2009 International Conference on Machine Learning and Computing
IPCSIT vol.3 (2011) © (2011) IACSIT Press, Singapore

SPINS: Security Protocols for Sensor Networks

Fasee Ullah, Tahir Mehmood, Masood Habib, Muhammad Ibrahim

Shaheed Zulfikar Ali Bhutto Institute of Science and Technology Islamabad, Pakistan

Abstract. Sensor network is a dominant technology among different wireless communication technologies due to its great deal of efficiency. Security is the critical issue for every types of network whether it is sensor networks or other networks. So far, many of the researchers have thought to physically implement the sensor nodes and sensor networks but their work was not enough to create any valuable security for different communicating devices during communication processes.This paper presents a model that works on SPINS security building blocks because Sensor network works in very resource constraint environment and only SPINS security protocol can fulfill those requirements of the proposed model. SPINS provides two security building blocks, SNEP and µTESLA. This model presents some unique processing units features such as Beacon message, Data controller unit etc. This security model is best to achieve targets but main issue in sensor network is still not solved about the management of power (short battery life), computation overhead and low storage capacity of memory. The proposed model scenarios have been simulated in QualNet 4.5.

Keywords: Sensor node model, Sensor network communication architecture, ADC, DBU.

1. Introduction

A Sensor is a device that has the capability of sensing to receive a signal and responds to that signal in individual manner. Sensor network consists of multiple detection stations called sensor nodes; each of which is smaller in size and communicates with other nodes in short range distance. Sensor devices require high power consumption, low storage capacity, light weight and portable. Sensor networks are used for monitoring at various diverse locations. So the diverse locations are: Video surveillance, weather conditions monitoring, Air traffic control (Military purpose), Robot control etc. Sensor technology is one of the cheapest technologies to provide security in very restrictive environment. SPINS [1] offers two set of protocols SNEP and µTESLA. These two protocols provide enough security mechanism to adjust the requirements of sensor networks. SNEP (Secure Network Encryption Protocol) providing data confidentiality, two-party data authentication, and data freshness with low overhead [1]. µTESLA (the "micro" version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol) providing authenticated streaming broadcast [1]. Sensor node has less capacity of storage, memory and power. The design of SPINS protocol is much more summarized and there working operations are very suitable but there is no such efficient design of model or no communication architecture defined properly. Therefore, we proposed a model of wireless sensor node and also the communication architecture model of wireless sensor network. The working operation of the model is very simple and clear. It uses Beacon message unit which has predefined format to know the state of node whether it is active (live) or in de-active state.

Section 2 describes the existing model of sensor node and communication architecture model. Section 3 specifies security requirements & threats. The architecture of the proposed model and proposed communication pattern of sensor network is given in section 4, section 5 reviews SPINS security protocols, comparison of the existing and proposed model in section 6, while the simulation study is described in section 7, in section 8 we conclude with future work and in last References are given.

2. Existing Model of Sensor Node and Communication Architecture Model

Sensor node consists of four main components according to [2]: Sensing unit, Processing unit, Transceiver and Power unit, shown in figure 1[2]. Sensing unit has further subunits that are: Sensor and

ADC (Analog to Digital converter) units. The analog unit (ADC) produces analog signals which is based on sensor observations and converts the observed information into digital signal for further processes. The processing unit has also two units, Processor and Storage. The processor is just like a computer processor used for various computational and decision making purposes, and storage unit is used for storing of sensed information for future use. Transceiver has the capability to send and receiver different input and output data and power unit which is the vital thing for sensor nodes and sensor network. Power unit is used to maintain the voltage of sensor nodes. Other optional rectangle shapes are shown in dotted formatted in figure 1[2]. Sensor node also requires some knowledge from other node(s) and accurate routing path, to achieve the target through Location Finding System unit. Sometimes sensor node requires movement to different directions to find out the assigned tasks and this assigned task can find out through Mobilizer unit. The optional unit is power generator which will work as a backup power generator in case of any failure of power unit as shown in figure 1[2].

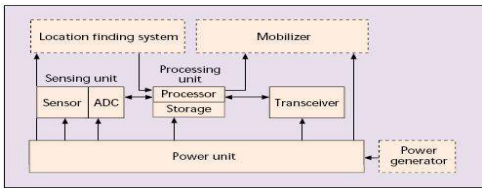

Figure 1: Components of Sensor Node [2]

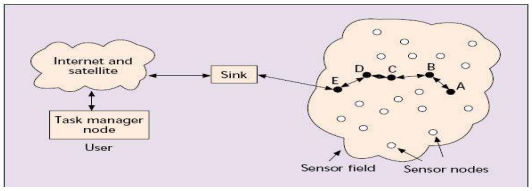

Figure 2: Sensor node communication architecture [2]

Usually sensor nodes are dispersed in sensor field. Each sensor can collect information, process the information and then send back the processed information by using of multi-hope to the sink (Base Station). The sink further sends to the internet or satellite for further processing and may communicate with task manager node as shown in figure 2[2]. There is no such organized form of data gathering and no cluster head to maintain communication inside sensor network and outside networks properly because any time can any kind of attack may occur and disturb their communication. The network of sensors consist of hundreds to thousands nodes are placed through out the sensor field. Each sensor node is placed “ten [2]” feet away from other node but this ten feet is also base on the use of sensors in unattended environment. The topology of sensor network is based on changing mode of requirements.

3. Security Requirements and Threats

A sensor network shares some common points with a typical computer network but also introduces new kind of requirements according to the security prospective such as “limited memory and storage space, limited power, unreliable transfer, conflicts [3]” etc. Therefore, sensor network requires some security without interruption during communication. To secure the sensor network the following services must be provided according to [3]: Data confidentiality, data integrity, data freshness, availability, self organization, time synchronization, secure localization and authentication. Sensor network works in a constraint environment as compared to the traditional network. Due to this situation it cannot directly use any existing security approach for wireless sensor network and can’t trust on Base Station. There are two main types of attacks: “Passive attack and Active attack [5]”.

4. A Proposed Model of Sensor Node

This proposed model has capabilities to make sensor node possible and feasible for wireless communication. “Sensing unit [2]” is the core processor of sensor node. This sensing unit processor consists of two subunits, sensor unit and ADC (analog to digital converter). Sometimes sensor unit is called sensor processor. The second unit of sensor node is Data Processing Unit (DPU). This unit is basically used for encryption and decryption of payload (data) and beacon messages. It can store up to 25 KB of information. The beacon message unit has connected with PDU for keeping the information when sensor unit is busy for other decisions. The beacon message unit connects mobilizer unit and PDU unit. Its main utility of connection with mobilizer unit is to share load balancing because of Transceiver unit; it will just send and receive the information other than beacon messages. The start and end bits of a sensor node is 01 and 10 respectively. The active node bits format is 1111 and dead (de-active) node bits format is 0000. So the whole

message format of Active node will be 01111110 and as same for the De-active node will be 01000010. The beacon message predefined interval is from 10 millisecond to 15 millisecond, if it exceeds from 15msec then that node will be considered as a dead node and it will be ignored for further communication in future and this interval can also keep on demand and must send to cluster head node within 15 millisecond otherwise the node will reconfigure itself again. The working functionality of this proposed model is shown in figure 3.

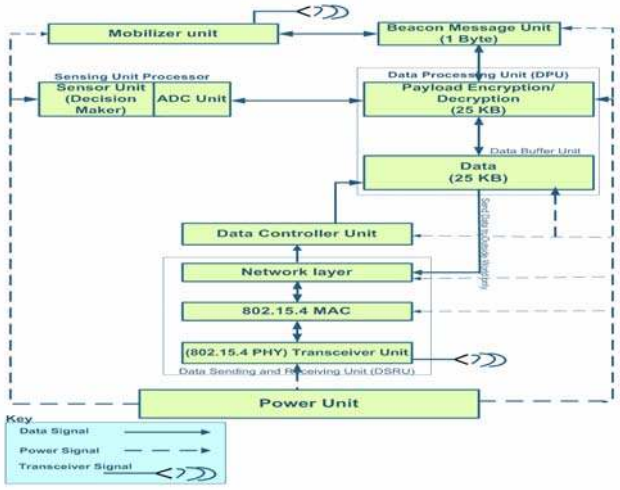

Figure 3: A possible architecture of a Wireless Sensor Node

The term Mobilizer is inherited from mobility because mobility is used from movement purpose as well as for fast communication vehicle or for sensitive connectivity. Mobilizer is the new feature of the sensor network. Sometime sensor node requires move to different directions (e.g. omni-direction) to find out the assigned tasks. The other benefit of this unit is to observe environments when sensor node is stationary. The sensor node must share new identity (ID) to the cluster head as sensor node moves gradually. Data Buffer Unit (DBU) is connected with Payload unit and Data controller. It also occupies 25KByte of storage space and it works as a RAM. This Data Buffer Unit is used to keep the data when DPU unit has overflow. Data controller unit which works as an intelligent way to know whether to send data to buffer unit or not and it has flexibility in load balancing when there is no capacity in buffer (RAM). Network layer is responsible for source to destination delivery of packets in multiple available paths (multi-hop) or networks. In sensor network there is no clear concept of transport layer because transport layer is basically used to make fragmentation of data but sensor node has limited memory and there is no option to use Transport layer for data fragmentation. SPIN protocol supports three types of messages according to [2]: ADV, REQ and DATA.

The primary concern of MAC protocol is collision avoidance, energy efficiency and scalability in a node density and the second concern is latency, fairness, bandwidth utilization and throughput in traditional MAC. IEEE 802.15.4 MAC protocol is designed for sensor network with low-rate of its special goal to keep less consumption of energy. IEEE 802.15.4 MAC uses superframe which is defined by a “periodic beacon [4]” signal and send to a “personal area network (PAN) coordinator [4]”. Physical layer has strong capabilities of frequency generation and frequency selection etc. There are two techniques used for signal modulation: “Binary and M-ary modulation [2]”. M-ary modulation is best to send multiple bits per symbol but its required high energy with complex circuit design while binary modulation has low-power consummation with many trade off parameters. Last one is power unit; Power unit is used to maintain the voltage of sensor nodes. The sensing capability of sensor node depends on the power unit because of without power unit the sensing devices may useless.

4.1. A Proposed communication architecture of Sensor Network

The communication pattern of proposed model of sensor network is based on hierarchical tree structure. No sensor node can directly communicate with outside sensor nodes. Every communication steps should be through proper channel. Before establishing the sensor network, there should be sensor field where sensor nodes will sense different sensing signal information from environments. In proposed figure 5, there are two cluster head (B, C) with its own cluster zone and one parent node (A) and their connectivity among these

nodes will be wireless technology. These sensor nodes (Base Stations) will have high capacity of storage as well as of power. In each cluster zone, there are number of sensor nodes and the nearest sensor node of other node will be sensor zone neighbour. No sensor node can directly communicate with other sensor node cluster. For example: sensor node of cluster B wants to communicate with sensor node of cluster C or outside of sensor field. That sensor will first send message to cluster head B and the cluster head B will send to parent node A of sensor field because parent node A works as gateway for inner and outer connectivity and the parent node A will forward the message to cluster head C and further is the responsibility of sensor head cluster C to forward the message to appropriate destination. Cluster head node is responsible for data gathering in its own cluster zone, inside communication and with outside world communication but in some cases, inside communication can be done directly between sensor nodes under the cluster head supervision. The parent node A is further connected with internet through wired technology for any query generated by deployment of sensor networking personnel or will give access of information to internet users.

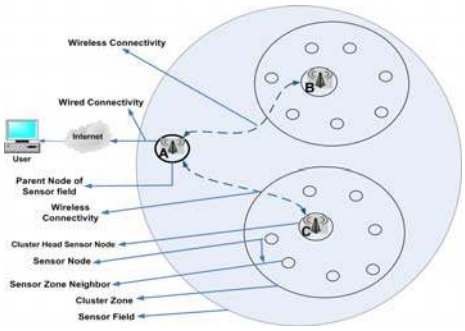

Figure 5: communication architecture of sensor network

5. SPINS Security Protocols

SPINS [1] provides two set of security protocols for securing communication channels according to different requirements of wireless security. These two protocols are "SNEP and μTESLA [1]". SNEP protocol provides: data confidentiality, two party data authentication, integrity, replay protection, weak message freshness. A simple form of data confidentiality is to keep the data encrypted but this is not a pure security of data, because to use another property of security called "Semantic Security [1]". A common solution for achieving message authenticity and integrity is to use a Message Authentication Code (MAC) [6]. This MAC is added with a message as a signature. On the receiver side, receiver performs the same computation on received message and compares the generated message MAC value with sent MAC value which gives whether that message is from legitimate user or not. So these scenarios make the SNEP protocol feasible for sensor network.

Base station and sensor nodes must be loosely time synchronized and each node has information of upper bound on maximum time synchronization error. This is the needs of μTESLA. Before sending an authenticated packet, the base station computes MAC on a packet with key and this key will be secret for certain period of time. When a receiver receives a packet, this packet will store in buffer and will assure the MAC key knows only base station and there will be no changed in packet during transmission.

6. Comparison of Existing and Proposed Models

Today's technology comes up more intelligent with various numbers of variations and this is the need of today's world.

6.1. Comparison of existing and proposed model of senor node

The common components in both models are: Sensor unit, Storage unit, Transceiver, Mobilizer (optional) and Power unit but in existing model, the working capability of mobilizer unit is for movement purposes only and that is an optional point but not included in existing model. In proposed model, Mobilizer has two functions; first for movement purpose to move anywhere and second is for observing the movement of other things in environment according to the needs. Transceiver works here as a physical layer used for sending and receiving of signals with different modulation schemes. The proposed model has Beacon message unit,

which is used to know the status of the node either it is active state or de-active state with its predefined format. Data controller unit which works as an intelligent way to know whether to send data to buffer unit or not and its main aim is load balancing when there is no capacity in buffer. The network layer, MAC layer and Transceiver (Physical layer) unit are called Data sending and Receiving Unit (DSRU).

6.2. Comparison of Communication architecture models of Sensor Networks

The communication architecture of existing model is not properly organized. In existing model, every sensor node can communicate through use of multi-hop reach to destination and there is no such centralized and high power node to communicate among sensor nodes whether it is locally or outside to the senor environment but in proposed model, everything is properly organized according to the need of communication rules and regulation.

7. Simulation Study

QualNet 4.5 is used for simulation of sensor networks showing graph of Packets flow. There are three nodes in this simulation. The whole simulation was run for 1 minute. This figure 7 shows the data flow information of sent packet, received packet and with throughput of nodes. This models offer a very good throughput as for as sensor network is concerned. It has very good throughput rate that is 11 Kbps. This model uses special mechanism for utilizing the scarce resources, as sensor networks has.

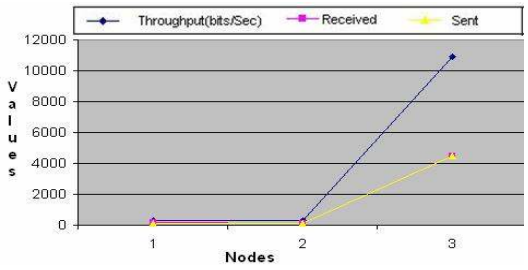

Figure 7: Packet Flow of Sensor Node

8. Conclusion

Security is the main concern of communication. Security has some merit and demerit according to the nature of practice. Sensor networks are one of them to provide high flexibility, fault tolerance, high sensing conformity and low cost. These features of sensors have given rise to many new applications from existing applications. In existing model, there is no centralized base station or cluster head node to control the communication and authentication process that can also bottleneck of the network but in proposed model, there is a centralized cluster head node to control all kind of communications with some unique features. In future there is a need of more examinations to work on the different modulation techniques of Transceiver unit especially in the area of sensor node and also need of memory with high computation speed process and power unit.

9. References

[1] Adrian Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar. SPINS: Security Protocols for Sensor Networks, *Mobile Computing and Networking 2001Rome*, Italy Copyright 2001 ACM.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Survey on sensor networks, *IEEE Communications Magazine*, 40(8):102–114, August 2002.

[3] J. P. Walters, Z. Liang, W. Shi, V. Chaudhary, Wireless Sensor Network Security: *A Survey, 2006 Auerbach Publications, CRC Press.*

[4] B. Krishnamachari, Networking Wireless Sensors, chapter no. 6, *Medium-access and sleep scheduling, published in 2005*, www.cambridge.org.

[5] K. CHANG and K. G. SHIN, "Distributed Authentication of Program Integrity Verification in Wireless Sensor Networks, *ACM Transactions on Information and Systems Security*, Vol. 11, No. 3, Article 14, March 2008.

[6] C. Karlof, N. Sastry, D. Wagner, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, 2004 *ACM 1581138792/04/0011.*