Reliable Random Key Pre-Distribution Schemes for Wireless Sensor Networks

Si Gwan Kim

***Abstract*—The development of small-size, low-cost, and low-power sensors that possess sensing, signal processing and wireless communication capabilities is becoming popular for the wireless sensor networks. Cluster-based routing protocol is a good choice to achieve the energy efficiency for the wireless sensor networks. Due to the limited resources and energy constraints, complex security algorithms cannot be employed in sensor networks. In this paper, we propose a cluster-based routing protocol with a key pre-distribution scheme which improves the resilience of the network. In addition, our scheme is suitable for link error-prone environments. We describe the details of the algorithm and compare it with other schemes. Simulation results show that the proposed scheme achieves better performance in terms of security, efficiency and key connectivity.**

***Index Terms*—Cluster, key pre-distribution, security, wireless sensor networks.**

I. Introduction

Wireless sensor network(WSN) is a core technology in ubiquitous computing. Composed of tens and thousands of sensor nodes, sensor network can work in the environment to which human cannot easily approach. Security is critical for WSNs applications, such as home security monitoring and military deployments. In these applications, each sensor node is highly vulnerable to many kinds of attacks due to each node's energy limitation, wireless communication, and exposed location, which make the task of incorporating security in WSNs a challenging problem. In WSNs security, the key management problem is one of the most fundamental aspects.

The clustering technique is a good routing solutionthat minimizes the battery energy in the WSNs [1], [2]. Cluster is formed by each cluster head and cluster member collects information on surrounding environment and processes it to send it to cluster head. Cluster head can prevent flooding of inefficient query by performing data combination to prevent the transmission of redundant or similar information.LEACH, which is the representative clustering technique, is composed to select a cluster head for each cluster in each round. However, cluster head of each cluster cannot work as head in diverse situations such as link disconnection, node movement, etc. Thus, the information of member node cannot be sent to head node sometimes. This paper suggests a new reliable cluster head selection algorithm to improve such problem of LEACH. The suggested cluster head selection algorithm selects two cluster heads in each round to increase the probability of sending message of member node to sink node. In addition, security mechanism is enhanced by incorporating random key pre-distribution schemes.

The key management problem has been extensively studied in the WSNs [3], [4]. However, applying the public key management scheme in the WSNsis impractical due to the resource constraints of sensor nodes in the real world. The key pre-distribution scheme using symmetric encryption techniques is another form of solution. Eschenauer and Gligor [5] proposed a random key pre-distribution scheme. Before deployment, each sensor node receives a random subset of keys from a large key pool. Two neighbor nodes find one common key within their subsets and use that key as their shared secret key. In the cluster-based protocol, cluster head node and its member node must have their shared keys to communicate. But there may be some cases where orphan nodes which do not share the key between the cluster head nodeand their member nodes in the cluster may exist.Our algorithms reduce the number of orphan nodes as we have two cluster heads in a cluster.

In this paperwe suggesta random key pre-distribution scheme based on our previous cluster head selection algorithms [6] to improve the security issues. The suggested cluster head selection algorithm selects two cluster heads in a cluster for each round to increase of probability sending message of member node to sink node so as to reduce the number of generated orphan nodes and then to improve the message delivery ratio. By simulation,it was confirmed that cluster head selection algorithm suggested in this paper improved message deliveryratio than the previous algorithm when wireless link error occurs.

The remainder of the paper is organized as follows. Section II describes related works. Section III discusses our schemes. Section IV evaluates the proposed schemes. Finally, we summarize our results in Section V.

II. Related Works

Typical sensor networks applications include a variety of military, medical, and environmental applications. In these applications, the tasks performed by the sensors include sensing the environment, processing the data, and sending data to the base station.

Cluster-based routing in wireless sensor network prevents unnecessary energy waste caused by redundant transmission of similar data of adjacent node and to reduce load on the relay node. The operation of LEACH protocol based on the cluster is composed of two stages called round and it is formed of the repetition of such round. As adjacent sensor nodes usually have similar data, cluster head collects data

Manuscript received April 23, 2014; revised July 7, 2014. This work was supported by Kumoh National Institute of Technology.

Si Gwan Kim is with Kumoh National Institute of Technology, Gumi, Korea (e-mail: sgkim@kumoh.ac.kr).

DOI: 10.7763/IJIET.2015.V5.584

from cluster member node to reduce energy waste caused by redundant transmission of information. Then, they are combined and directly transmitted to sink node.In many applications, some sensor nodes may fail or be blocked due to power shortage, node malfunction, or environmental interferences. The failure of sensor nodes should not affect the overall task of the sensor network. Tolerating the failure of CHs is necessary to avoid the loss of valuable sensor data. The easiest way to recover from a CH malfunction is to reorganize the cluster. However, this reorganizing the cluster requires additional time and consumes valuable resources. Another solution is to assign backup CHs for recovery. The selection of a backup and the role such spare CH will play during normal network operation varies. When CHs have long radio range, neighboring CHs can adapt the sensors for the malfunctioning cluster. Rotating the role of CHs among nodes in the cluster can also enhance the fault-tolerance as well as the load balancing.

Various key distribution schemes have been studied for wireless sensor networks, considering the resource-constrained sensor nodes used in these networks [7]-[13]. Eschenauer and Gligor [5] proposed a random key pre-distribution scheme. In this scheme, each sensor node randomly picks a set of keys from a key pool before deployment so that any two sensor nodes have a certain probability to share at least one common key. After key discovery, two neighbor nodes that have a common key use that as the key for secure communication. Based on this basic scheme, several schemes with enhanced security features have been suggested. Chan et al. extended this idea and developed two key pre-distribution techniques: a q-composite key pre-distribution scheme and a random pair-wise key scheme. Both schemes improve the security over the basic key pre-distribution scheme. But, they cannot scale to large sensor networks.

Liu [14], [15] improved the resilience of the network with the "threshold schemes". In this scheme, when the number of compromised nodes is less than the threshold, the probability that communications between any additional nodes are compromised is nearly zero. This property lowers the initial payoff of small-scale network breaches to an adversary and makes it necessary for the adversary to attack a significant portion of the network.

SecLEACH [16] is a LEACH-based protocol for securing node-to-node communication in WSNs. Using random key pre-distribution, SecLEACH introduced symmetric key and one-way hash chain for security. SecLEACH provides authenticity, confidentiality, integrity and freshness for node-to-node communication.

III. Our Algorithms

Our routing algorithm is based on. At first, some initializations are needed for key managements. Then, setup stage and steady state stage follows.

A. Initializations

Prior to network deployment, we generate a large pool of S keys and their unique ids. Each node is then assigned a ring of m keys drawn from this pool pseudo randomly. For each node i, we use a pseudo random function (PRF) to generate its unique id_i. id_i is then used to seed a pseudo random number generator (PRNG) of a large enough period to produce a sequence of m numbers. R_i, the set of key ids assigned to i, can then be obtained by mapping each number in the sequence to its correspondent value modulus s. Also prior to deployment, each node is assigned a pair-wise key shared with the base station(BS).

B. Set up Stage

Two cluster heads which consist of primary cluster head and secondary cluster head are selected in setup stage. Primary cluster head node is decided first. Initially, node n selects random number between 0 and 1 to select the primary cluster header. If the number is below threshold, T(n), the node becomes the primary cluster header in the current round. Threshold is defined as follows and any other method of previous works can be used to select a head node. If a random node is selected to be the primary cluster head, this primary cluster head advertises the fact that it becomes the primary cluster head, *i.e.*, ADV_CH message including its ID and nonce to neighboring nodes by using CSMA MAC protocol. Each cluster head selects other CDMA code to avoid interference with other cluster and informs this CDMA code to sensor node in the cluster. After receiving ADV message from each cluster head, each normal node other than head node computes the set of CHs keys IDs and choose the nearest CH, which becomes the primary cluster head, with whom they share a key; these sensor nodes then send JOIN-REQ message, protected by MAC that is produced by the shared key, and the nonce that is broadcasted by the primary cluster head node, to prevent reply attacks; the ID of the key chosen to protect the link is also sent with the to make the primary cluster head node knows which key to use for verifying the MAC. To complete the setup phase, CHs send the time schedule to sensors that choose to become their members (step3).

$$T(S) = f(x) = \begin{cases} \dfrac{P}{1 - P \times (x \bmod \dfrac{1}{p})}, & \text{if } n \in G \\ 0, & otherwise \end{cases}$$

P refers to the probability to be cluster header, r, the present round and *G*, the group of nodes which are not selected as cluster header in the recent 1/P round.

After selecting its own primary cluster head, each node sends JOIN-REQ message to its primary cluster head by using CSMA MAC protocol. Then, the primary cluster head receiving JOIN-REQ decides its member node to which its cluster belongs. After selecting node that consumes the least energy among member nodes, primary cluster head informs this node as the secondary cluster head. These two cluster head nodes are in charge of coordinating data transmission of nodes in their cluster. Primary cluster head arbitrarily separates member nodes into two groups and composes TDMA schedule to transmit them to secondary cluster head and member nodes. Setup stage finishes and steady-statestage begins after TDMA schedule is known to all nodes in the cluster.

C. Steady State Stage

The steady state stage that follows setup stage where cluster is formed is composed of frames. In this stage, member nodes send their data to the primary cluster head or secondary cluster head only from their transmission slot assigned in advance. Each sensor node transmits data by using CDMA code received from primary or secondary cluster head in the assigned time and turns off transmission logics in the time which is not assigned to it so as to save energy. Sensor-to-CH communications are protected using the same key used to protect the Join Request message. To prevent replay attacks, a value calculatedfrom the nonce and the reporting cycle is also included. After receiving data from all sensors in the cluster, the primary or secondary cluster head decrypts sensor data and combine data, then sends it to the BS protected by the symmetric key shared with the BS. A counter is included in the MAC value for freshness.

Fig. 1 and Fig. 2 show the examples how cluster is formed for the previous LEACH algorithm and suggested algorithm. In the LEACH method, head node is composed of *H* and its member node is composed of n_0~n_8. Time schedule is shown in Fig. 1. In this case, there is only one cluster *H* to which member node belongs in one round and thus data is sent to only one head node as shown in Fig. 2.

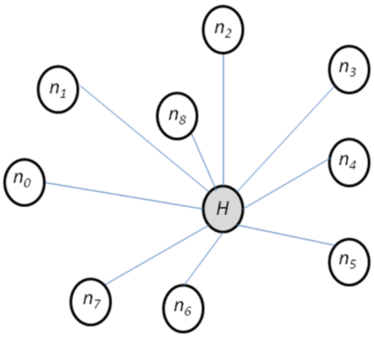


Fig. 1. Example of clustering (LEACH).

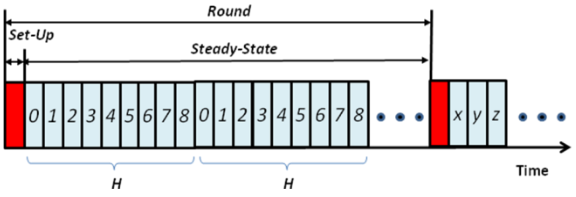
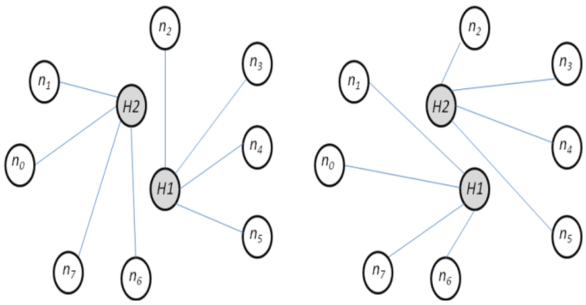


Fig. 2. Example of time schedule (LEACH).



a) First frame b) Second frame

Fig. 3. Example of clustering (suggested algorithms).

In the suggested method, two cluster heads are selected when cluster is formed and each member node belongs to two cluster heads. Thus, message is alternately sent with two head nodes as per time schedule. Fig. 3 shows our method with same node configurations as in Fig. 1. Member nodes belonging to a cluster arenode n_0 ~n_7 and head nodes are *H*1 and *H*2. Node *H* acts as the primary cluster head *H*1 and node $n_8$act as the secondary cluster head *H*2. The member node managed by two cluster heads are composed of member node group, n_2, n_3, n_4, n_5 and another member node group, n_0, n_1, n_6, n_7. Once steady state stage starts, *H*1 communicates with node n_2, n_3, n_4 and n_5. And, node *H*2communicates with node n_0, n_4, n_6 and n_7 in the first frame.Then, *H*1 communicates with n_0, n_4, n_6 and n_7, and *H*2 communicates with n_2, n_3, n_4 and $n_5$in the second frame and so on. As shown in Fig. 4, this process is repeated in the current round. Once this round is terminated, another round starts with set-up stage and steady state stage.

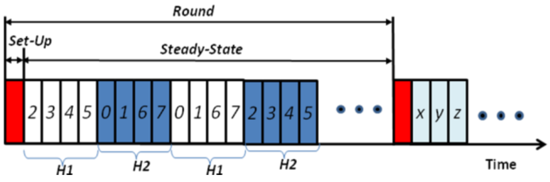


Fig. 4. Time schedule for node H1 and H2.

IV. Simulations

The performance of clustering algorithm suggested through simulation is analyzed in this section. NS-2 is used to perform simulation to compare and analyze performance with that of LEACH with security features such as SecLEACH. Our algorithm performs better than the previous SecLEACH scheme in message delivery ratio, the quantity of received data in comparison with the consumed energy and overhead of cluster composition.

A. Simulation Environment

SecLEACH algorithm [16] and suggested algorithm are performed in the same condition with various simulation environments. The size of network is 50m ×50m and sink is located outside of network. Simulation environments are as follows: simulation time is 900 sec, packet size is 50 bytes, communication range is 15 m, initial energy is 2 J, aggregation energy is 5 nJ, transmitter energy is 600 mW, receiver energy is 300 mW and idle energy is 120 mW. The performance of algorithm is observed with various network densities by increasing the number of message generating nodes from 20 to 60. The network node periodically reorganizes cluster and cluster head collects data by assigning same time to member node of cluster. We have performed three experiments to evaluate our schemes as follows: Number of Orphan Nodes,Packet Delivery Ratio and Overhead of maintain two cluster heads.

B. Number of Orphan Nodes

During the clustering decision, some nodes will not be matched with any cluster head because there may be no share key between the member node and its cluster head node.We call these nodes orphan nodes.Some solutions to deal with the orphan nodes are suggested in the previous works.Generally, more orphan nodes result in the poor performance of the network.

Fig. 5, Fig. 6 and Fig. 7 show the number of orphan node with varying the size of key ring (from 20 to 75) and key pool (from 1000 to 3000). The average ratio of cluster head in the network is 5%. In all cases, as the size of key ring grows, the number of orphan nodes decreases as expected.Our method always performs better than the previous works, because our method generates less orphan nodes than SecLeach. Less orphan nodes mean the connection probabilities between the head nodes and their member nodes are high. Thus our methods deliver sensor data from a node to the cluster head and finally to BS with higher probability than SecLeach.

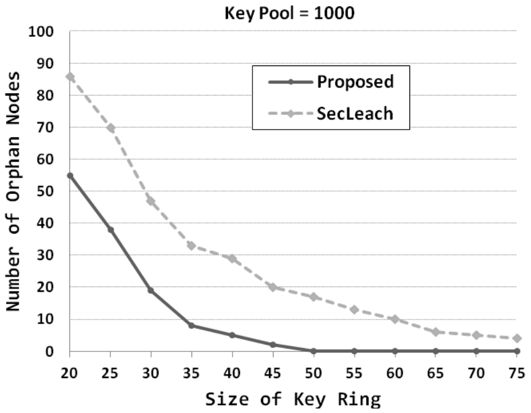


Fig. 5. Generated orphan nodes (pool=1000).

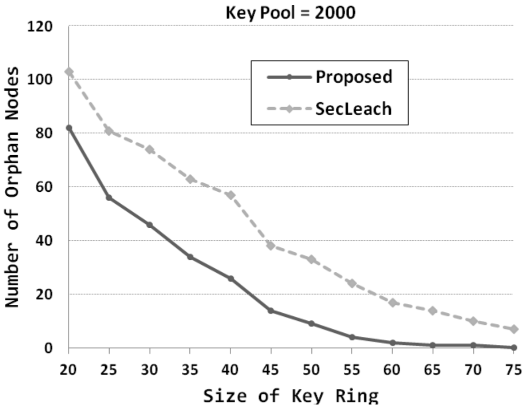


Fig. 6. Generated orphan nodes (pool=2000).

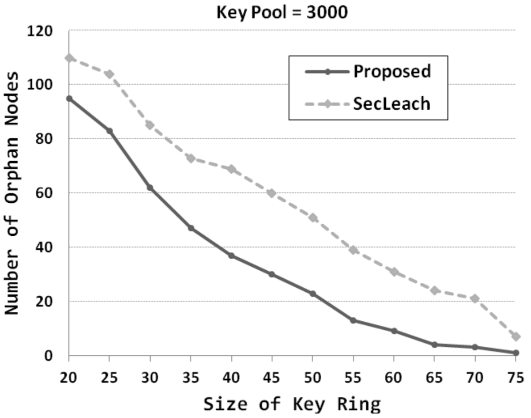


Fig. 7. Generated orphan nodes (pool=3000).

C. Packet Delivery Ratio

Message delivery ratio of member node to sink was simulated with5% wireless link errors. The message delivery ratio was measured when the number of node was 100, the number of message generating node is 20, 40 and 60 and the interval time between messages changes from 0 second to 100 seconds.

Fig. 8, Fig. 9 and Fig. 10 show message delivery ratio when the number of message for each node is 20, 40 and 60 suggested algorithm was found to have the transmission ratio higher than that of SecLEACH algorithm by about 10%. This is because the numbers of orphan nodes are generated more for the SecLeach, where there may not exists share keys between head node and its member node. In addition, the message collected in the member node cannot be sent to the destination, i.e., sink node, since the route to cluster head is lost by wireless link error between the head node and its member node in the case of SecLEACH. However, the ratio of successful transmission to sink node is high, because the suggested algorithm can selectively transmit the message generated in member node to two cluster heads in each cluster.

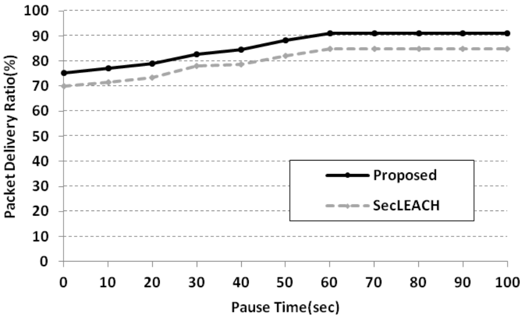


Fig. 8. Message delivery ratio (sources=20).

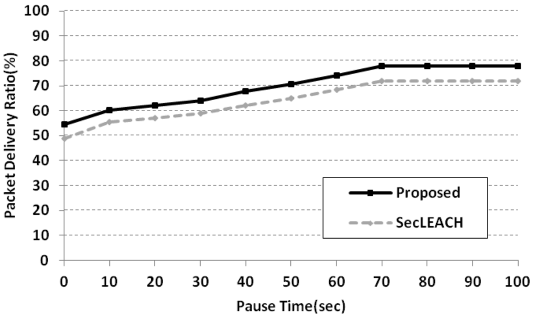


Fig. 9. Message delivery ratio (sources=40).

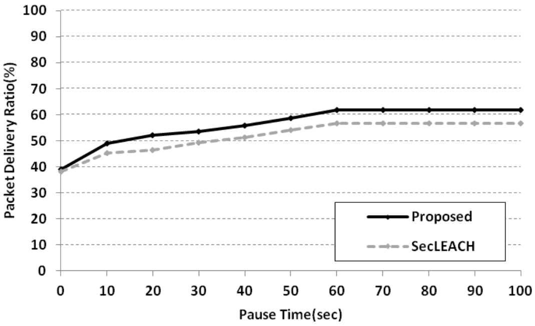


Fig. 10. Message delivery ratio (sources=60).

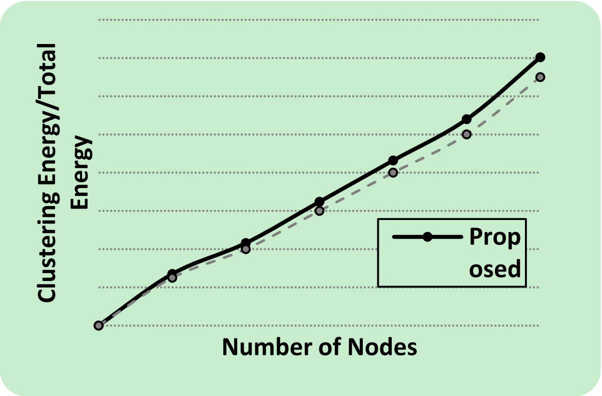


Fig. 11. Overhead of maintaining two cluster heads.

D. Overhead of Maintaining Two Cluster Heads

Fig. 11 shows the ratio of energy consumed to compose cluster compared to whole energy consumption byvarying the number of node from 100 to 600 so as to check the overhead of maintaining two cluster heads. The suggested algorithm was measured to consume slightly more energy in clustering than the SecLEACH due tomaintaining two cluster heads.

V. Conclusion

This paper suggests secure cluster-based routing algorithm based on key pre-distribution scheme. Our proposed algorithm improves the probability of transmission to sink node, even if link errors exist in sensor network. Since each cluster has only one cluster head in the cluster-based algorithmin the previous works, message of member node may not be transmitted to sink node through head node due to link error. In this paper, we have attempted that message could be transmitted with high probability by maintaining two cluster heads in each cluster. In addition, the probability of key share between the cluster head and member node is improved significantly as we maintain two cluster heads. Simulation was performed in terms of message delivery ratio to compare the performance of suggested algorithm with that of the previous method. When there are wireless link errors, the suggested algorithm shows higher message transmission ratio than that of the previous method by around 10%. But our algorithms consume slightly more energy than the previous works by maintain two cluster heads.

References

[1] I. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-114, 2002.

[2] Y. Liang and H. Yu, "Energy Adaptive Cluster-Head Selection for Wireless Sensor Networks," in *Proc. Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2005, pp. 634-638.

[3] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," *Lecture Notes in Computer Science*, vol. 740, pp. 471-486, 1993.

[4] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," presented at IEEE INFOCOM, 2004.

[5] L. Eschenauer and V. Gligor, "A key management scheme fordistributed sensor networks," in *Proc. the 9th ACM Conf. on Computer and Communications Security*, NewYork: ACM Press, pp. 41-47, 2002.

[6] S. Kim, "Reliable cluster-based routing algorithms in wireless sensor networks," *Applied Mechanics and Materials*, vol. 284-287, pp. 2147-2151, 2012.

[7] H. Chan, A. Perrig, and D.Song, "Random Keypredistribution schemes for sensor networks," *IEEE Symposium on Security and Privacy*, Berkeley, California, May 11-14, 2003, pp. 197-213.

[8] M. Li, S. Yu, D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Trans. Sen. Netw.*, vol. 9, no. 2, pp. 1-35, 2013.

[9] W. Du, J. Deng, Y. Shan, S. Chen, and P. Varshney, "A Key ManagementScheme for Wireless Sensor Networks Using DeploymentKnowledge," *INFOCOM 2004*, vol. 1, pp. 7-11 March 2004.

[10] W. Du *et al.*, "A pairwise key pre-distributionscheme for wireless sensor networks," in *Proc 10th ACM Conference on Computer and Communications Security (CCS)*, Washington, DC., 2003, pp. 42-51.

[11] D. Liu and P. Ning, "Establishing pairwise keys indistributed sensor networks," *ACM Transactions onInformation and System Security*, vol. 8, no. 1, pp. 41-77, 2005.

[12] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," *IEEE Symposium on Research in Security and Privacy*, 2003, pp. 197-213.

[13] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in *Proc. the Tenth ACM Conference on Computer and Communications Security (CCS 2003)*, 2003, pp. 42-51.

[14] D. Liu and P. Ning, "Location-based pair-wise key establishments forrelatively static sensor networks," in *Proc. ACM Workshop Security of Ad Hoc and Sensor Networks*, 2003.

[15] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensornetworks," in *Proc. the 9th ACM Conference on Computer and Communications Security*, 2003.

[16] L. B. Oliveira, H. C. Wong *et al*., "SecLEACH - A random key distribution solution for securing clustered sensor networks," in *Proc. Fifth IEEE International Symposium on Network Computing and Applications*, 2006, pp. 145-154.

Si-Gwan Kim received the B.S. degree in computer science from Kyungpook Nat'l University in 1982 and M.S. and Ph.D. degrees in computer science from KAIST, Korea, in 1984 and 2000, respectively. He worked for Samsung Electronics until 1988 and then joined the Department of Computer Software Engineering, Kumoh National Institute of Technology, Gumi, Korea, as a professor. His research interests include sensor networks, mobile programming and parallel processing.