A Study for Security and Efficient Broadcasting of Sensor Network

Nam-Pil Cho*, Young-Ju Han *, Tai-Myung Chung **
* Computer Engineering Sungkyunkwan University
**School of Information & Communication Engineering Sungkyunkwan University
e-mail : {npcho, yjhan}@imtl.skku.ac.kr*, and tmchung@ece.skku.ac.kr**

Abstract - Lots of researches have been focusing on ubiquitous computing which means wherever, whenever, whatever the required information must be accessible. In ubiquitous computing environment, ubiquitous sensor network (USN) is the basis technology for gathering and transferring the required information.
However sensor network characteristically has more severe vulnerability than the existing networks do. The paper presents operation of secure protocols for delivering information in secure in ubiquitous computing environment and show improvement of the secure transferring protocol.

Keywords: Sensor Network Security

1 Introduction

Sensor network is kind of AD-hoc network that is consisted of sensor that collect and deliver information by specification request. Sensor network can divide by Ubiquitous Sensor network (USN) and Wireless Sensor network (WSN).

Although point Ubiquitous Sensor network and Wireless Sensor network intend each other is different, ultimate purpose of sensor network endows computing ability and radio communication to all things that can communication "When" or "Where" and embodies possible Ubiquitous surrounding. Sensor network may be applied from many parts of real life and much informations may get into through this. Authenticity of such passed information is important point to not only stability of service that is offered through sensor network but also personal information protection. But, sensor network by unique special quality security much limitations connote .Communication between sensor nodes uses radio communication way in sensor network. These radio communication method has big weakness to security although do not receive restriction of place. Also, have special quality that number of sensor is very much and insertion and exclusion of sensor, transfer occurs frequently. Therefore, tapping of data or insertion of malicious node can be achieved easily. Must recognize the importance of these security and consider from environment construction without allowing security application by the latter to construct efficient environment.

2 Relation research

This paper propose the improved SPINS[1] that is one of sensor network security protocols.

2.1 The definition of the sensor network

The sensor network is defined as a system composed of devices(processors) able to sense , do some simple jobs and communicate each other wirelessly. The sensor are attached to stuffs, and transmits and forwards the sensed information to a host or the Internet so the remote can notice what's going on there.[5] This means that computing devices can be attached to the stuffs and even to the people due to the developed technology.

2.2 Sensor network routing protocols

Routing techniques gets divided by plane Routing technique and hierarchical Routing techniques in sensor network.

2.2.1 SPIN

SPIN (Sensor Protocol for Information via Negotiation) [2] is a flat routing protocol for the sensor network. The main feature of the protocol is that the protocol needs negotiation to transmit to the interested nodes. This is the way to complement the deficiency of flooding.

The SPIN has three sorts of messages of ADV, REQ, DATA. A node sends an ADV message including meta data to transmit data. In the case that the receiving node is interested, the receiving node send REQ to the sender of the ADV message. The sender that received the REQ message transmits the date to the origin of the REQ message.

This shows the operation of the SPIN

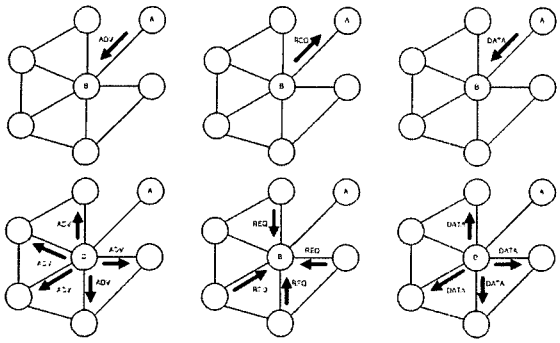

Figure 1 Operation SPIN

2.2.2 LEACH

LEACH (Low-Energy Adaptive Clustering Hierarchy) [3] adopted clustering routing method in other words hierarchical routing mothod.

Entire sensor network is devided into some clusters to communicate with the base station. Each cluster elects cluster head that is responsible for the transmitting the aggregated data from the nodes in the cluster. Cluster head are elected randomly for even battery comsume. LEACH uses the time unit called round that is also divided into election phase, and continuance state. In election phase, all node participate to elect the cluster head. once the cluster head is elected, the elected one announces that It is the cluster head for the round. In continuance state step, data transmitions are conducted according to the TDMA schedule. Nodes in the cluster sleep or wake up to reduce the energy consume according to the TDMA schedule.

2.3 *Sensor network security protocol*

2.3.1 SPINS (Security Protocol for Sensor Network)

SPINS is composed of SNEP (Sensor Network Encryption Protocol), μ TESLA (the " micro" version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol).

2.3.1.1 SNEP

SNEP provides the following security components.

- data integrity
- message authentication for each party
- replay attack protection
- freshness
- integrity

SNEP authenticates each party with the shared key based MAC. To provide confidentiality, the value of count is encrypted along with data. Since encrypting the same message shows the whole new value with the count value. MAC is used for the replay attack protection and, integrity. SNEP saves the amount of transmitted data, since it needs lower communication overhead, and the two node share the count value, and it uses secret key algorithm like RC5.

$$A \rightarrow B : N_A, H_A$$
$$B \rightarrow A : \{R_B\}_{\langle k_{encr}, C\rangle}, MAC(k_{mac}, N_A | C | \{R_B\}_{\langle k_{encr}, C\rangle})$$

K_{encr} : Security Key
K_{mac} : MAC Key
C : counter, initialization vector
N_A : nonce

Figure 2 SNEP Message

2.3.1.2 μ TESLA

Typically, the authenticating the broadcast data uses a public key algorithm to provide security. However, a sensor node can't afford to use a public key algorithm.

A μ TESLA using the one way key chain with time delayed mechanism is the modified version of TESLA[6] that emulates the source authentication in public key mechanism. A base station produces last key in key chain randomly, and derives other key with an one way hash function. Only in the time unit, the key is distributed.[7] After node caught the key in the time unit, the node can authenticate the message using the key derived from one way hash function.

$$M \rightarrow S : N_M$$
$$S \rightarrow M : T_S \mid K_i \mid T_i \mid T_{int} \mid \delta$$
$$MAC\ (k_{MS}, N_M \mid T_S \mid K_i \mid T_i \mid T_{Int} \mid \delta)$$

Ts : current time
Ki : one-way key chain using past interval i
Ti : starting time
Tint : time interval
δ : disclosure delay

Figure 3 μ TESLA Message

μ TESLA allows us to authenticate the broadcasting message from a BS. However the mechanism needs time synchronization. And as the number of nodes increases, and time assignment for each node increases, so it takes long time to authenticate from a BS to a leaf node. And in the case that a node needs to broadcast, the node send the message to the BS using SNEP, and the BS transmits the received message using μ TESLA. This is because a node has too limited memory and computing power to store all keys shared with each nodes, and although it can, it not able to recompute the key chain, each time the broadcasting occurs.

2.3.2 LEAP

LEAP[4] is the key management protocol having 4 encryption keys in the sensor network. In SPINS, a node communicates with other nodes through the method of broadcasting of BS. However LEAP authenticates one-hop broadcast data using one way key chain. It does have difference compared to the μ TESLA.

These are the encryption keys used in LEAP

- Private key : each node has its own key shared with the BS. This shared key makes the secure channel between the node and the BS.
- Group key : this is the key that the BS uses to encrypt the message to broadcast.
- Cluster key : It is key that abutting all nodes share one node and the node. This key is used mainly when do regional broadcasting
- Pairwise Shared key : each node shares a key with its one hop neighbor. The key is used for privacy or source authentication. For instance, it is used for distribute a cluster key securely to a neighbor.

3 Efficient broadcasting

Though SPINS is supporting broadcasting of node using μ TESLA techniques, this has shortcoming that node is no direct connection takes part in communication. Finally, broadcasting of node generates energy consumption of node that may not do direction participation. Furthermore, in case sensor network is consisted in vast area, broadcasting message that happen at specification node is valid own neighborhood or cluster extent inside, it is dozen. It brings waste in energy consumption side to whole network that all nodes of network are concerned in communication to transmit this message. Because one of method to solve these problem uses LEAP's cluster key, there is method that direct communication capacitates at node.

3.1 Research environment

Considered surrounding for energy consumption comparison of direct broadcasting at node that utilize LEAP's cluster key and use μ TESLA broadcasting like Table 1.

Node composition	Node of a n_{all} is distribution by true square shape	
Broadcasting exten t	Abutting 8 node	
Energy expenditure	Data transmission	E_{ds}
	Data reception	E_{dr}
	ADV, REQ Transmission	E_{mds}
	ADV, REQ Reception	E_{mdr}
Distance to base station (hop)	n	

Table 1 Research environment

The about 80% amount of energy consumption of node happens at sending and in-comming of data. Therefore, this research focuses data transmission and in-comming by broadcasting and progresses. LEACH's Clustering, SPINS and dictionary height division in LEAP suppose that is achieved beforehand, and most suitable path SPIN and from LEACH to base station transceiver system is established and data that is passed through most suitable path is valid to node of abutting unit of measure. LEACH's Clustering, SPINS and LEAP key distribution suppose that is achieved beforehand, and most suitable path to base station is established in SPIN and LEACH and data that is passed through most suitable path is valid one hop neighbor node.

3.2 SPIN routing protocol and SPINS security protocol

Sending of data in SPIN routing protocol is achieved limiting in interested node after send of MetaData data. That is, data delivery of 3 times is done all in case consider two nodes, and sending and in-comming of data of 6 times happen all. Data transmission type is broadcasting between sensor node. So, abutting nodes 45 times happen data transmission of sensor node. But excepts repetition in-comming and in-comming that is not valid consumption of energy through sending and in-comming of 14 times happens.

When data sending and in-comming between two nodes are done, is as following if state energy expenditure E_{nn}.

$$E_{nn}= (E_{mds}+3E_{mdr}+E_{ds}) +3(E_{mdr}+E_{mds}+E_{dr}) \quad (1)$$

Because must flow n hop to get base station, energy expenditure E_{nb} to base station arrival is as following.

$$E_{nb}=n\{(E_{mds}+3E_{mdr}+E_{ds})+3(E_{mdr}+E_{mds}+E_{dr})\} \quad (2)$$

Next formularize is displaying data transmission energy consumption expense from base station to node.

$$E_{bn} = n_{all} E_{dr} \quad (3)$$

3.3 SPIN routing protocol and node directly broadcasting.

When communicate between two nodes, expenditure of energy is same with formularize (1) and energy expenditure that reach to destination node is same with formularize (2). Only, n value has few value relatively. An experiment establishes n value by maximum 5. This

means that do broadcasting from sauce node to node of maximum 5 unit of measure.

3.4 LEACH routing protocol and SPINS security protocol

If number of sensor network's whole node are n_{all} and cluster exist as C, number of node per one cluster can mark by n_{all}/C. Also, maximum hop count is $(n_{all}/C)^{1/2}$ from one node to cluster head.

As is different from SPIN transmit data through direction broadcasting without negotiation process, energy consumption is as following.

$$E_{total} = n(E_{ds} + E_{dr}) + \left(\frac{n_{all}}{C}\right)(E_{dr}) \quad (4)$$

N value can have value from 1 to $(n_{all}/C)^{1/2}$ in formularize(4).

3.5 LEACH routing protocol and node directly broadcasting

It is resemblant way almost with 5.3, but show difference by practice way of routing protocol. That is, data transmission is achieved directly without negotiation process.

$$E_{total} = n\,(E_{ds} + E_{dr}) \quad (5)$$

In case n has big value in formularize (5), destination node or group great distance to street.

4 Conclusions

Necessary value is energy expenditure that is real at node in an experiment. Size of data being 500byte, energy expenditure is 2.4mW when sending, 0.8mW is consumed when receive. When meta data value ADV and REQ are 16byte, energy expenditure is 0.08mW when sending, consume 0.03mW energy when receive.[2] Figure 5 show to energy expenditure each model .Can confirm that energy wastage in SPIN that is representative plane routing technique is biggest. Also, can pare down consumptions of much energy relatively than broadcasting in same condition if take advantage of cluster key. Destination node or group's hop count can act by variable, but probability that specification node does broadcasting to node or group in far distance physically in wide sensor network is rare extremely.

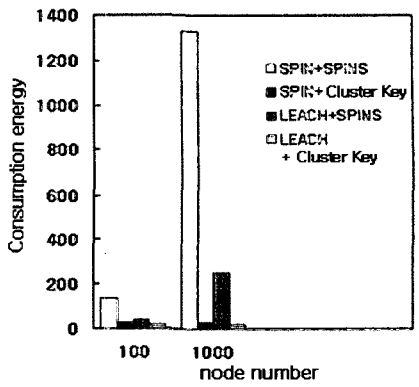

Figure 4 Energy expenditure of each model

Acknowledgement

This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment)

References

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar. "SPINS: Security Protocols for Sensor Networks." In Proc. Of Seventh Annual ACM International Conference on Mobile, Computing and Networks(Mobicom 2001), July 2001.

[2] W.R. Heizlman et al., "Adaptive Protocol for Information Dissemination in Wireless Sensor Network"Proc. ACM Mobicom'99, 1999, pp.174-185

[3] Wendi B. Heinzelman et al., "An Application-Sepecific Protocol Architecture for Wireless Microsensor Networks,"IEEE Trans. On Wireless Communications, Vol.1, No.4, Oct. 2002, pp.660-670

[4] Sencun Zhu, Sanjeev Setia, Sushil Jajodia "LEAP: Efficient Security Mechanisms for LargeScale Distributed Sensor Networks" CCS'03, Aug 2004

[5] Gang seokcheol "The future of sensor network age", Electron Information Center, 2004.

[6] Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Song. "Efficient authentication and signing of multicast streams over lossy channels." In IEEE Symposium on Security and Privacy, May 2000.

[7] L. Lamport. "Constructing digital signatures from a one-way function." Technical Report CSL-98, SRI International, Oct 1979.