Design of Secure Clustering Routing Protocol using SNEP and μTESLA on Sensor Network Communication

Kun-Won Jang[†], *Woo-sik Jung*[††], *Dong-kyu Shin*[†††] *and Moon-Seog Jun*[††††]

Dept. of Computer Science, Soongsil University

Summary
Contrary to general network, sensor network has many restrictions such as energy recharge. Accordingly, security mechanism used to general network cannot be applied to sensor network. Many researchers propose method of security and energy efficiency separately. To maximize energy efficiency, the methods to support data aggregation and cluster-head selection algorithm are proposed. To strengthen the security, the methods to support encryption techniques and manage a secret key that is applicable to sensor network are proposed. However, energy and security issues are trade-off. This paper is devoted to design secure routing protocol combining conventional routing protocol with security protocol. This new protocol is that encryption algorithm and key management method are applied to specific routing protocol. Finally, we appreciate proposed protocol and look about future work.

Key words:
Sensor network, Key management, Clustering, Energy savings.

1. Introduction

Recent progress in wireless communication technology introduces smaller sensor node and wider bandwidth for remote communication. Also this technology brings lower cost, lower energy and multi-functional sensor node.
Research directions related to sensor network are security and energy efficiency. In the respect of sensor network security, peculiarity that sensor has restricted resource and requirement to support low cost construction for a common use make security needs unimportant. Accordingly, many researchers propose privacy protection method using RFID tag that is sensor network application except encryption method [1]. However, simple privacy protection cannot solve security vulnerability in wireless network, so security protocol such as SPINS(Security Protocols for Sensor Network) [3] and LEAP (Localized Encryption and Authentication Protocol) [2] has been proposed. Next, in the respect of energy efficiency, energy recharge is impossible because many sensor systems may be operated in absence of manager or under hostile environment such as battlefield. So sensor network context is affected by the life cycle of applied sensor node and the methods for an energy saving such as Directed Diffusion [4] and LEACH (Low-Energy Adaptive Clustering Hierarchy) [5] are proposed.
This paper is devoted to propose new type of secure routing protocol that supports both energy efficiency and security. In section 2, we analyze proposed method related to security and energy efficiency for sensor network system. Next, in section 3, we propose secure clustering protocol combined security with routing protocol. In section 4, we analyze our proposal. Finally, section 5 offers conclusion and issues for the future work.

2 Related work

There is close correlation between energy efficiency and security strength. Security incurs processing overhead by additive CPU usage and restricted energy decreases the life cycle of encryption system or authentication key. When the life cycle of sensor network system expires, sensor network needs to be reconstructed and reinstall the secret key. This process brings necessarily additive energy consumption. Accordingly, relation between energy efficiency and security is trade-off and we must consider unified research. This section describes existed researches.

2.1 Security requirement

Conventional security solutions do not fit into sensor network system because these do not consider the structural specific of resource restriction and recharge problem. Recent researches are to minimize processing overhead and propose protocol that suit to sensor network.
SPINS [3] protocol provides not only data encryption but also message authentication and user identification service though this protocol uses symmetric key. Figure 1 shows time line key chain of SPINS protocol. SPINS protocol also provides broadcast authentication service using key chain.

Manuscript received August 2005.

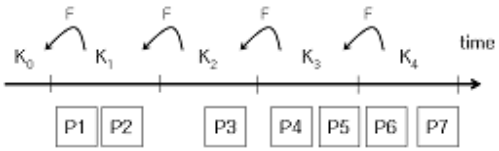

Fig. 1. SPINS's time-released key chain for source authentication

Symmetric key method has the problem that whole system may be vulnerable if one key is revealed in the case that many users share one key. So, key management is very important. Sensor network communication consists of several types [11]; BS (Base station) inquires for sensor node, nodes transmit data each other, and node transmits unified data to BS. LEAP [2] protocol provides various types of key management methods such private key, pairwise key, cluster key, and group key.

2.2 Energy requirement

Sensor network has restricted energy resource. Energy consumption patterns in sensor network are data processing and transmission. Data transmission cost is generally more expensive than data processing, so method that intermediate node integrates data and sends it to BS is preferred than method that each sensor node directly sends data to BS [4].

Fig. 2. Round time line of Set-up and Steady-state phase

Sensor node is standing by for energy saving except sending data. However, the node energy to gather data is rapidly exhausted because this node spends consistently its power for data gathering, integration, and transmission. LEACH protocol proposes clustering and energy consumption method for efficient data integration [5][12][13].

3 Proposed protocol

Vital considerations for sensor network are to maximize energy efficiency and provide proper security service by minimizing data storage and processing overhead. Many researchers have been studied separately energy efficiency and security issues so far. However, these issues are trade-off. The method to maximize energy efficiency must bring weak security and vice versa. Accordingly, we must consider both issues at the same time.

This paper is devoted to propose the method that induces balanced energy consumption by fair clustering mechanism and extends the life time of sensor network, and security method that minimizes power usage and processing overhead and can apply to sensitive sensor network system. Firstly, we define communication types and key interchange algorithms in sensor network, and propose secure clustering method. Also, we propose the method to exchange securely data after building cluster.

3.1 Definition

3.1.1 Key

This paper uses four types of keys; private key, pairwise key, cluster key, and master key [2]. All nodes include master key from manufacturing phase, and all keys is not submitted during communication and generated by function f(u). u is node, BS does not keep any keys and generates it by operation when needing it. The private key of node u is generated by master key.

$$K_u = f_{K^m}(u)$$

Communication between nodes is a general type and pairwise key is needed for this. Node u and v generate pairwise key and each node does using key generation function.

$$K_{uv} = f_{K^v}(u)$$

Cluster head and cluster nodes must share cluster key for communicating. Cluster head u and all cluster node v1, v2, v3, …. , vm generate cluster key and share it. Cluster u generates random value r and generates cluster key by key generation function. Generated cluster key is transmitted to all cluster nodes after encrypting it with pairwise key. C is counter value.

$$K_c = f_{K_u}(r)$$

$$u \rightarrow v_i : E_{|K_{uv},C|}(K_c), MAC(K_{uv}, C \mid E_{|K_{uv},C|}(K_c))$$

3.1.2 Message transmission

Node u transmits encrypted message D to node v like next and attaches counter C to it for semantic security. Key is different according to the communication type.

$$u : D = E_{|K_u,C|}(M)$$

$$u \rightarrow v : D, MAC(K_u, C \mid D)$$

3.1.3 Broadcasting

We use μTESLA [3] for broadcasting. μTESLA is loosely synchronized scheme. BS uses present time interval t for

computing the message authentication code (MAC) of a packet. If time interval t is over and system discloses key value K_t after delayed time i, node v can authenticate received packet. Accordingly, when nodes is added, new node must know authentication value $K_i = F(K_{i+1})$ and master key, and is loosely synchronized by the key release schedule of one-way key chain. The message that BS transmits to new node u must include present time T_s, Key K_i of one-way key chain used in past time interval i, launching time T_i at time interval i, time interval duration T_{dura} T, and delay time δ . New node v sends request message for broadcasting authentication and includes nonce for receiver identification. Next, BS sends authentication message to node v.

$v \rightarrow BS : N_v$

$BS \rightarrow u : T_s \mid K_i \mid T_i \mid T_{dura} \mid \sigma, MAC(K_v, N_v \mid T_s \mid K_i \mid T_i \mid T_{dura} \mid \sigma)$

3.1.4 Clustering

We use dynamic clustering method to increase energy efficiency by data integration [5]. For fair energy consumption, each node is randomly elected as a cluster head by probability $P_u(t)$, then $P_u(t) = 0$. So, this node is only cluster node until several rounds. To construct cluster, system computes provability $P_u(t)$ that the non-cluster head node of all sensor node N become a cluster head and non-cluster head node decides to become a cluster head at next round r+1. The cluster head number elected each round is k.

$$P_u(t) = \frac{k}{N - K\left(r \bmod \frac{N}{K}\right)}$$

3.2 Communication types

There are three types of communication forms such as unicast, multicast, and broadcast in sensor network. Unicast is the communication method between node and BS or node and node. Transmission from node to BS is the case that cluster head gathers, refines, and integrates data, and is encrypted with a private key that node and BS share using CSMA technique. Transmission from node to node is the case that non-cluster head node sends a raw data to cluster head, and is encrypted with a pairwise key.

$u \rightarrow BS : E_{|K_u, C|}(M), MAC(K_u, C \mid E_{|K_u, C|}(M))$

$u \rightarrow v : E_{|K_{uv}, C|}(M), MAC(K_{uv}, C \mid E_{|K_{uv}, C|}(M))$

Multicast is the communication method among nodes. Precisely, this is the case that cluster head sends a query message to all cluster nodes, and is encrypted with cluster key.

$u \rightarrow v_i : E_{|K_c|}(M), MAC(K_c, E_{|K_c|}(M))$

Broadcast is the communication method from BS to all sensor network nodes. Broadcast message needs not to encrypt but needs to authenticate source message. Because proposed protocol is installed by synchronized scheme, MAC may be verified by K^T_i that is disclosed after time interval i.

$BS \rightarrow *: M, MAC(K_i^T, M)$

3.3 Cluster formation

Although sensor network may not need communication security according to an application area, we assume that all communication messages in cluster need security for sensitive application area such as battlefield.

Node elected as cluster head must broadcast his qualification to all sensor networks. For broadcasting, node generates the key chain and computes all key values. However, the storage of key chain and computation bring a lot of overhead, so sensor node cannot perform these works. Accordingly, sensor node depends the generation of key chain, computation, and broadcasting on BS. The communication method between cluster head and BS is unicast.

① Cluster head broadcasts his qualification through BS

$u \rightarrow BS : E_{|K_u, C|}(M), MAC(K_u, C \mid E_{|K_u, C|}(M))$

BS that receives request message from cluster head performs broadcasting and releases keys after time interval i. Each node in sensor network buffers received broadcasting message and authenticates it with released key later.

② BS broadcasts the request works

$BS \rightarrow *: u, MAC(K_i^T, u)$

Receiver node v authenticates broadcast message, selects cluster head u by lowest energy path, and constructs cluster with cluster head u.

③ v selects a cluster head (clustering)\

$v \rightarrow u : v, MAC(K_v, u \mid v)$

④ u and v generate pairwise key separately by operation

$K_{uv} = f_{K_u}(u)$

After generating a pairwise key, node v sends Join-request message to cluster head u.

⑤ v sends Join-request message to u

$v \rightarrow u : E_{|K_{uv}, C|}(M), MAC(K_{uv}, C \mid E_{|K_{uv}, C|}(M))$

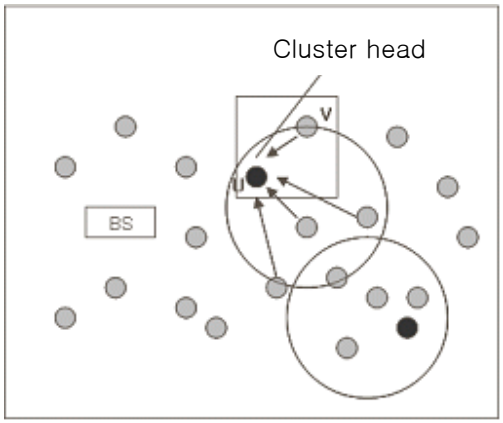

Fig. 3. Cluster head selection

After clustering, cluster head u constructs TDMA schedule and transmits it to cluster nodes. The communication type between cluster head and node needs cluster key.

⑥ Cluster head u generates a cluster key

$K_c = f_{K_u}(r)$

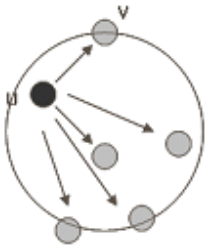

Fig. 4. TDMA schedule transmission

⑦ u sends generated cluster key to all cluster nodes

$u \rightarrow v_i : E_{|K_{uv_i},C|}(K_c), MAC(K_{uv_i}, C \mid E_{|K_{uv_i},C|}(K_c))$

⑧ u sends securely TDMA schedule using cluster key by multicast method

$u \rightarrow v(*) : E_{|K_c|}(M), MAC(K_c, E_{|K_c|}(M))$

3.4 Data Transmission

After clustering, cluster node may send data to cluster head during assigned time slot. To do this, BS transmits synchronized signal to each node and nodes can launch secure clustering at the same time.

$v \rightarrow BS : N_v$

$BS \rightarrow u : T_s \mid K_i \mid T_i \mid T_{dura} \mid \sigma, MAC(K_v, N_v \mid T_s \mid K_i \mid T_i \mid T_{dura} \mid \sigma)$

Non-cluster head node goes into stand-by mode for energy saving except the assigned time slot. Cluster head gathers and combines data from the node of cluster.

$v \rightarrow u : E_{|K_{uv},C|}(M), MAC(K_{uv}, C \mid E_{|K_{uv},C|}(M))$

When cluster head finishes the data transforming, it sends output to BS. Generally, the length between cluster head and BS is long and data volume is large. Accordingly, these processes need much energy. Transmission method uses fixed spreading code and CSMA [5] that node waits a time if other node is in data transmission and vice versa.

$u \rightarrow BS : E_{|K_u,C|}(M), MAC(K_u, C \mid E_{|K_u,C|}(M))$

4 Evaluation and analysis

This section evaluates proposed protocol by security and energy efficiency. We describe data confidentiality, integrity, authentication, and freshness related to the security, and fair energy consumption for a whole sensor network related to the energy efficiency.

4.1 Security

Attacker and other network must not access data that sensor node gathers in secure sensor network. This is very important issue in sensitive sensor network system such as battle field. Also, our proposed protocol can prevent packet fragmentation because SNEP [3] brings only 8byte overhead. Proposed protocol provides confidentiality and semantic security by an encryption. Because attacker can forecast the cipher text if system encrypts repeatedly the same plain text, we add the counter value to each message and can get different cipher text every time. Counter value is not transmitted between sender and receiver and both increase and keep it whenever transmitting the message. Lastly, we use MAC for providing data authentication and integrity.

Key management is very vital problem because SNEP uses symmetric key for decreasing message overhead of asymmetric key method. Because many nodes shares only one key in symmetric key method, all nodes may be vulnerable if the key is revealed. Accordingly, we use LEAP [2] protocol for secure key management.

Proposed protocol needs the secure communication between node and BS, and nodes for clustering. We propose various key management schemes according to the communication type such as unicast, multicast, and broadcast. Also, proposed protocol can encrypt and authenticate all processes of clustering and data transmission.

For eliminating spoiled node and adding new node, secure protocol must provide broadcasting service. We use μTESLA [3] that is symmetric key method using delayed key disclose. This method can prevent an attacker from disguising as BS through time slot, and can securely add a new node.

Table 1 shows application protocols and mechanisms that this paper uses.

Table 1. Applied security service

	SPINS	LEAP	Mechanism
Confidentiality	O		Encryption
Semantic Security	O		Counter
Data authentication & Integrity	O		MAC
Freshness	O		Counter & nonce
Key management		O	

4.2 Energy efficiency

There are many researches related to the energy efficiency such as data-centric protocol. Because the cost of data transmission is more expensive than the cost of data processing, we can save the energy if mediate node can integrate data and send only required data. Addition to this, the communication type between remote sensor node and BS is based on multi-hop scheme, so more energy is needed. However, these data-centric protocols may bring intensive energy consumption. Cluster head continually communicates with its node and should send gathered data to BS. Accordingly, the energy of specified node is exhausted and whole network must be reinstalled. Our proposal checks hot spot and changes the cluster head by each round. Although we need additive energy to change cluster head, there many advantages that all sensor node spend fair energy and keep consistent performance during the lifetime of sensor network.

5 Conclusion

The advantage of sensor network is the easiness to apply and manage it. If sensor network system is installed once, node can consistently gather data during its lifetime without concerning its context. However, because its lifetime may be decreased due to restricted resource and impractical recharge method, security service cannot be provided and many researchers have been proposed only restrictive method related to the energy efficiency. Accordingly, this paper is designed to combing existed researches related to energy efficiency with security service that have been studied separately so far. Because energy efficiency and security are trade-off, we must consider the effect and output when both are applied to the system. The security level of sensor network may be different according to the application area. Low security level may be applied if data is not vital, and high security level must be applied if data is sensitive. This paper proposes the method that is fit into high security service among various communication types of sensor network. We hope for the research of differentiated security level and energy efficiency by the application service.

References

[1] S. Sarma, S. Weis, and D. Engels, " RFID Systems and Security and Privacy Implications," Auto ID Center White Paper, November 2002.

[2] S. Zhu, S. Setia, and S. Jajodia, " LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," In Proceedings. of the 10th ACM CCS '03, October 2003.

[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, " SPINS: Security Protocols for Sensor Networks," In Proceeding. of Seventh Annual ACM International conference on Mobile Computing and Networks(Mobicom), July 2003.

[4] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," In Proceedings. of Fourth Annual ACM International conference on Mobile Computing and Networks(Mobicom), August 2000.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Transactions on Wireless Communications,,Vol. 1, No. 4, pp. 660-670, October 2002.

[6] R. Gennaro and P. Rohatgi, "How to sign digital streams," Advances in Cryptology - Crypto '97, In Burt Kaliski, editor, pp. 180-197, 1997.

[7] P. Rohatgi, "A compact and fast hybrid signature scheme for multicast packet authentication," In 6th ACM Conference on Computer and Communications Security, November 1999.

[8] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," IEEE Symposium on Security and Privacy, May 2000.

[9] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," In Advances in Cryptology, Proceedings of CRYPTO'92, LNCS 740, pp. 471-486, 1993.

[10] C. Karlof, N. Sastry, U. Shankar, and D. Wagner, "TinySec: TinyOS Link Layer Security Proposal," Unpublished manuscript, version 1.0, July 2002.

[11] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," To appear in Proceeding of First IEEE Workshop on Sensor Network Protocols and Applications, May 2003.

[12] T. Shepard, "A channel access scheme for large dense packet radio network," In proceeding of ACM SIGCOMM, pp. 219-230, August 1996.

[13] T. Kwon and M. Gerla, " Clustering with power control," In proceeding of MILCOM, vol. 2, November 1999.

[14] T. Murata and H. Ishibuchi, "Performance evaluation of genetic algorithms for flowshop scheduling problems," Proceeding of 1st IEEE conference Evolutionary Computation, vol. 2, pp. 812-817, June 1994.

Biography

Kun-Won Jang received the B.S. degree in English Literature and Management Information System from Korea Univ., Korea, in 1998, and the M.S. degrees in Computer engineering from Soongsil Univ., Korea, in 2003. His research interests include in the Network Security, Sensor Network, PKI, and Information Hiding.

Woo-Sik Jung received the B.S. degree in Computer Science at Kwangwoon Univ., M.S. and Ph.D degrees in computer science from Soongsil Univ., Korea, in 1982, 2003. He has been taught and researched as a full professor at Dongseoul College. His research interests include Network Security, Cryptography and Information Hiding.

Dong-Gyu Shin received the B.S. degrees in Division Of Information Communication from Cheonan Univ., Korea, in 2004. His research interests include in Network Security, Sensor Network, RFID, Payment System and Cryptography.

Moon-Seog Jun received his B.S. at Soongsil Univ, M.S. and Ph.D degrees in computer science from University of Maryland, USA, in 1985, 1988. He taught computer Network at Morgan State University and researched Physical Science Lab. New Mexico, USA. He has been taught and researched as a full professor at Soongsil University. His research interests include Network Security, Cryptography, Computer Algorithms, and Network Protocol.