitives.

REFERENCES

[1] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen & David E. Culler, “SPINS: Security Protocols for Sensor Networks,” Wireless Networks 8, 521.534, 2002_ 2002 Kluwer Academic Publishers. Manufactured in The Netherlands | [2] Dorothy E. Denning, “ An Intrusion-Detection Model.,” In IEEE Symposium on Security and Privacy. IEEE, 1986. | [3] Harold Vogt,“Protocols for Secure Communication in Wireless Sensor Networks,” (thesis) Swiss Federal Institute Of Technology, Zurich,2009. | [4] J. Heo, C.S. Hong, " Efficient and Authenticated Key Agreement Mechanism in Low-Rate WPAN Environment," Proceedings of the 1st IEEE International Symposium on Wireless Pervasive Computing, Phuket, Thailand, pp. 1-5, 16-18,January2006 | [5] M. Luk, G. Mezzour, A. Perrig, and V.Gligor, "MiniSec: A Secure Sensor Network Communication Architecture," in IEEE International Conference on Information Processing in Sensor Networks (IPSN'07), Cambridge, Massachusetts, USA, 2007. | [6] Ritu Sharma, Yogesh chaba, Yaduvir Singh, “Analysis of Security Protocols in Wireless Sensor Network”, Int. J. Advanced Networking and Applications 707 Volume: 02, Issue: 03, pp: 707-713 (2010). | [7] Sahana, A.Mishra, I.S, “Implementation of RSA security protocol for sensor network: Design and Network analysis”, IEEE Conference, Feb 28, 2011-March 3, 2011. | [8] S. Zhu, S. Setia, and S. Jajodia. “Leap: efficient security mechanisms for large-scale distributed sensor networks”, In CCS ’03: Proceedings of the 10th ACM conference on Computer and communications security, New York, USA, 2003, pp.62–72. | [9] T.C. Aseri, N. Singla, “Enhanced Security Protocol in Wireless Sensor Networks”, Int. J. of Computers, Communications & Control,.N 1841-9836, E-ISSN 1841-9.844 Vol. VI (2011), No. 2 (June), pp. 214-221 | [10] ZigBee Alliance, ZigBee Security Specification Overview, [Online] Available: http://www.zigbee.org/en/events/documents/december2005_open_house_presentations/zigbee_securiy_layer_technical_overview.pdf. | [11] ZigBee Specification v1.0: ZigBee Specification (2005), San Ramon, CA, USA: ZigBeeAlliance.http://www.zigbee.org/en/spec_download/download_request.asp | [12] 802.15.4: Wireless Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LRWPANs), 2003 New York: IEEE Standards Association. |