Int. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844
Vol. VI (2011), No. 2 (June), pp. 214-221

Enhanced Security Protocol in Wireless Sensor Networks

T.C. Aseri, N. Singla

Trilok C. Aseri, Neha Singla
PEC University of Technology
Computer Science & Engineering Department
House No. 808, PEC Campus, Sector-12, Chandigarh-160012 (India)
E-mail: a_trilok_chand@yahoo.com, nehasingla1409@gmail.com

Abstract: The need for security in communications is in fact not new. This need has existed in military communications for thousands of years. In this paper, we focus on network protocols that provide security services. Wireless sensor network is an emerging technology that shows applications both for public as well as military purposes. Monitoring is one of the main applications. A large amount of redundant data is generated by sensor nodes. This paper compares all the protocols which are designed for security of wireless sensor network on the basis of security services and propose an improved protocol that reduces communication overhead by removing data redundancy from the network. By using the message sequence number we can check whether it is old message or new message. If the message is old then no need to send that message thereby reducing overhead. It also integrates security by data freshness in the protocol.
Keywords: data freshness, protocol, security, wireless sensor network.

1 Introduction

Sensor networks are typically data driven, i.e., the whole network cooperates in communicating data from sensors (information sources) to information sinks. Low-cost, low power, multifunctional sensor nodes that are small in size and communicate untethered in short distances have been developed due to the recent advances in wireless communication. These tiny sensors have the ability of sensing, data processing, and communicating with each other. Wireless Sensor Networks (WSN) which rely on collaborative work of large number of sensors are realized. A WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm. Wireless sensor network is one of the most exciting and challenging research areas.

Nodes in sensor networks have restricted storage, computational and energy resources; these restrictions place a limit on the types of deployable routing mechanisms. Additionally, ad hoc routing protocols for conventional wireless networks support IP style addressing of sources and destinations. They also use intermediate nodes to support end-to-end communication between arbitrary nodes in the network. It is possible for any-to-any communication to be relevant in a sensor network; however this approach may be unsuitable as it could generate unwanted traffic in the network, thus, results the extra usage of already limited node resources. Many-to-one communication paradigm is widely used in regards to sensor networks since sensor nodes send

their data to a common sink node for processing. This many-to-one paradigm also results in non-uniform energy drainage in the network.

The applications for WSNs are many and varied, but typically involve some kind of monitoring, tracking, and controlling, intelligent buildings, transportation, space exploration, disaster detection. In order to operate these applications successfully, it is necessary to maintain privacy and security of the transmitted data.

The rest of the paper is organized as follows: section 2 explains security requirements, section 3 presents a review of the relevant work, section 4 presents the proposed protocol, section 5 shows the results and discussion, and section 6 concludes the paper.

2 Security Requirements

2.1 Confidentiality

Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighboring networks. The confidentiality objective is required in sensors environment to protect information traveling between the sensor nodes of the network or between the sensors and the base station from disclosure, since an adversary having the appropriate equipment may eavesdrop on the communication. By eavesdropping, the adversary could overhear critical information such as sensing data and routing information.

2.2 Authentication

In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. As in conventional systems, authentication techniques verify the identity of the participants in a communication, distinguishing in this way legitimate users from intruders. In the case of sensor networks, it is essential for each sensor node and base station to have the ability to verify that the data received was really sent by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. If such a case happens and false data are supplied into the network, then its behavior could not be predicted, and most of the times the mission of WSN will not be accomplished as expected.

2.3 Integrity

Data integrity ensures the receiver that the received data is not altered in transit by an adversary. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous, for example, for the healthcare sector where lives are endangered. Integrity controls must be implemented to ensure that information is not altered in any unexpected way.

2.4 Freshness

One of the many attacks launched against sensor networks is the message replay attack where an adversary may capture messages exchanged between nodes and replay them later to cause confusion to the network. Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. To achieve freshness, network protocols must be designed in a way to identify duplicate packets and discard them preventing potential mix-up.

2.5 Availability

Availability ensures that services and information can be accessed at the time they are required. In sensor networks there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks. The availability of a sensor and sensor network may decrease for the following reasons [1]:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. Besides, as communication power increases so does the chance of a communication conflict or interference. A single point failure exists if we use the central point scheme such as a single sink or gateway. This greatly threatens the availability of the network.

3 Related Work

The various protocols which have been proposed for security in wireless sensor network by various authors are SPIN, LEAP, TINYSEC, ZIGBEE, SM. 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 starts when a SPIN node obtains new data that it is willing to share. It does so by broadcasting an ADV message containing meta-data. If a neighbor is interested in the data, it sends 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 two secure building blocks SNEP (Sensor Network Encryption Protocol) and ÎźTESLA (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 lowers communication overhead adding only 8 bytes per message [2]. TESLA authenticates the initial packet using the digital signature. For an authenticated packet to be sent, the base station computes a MAC on the packet with the key that is secret at that point in time. When a node gets a packet, it can confirm that the base station did not yet disclose the corresponding MAC key [3].

The goal of LEAP (Localized Encryption and Authentication Protocol) is to satisfy the security properties of authentication and confidentiality in a wireless environment where the intruder may eavesdrop, inject packets, and replay messages [4]. LEAP, as a key management protocol for sensor networks, is designed to support in-network processing, while restricting the impact of a compromised node to the network. In order to support the in-network processing necessary for most applications of these networks while at the same time providing security properties, such as security and authentication, similar to those of pairwise symmetric keys, LEAP specifies four types of keys: individual keys, pairwise shared keys, cluster keys and group keys. Individual keys are symmetric keys shared between the base station and each of the nodes. For example, a node might use the individual key to notify the base station of a suspicious neighbor. Pairwise shared keys are symmetric keys shared between a node and each of its neighbors. While pairwise shared keys are used to establish cluster keys, they prevent passive participation which is desirable for in-network processing. Cluster keys are symmetric keys shared between a node and all of its neighbors. These cluster keys can be used for locally broadcast messages such as a routing protocol might use and are also used for updating the group key. The group key, a symmetric key shared between the base station and all of the nodes, allows encrypted and authenticated messages to broadcast through the whole network.

In the next protocol, TINY SEC, the dominant 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. However, neighboring nodes in sensor networks often witness the same or correlated environmental events, and if each node sends a packet to the base station in response, precious energy and bandwidth are wasted. To prune these redundant messages to reduce traffic and save energy, sensor networks use in-network processing such as aggregation and duplicate elimination [5, 6]. Since in-network processing requires intermediate nodes to access, modify, and suppress the contents of messages, it is unlikely we can use end-to-end security mechanisms between each sensor node and the base station to guarantee the authenticity, integrity, and confidentiality of these messages. With authenticated encryption, TinySec encrypts the data payload and authenticates the packet with a MAC [7]. Single shared global cryptographic key, link layer encryption and integrity protection cryptography is based on a block cipher. TinySec is a research platform that is easily extensible and has been incorporated into higher level protocols.

In ZIGBEE, the concept of a Trust Center is introduced in the specification. Generally the ZigBee coordinator performs this duty. This trust center allows other devices to join the network and also distributes the keys. There are three roles played:

- trust manager, whereby authentication of devices requesting to join the network is done,
- network manager, maintaining and distributing network keys, and
- configuration manager, enabling end-to-end security between devices [8].

It operates in both Residential Mode and Commercial Mode. The Trust Center running Residential Mode is used for low security residential applications. Commercial Mode is designed for 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. It therefore cannot periodically update keys and allows for the memory cost to be minimal, as it cannot scale with size of the network. In commercial mode, it establishes 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. There are three types of keys employed, the Master Key, the Link Key and the Network Key. Master keys are installed first, either in the factory or out of band. They are sent from the Trust Center and are the basis for long-term security between two devices. The Link key is a basis of security between two devices and the Network keys are the basis of security across the entire network. Link and Network keys, which are either installed in the factory or out of band, employ symmetrical key-key exchange (SKKE) handshake between devices. The key is transported from the Trust Center for both types of keys. This operation occurs in commercial mode, as residential mode does not allow for authentication.

In the latest protocol, SM (Security Manager), a new method of key agreement has been proposed in [9], whereby, when a new device joins a network, the Security Manager (SM) gives 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 device 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 shows that SM protocol offers more services than the other existing protocols.

4 Proposed Protocol

A security protocol refers to a set of rules governing the interaction between peer processes to provide a certain type of security service. We propose a new security protocol. Security Manager (SM) [9] does not guarantee data freshness; and so, we suggest a protocol to make up for the weakness of SM. This provides a solution to maintain data freshness by checking the message sequence number. When the message is sent, it is checked by the message sequence number whether it is already sent or not. If the message is old then no need to send that message. By this way, we can reduce overhead. By reducing the overhead we can make the protocol more efficient. Authentication and confidentiality are also provided. Authentication is defined to provide assurance about the originator of a message. This prevents an attacker from mimicking the operation of another device in any attempt to compromise the network.

Confidentiality means keeping information secret from unauthorized parties. The standard solution to keep sensitive data secret is to encrypt the data with a secret key that only the intended receivers possess, hence achieving confidentiality.

Additionally, this protocol provides freshness through the use of freshness checks. These checks prevent replay attacks, as devices maintain incoming and outgoing messages. Whenever a node wants to send message, message sequence number will be checked.

One of the many attacks launched against sensor networks is the message replay attack where an adversary may capture messages exchanged between nodes and replay them later to cause confusion to the network. Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. To achieve freshness, network protocols must be designed in a way to identify duplicate packets and discard them preventing potential mix-up. This extra feature shows that proposed protocol offers more security services than the existing one.

In the proposed protocol, time interval Δt accounts for request time, response time, delay, as shown in (1) and (2). Freshness is computed as the difference between the time a data item is generated and the time it is received at the sink.

With data freshness,

$$\Delta t = t_{Rq} + t_{Rs} + \Delta d + t \tag{1}$$

Without data freshness,

$$\Delta t = t_{Rq} + t_{Rs} + \Delta d \tag{2}$$

Where t_{Rq} = request transmission, t_{Rs} = response transmission, Δd = sum of delays (delays in transmission and propagation), t = time when message sequence number is checked. In case of without data freshness, no message is checked.

Accuracy is measured as the ratio of total number of messages received at the sink to the total number of messages generated. In case of without data freshness, no message is discarded but in case of with data freshness the message, which is already sent then no need to send again. Therefore, the ratio of without data freshness is always one but it is less than one in case of with data freshness. We can calculate the packet ratio by (3) and (4) as follows:

Without data freshness,

$$PacketRatio = send/receive = 1 \tag{3}$$

With data freshness,

$$PacketRatio = send/receive < 1 \tag{4}$$

5 Results and Discussion

Sensor network is a promising and upcoming technology with usage in important applications. The resource constraint hardware, specialized software, low energy devices and hostile environment makes the security in wireless sensor networks a challenging task as and when compared to the traditional computer networks.

Energy efficiency can be achieved by reducing the number of packets transmitted. Without data freshness, each node will send a packet that will be forwarded to the sink whereas with data freshness no need to send all packets, this reduced number of packets transmitted improve the efficiency. Figure 1 shows the average latency. In case of with data freshness, average latency is constant as the number of nodes is increased while it is increased in case of without data freshness.

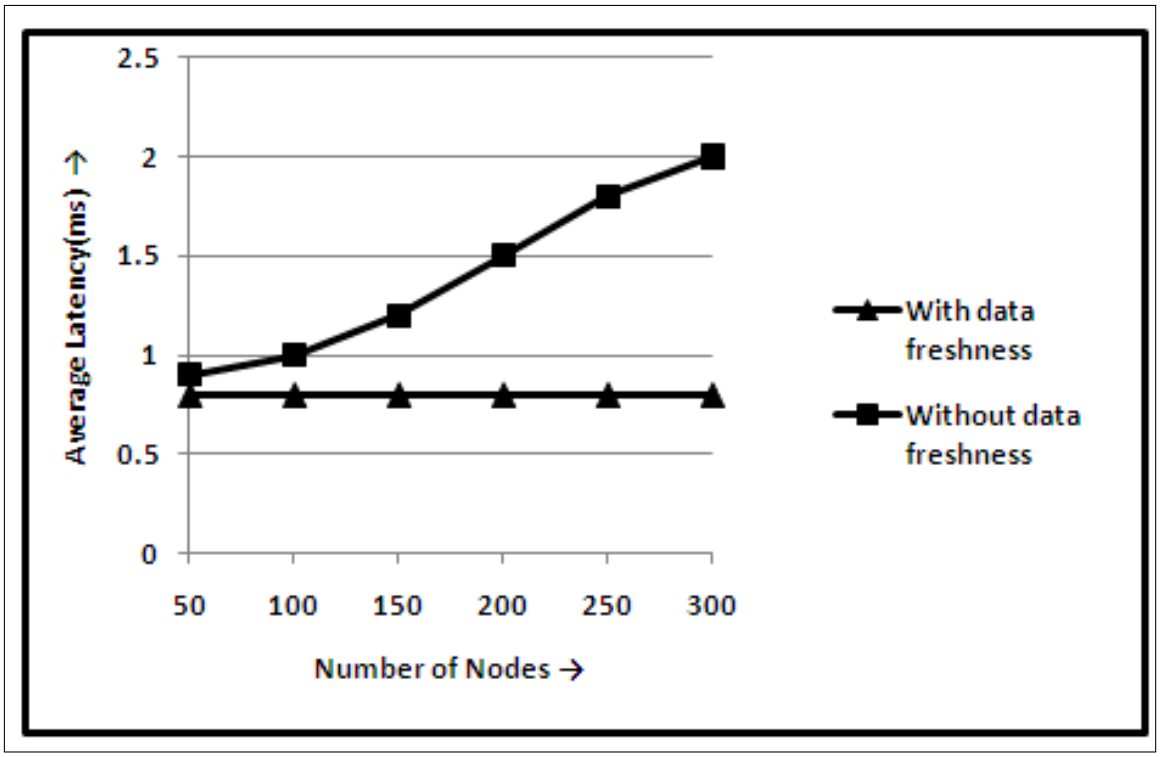

Figure 1: Number of nodes vs. Average Latency

Figure 2 shows the average packet delivery ratio. In case of with data freshness, average packet ratio is 100% because how many packets sent will definitely be received but in case of without data freshness some may already sent. This reduced number of packet transmitted also improves the efficiency.

The discussion of the security protocol and authentication mechanism allow for the construction of comparison table as in given Table 1, where they can be compared under similar headings. It can be seen from the table that new protocol is better than the existing protocol and offers more security services than the earliest one.

6 Conclusion

In this paper, firstly we propose a new security protocol for wireless sensor network. Secondly, we compared the performances of all the existing protocol with proposed protocol. SPIN

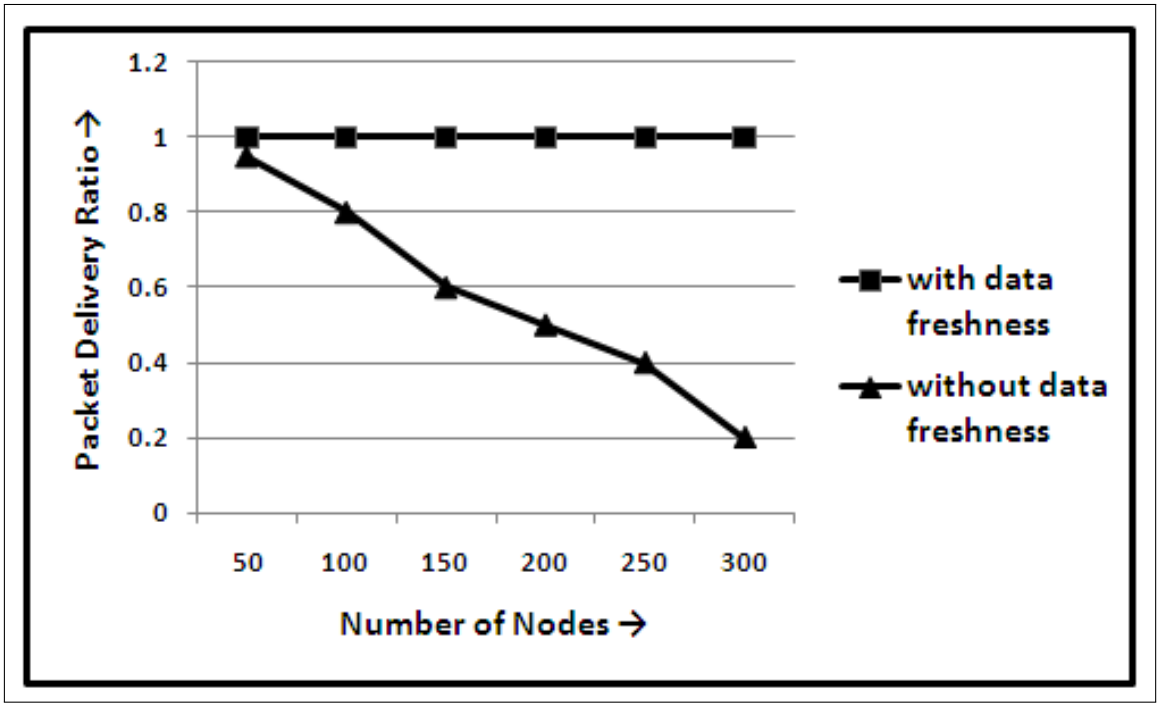

Figure 2: Number of nodes vs. Packet Delivery Ratio

Table 1: Security Architecture Comparison

Protocol / Service	C	F	I	Ava	IA	A
SPIN	YES	YES	YES	NO	YES	NO
LEAP	YES	NO	NO	NO	YES	NO
TINYSEC	YES	NO	NO	-	YES	YES
ZIGBEE	YES	YES	YES	NO	YES	YES
SM	YES	NO	NO	-	YES	YES
OUR PROTOCOL	YES	YES	-	-	YES	YES

C=Confidentiality, F=Freshness, I=Integrity, Ava=Availability, IA=Implicit Authentication, A=Authentication of user

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. Our protocol has one extra feature i.e. freshness. Freshness reduces the overhead. This extra feature shows that this is superior to the existing protocols. This also improves the efficiency.

Bibliography

[1] J.P. Walters, Zh. Liang, W. Shi, V. Chaudhary, *Security in Distributed, Grid, and Pervasive Computing*, Chapter 17, CRC Press, 2006.

[2] A. Perrig, R. Szewczk, J.D. Tygar, V. Wen, D.E. Culler, SPINS: Security Protocols for Sensor Networks, *Wireless Networking*, Vol. 8, No. 5, pp. 521-534, Sept 2002.

[3] A. Perrig, R. Canneti, J. D. Tygar, D. Song, The TESLA Broadcast Authentication Protocol, *CryptoBytes*, Vol. 5, No. 2, pp. 2-13, 2002.

[4] D. Boyle, T. Newe, Security Protocols for use with Wireless Sensor Networks: A Survey of Security Architectures, *Proceedings of the 3rd International Conference on Wireless and Mobile Communications, Guadeloupe, French Caribbean*, pp. 54, 04-09 March 2007.

[5] S. Madden, M.J. Franklin, J.M. Hellerstein, W. Hong, TAG: a Tiny Aggregation Service for Ad-Hoc Sensor Networks, *Proceedings of the 5th Symposium on Operating System Design and Implementation (OSDI), Boston, Massachusetts*, USA, pp. 131-146, 09-11 December 2002.

[6] S. Madden, R. Szewczyk, M.J. Franklin, D. Culler, Supporting Aggregate Queries Over Ad-Hoc Wireless Sensor Networks, *Proceedings of the 4th IEEE Workshop on Mobile Computing and Systems Applications (WMCSA), Callicoon, NY, USA*, pp. 49-58, 20-21 June 2002.

[7] C. Karlof, N. Sastry, D. Wagner, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, *Proceedings of the 2nd ACM International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA*, pp. 162-175, 03-05 November 2004.

[8] ZigBee Alliance, *ZigBee Security Specification Overview*, [Online] Available: http://www.zigbee.org/en/events/documents/december2005_open_house_presentations/zigbee_security_layer_technical_overview.pdf.

[9] 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 January 2006.