ISSN (e): 2250 – 3005 || Vol, 05 || Issue, 01 || January – 2015 ||
International Journal of Computational Engineering Research (IJCER)

Random Key Pre-distribution Schemes using Multi-Path in Wireless Sensor Networks

Si-Gwan Kim
Kumoh Nat'l Institute of Technology, Korea

ABSTRACT:
Low-cost, small-size and low-power sensors that incorporate sensing, signal processing and wireless communication capabilities is becoming popular for the wireless sensor networks. Due to the limited resources and energy constraints, complex security algorithms applied to ad-hoc networks cannot be employed in sensor networks. In this paper, we propose a node-disjoint multi-path hexagon-based routing algorithm with a key pre-distribution scheme in wireless sensor networks. We describe the details of the algorithm and compare it with other works. Simulation results show that the proposed scheme achieves better performance in terms of security, efficiency and message delivery ratio.

Keywords: *key pre-distribution, multi-path, routing, security, wireless sensor networks*

I. INTRODUCTION

Wireless sensor network (WSN) is becoming popular in critical applications. Composed of tens and thousands of sensor nodes, sensor network can work in the environment to which human cannot easily approach. Security issue is very important for WSNs applications, such as military applications. 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. Because of resource limitations and secure applications in WSNs, key management emerges as a challenging issue for WSNs. In WSNs security, the key management problem is one of the most important issues.

Traditional schemes in ad hoc networks using asymmetric keys are expensive due to their storage and computation cost. These limitations make key pre-distribution schemes a good choice to provide low cost secure communication between sensor nodes [1-3]. The main drawback of key pre-distribution schemes is that the capture of a single sensor node allows adversary easily access to all keys stored in the node. This may not only lead to compromise of the links established by the captured node but also to compromise of links between two non-captured nodes, since these two nodes may have used one of the captured keys to secure their communication.

Establishing single-path routing between the source and destination nodes is more common study topics in WSNs. However, compromise of nodes along the path would lead to failure of the path and loss of data. Furthermore, if routing path is compromised then the entire WSN is endangered. In sensitive applications, establishing reliability and availability is very important for an application to serve its objectives successfully. To offer multiple paths in order to enhance the availability, resilience and reliability of the network, many studies suggest various mechanisms. However, the use of multiple paths introduces additional security problems, since it makes data available at more locations, giving more opportunities to adversaries to compromise the data. Therefore, in sensitive environments it is important to protect the network from malicious actions in order to enhance and maintain the availability and reliability of the network.

As most of the routing protocols in WSNs have not been designed with security requirements, secure routing protocols are studied recently [4-7]. The key management problem has been extensively studied in the WSNs. However, applying the public key management scheme used in the wired networks is impractical due to the resource constraints of sensor nodes. The key pre-distribution scheme using symmetric encryption techniques is another form of solution. Eschenauer and Gligor [3] 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. If no common key is found, they need to exchange a secret key via a multi-hop path.

The rest of the paper is organized as follows. In section 2, we introduce the related works. In section 3, we describe our multi-path routing algorithm. In section 4, simulation results are shown and compare our algorithm with previous works. Finally, we summarize our results in section 5.

II. RELATED WORKS

Key management involves various techniques that support the establishment and maintenance of key relationships between authorized parties [7][8][13]. An effective key management scheme is essential for the secure operations in wireless sensor networks. In recent years, key pre-distribution scheme has been widely studied. Many random key pre-distribution schemes have been suggested. Eschenauer and Gligor [3] proposed the basic probabilistic key pre-distribution, in which each sensor is assigned a random subset of keys from a key pool before the deployment of the network. In these techniques [3], a small number of keys are selected from a key pool and stored into a sensor before the deployment of the network. After deployment, two neighboring sensors can establish a secure single-hop path if they share a common key. Otherwise they need to exchange a secret key via a multi-hop path. Many subsequent schemes are mainly based on the improvement on the E-G scheme. For example, the random pairwise keys scheme [4] pre-distributes random pairwise keys between a particular sensor and a random subset of other sensors, and has the property that compromised sensors do not lead to the compromise of pairwise keys shared between non-compromised sensors. Chan proposes a q-composite random key pre-distribution scheme [9] to increase the network resilience at the cost of processing overhead. This allows neighbors to have a secure communication only when they share at least q > 1 common keys. This scheme can efficiently improve the resilience against node capture attack, in which attackers can capture sensors and derive the preinstalled information still used by uncompromised nodes. In [12], combinatorial properties of the set systems are used to distribute keys to sensors prior to deployment, which improves connectivity of two neighboring sensors when the network size is large.

Path key establishment is widely used in key pre-distribution schemes. Establishing keys between two neighbor nodes without pre-installed common keys through a secure path must be solved. The key called path key is transmitted using secure communication channel through several intermediate nodes. However, if one of the nodes along the path is compromised, the key may be exposed. To solve this problem, some multipath key establishment schemes [8, 9] were proposed. These schemes can effectively stop revealing the key, but they have some drawbacks in forward attacks.

Shamir's secret sharing [11] based path key establishment mechanism is proposed to improve the security of path key establishment. Path key is treated as a secret need to share, which will be divided into several key segments. The key segments will be transmitted through a node-disjoint path respectively. Whenever the network encounter the stop forwarding attacks, the destination node can reconstruct the path key so long as the received key segments are no less than the threshold set in the scheme.

Some multi-path key establishment schemes were studied to solve the path key exposure problem [13]. The basic idea behind multi-path key establishment schemes is first studied by Perrig [14]. In [8], multiple node-disjoint paths were used for the end to end pairwise key establishment. In this scheme, the path key will be divided into n parts and each part is transmitted on a node-disjoint paths. When the destination node receives all the n parts of the key, it can reconstruct the path key. Another path key establishment scheme [9] use multiple one-hop paths instead of node-disjoint paths to enhance the security of path-key establishment. But if the captured node is on the intersect point of several paths between these proxies and drops all the key shares passing through it [10], the entire system is endangered.

After the completion of the shared-key discovery phase, many direct links are protected by a same key K_i, which may be known by many nodes in the network. Thus, the capture of a single node chain will compromise all those links. These problems are studied in multi-path key establishment schemes [14][15]. In these schemes, the source sensor node finds a multi-hop secure path toward the destination node. Each pair of neighboring nodes on the secure path shares at least one common key, which could be different along the path. Then a secret key is generated by the source node and sent toward the destination through the multi-hop secure path. This scheme works quite well when no nodes on the path are compromised and all sensor nodes forward the secret key honestly. But, these sensor nodes are susceptible to many kinds of attacks, such as eavesdropping, stop forwarding and distorting.

In [15], Huang and Mehdi propose a multiple key establishment scheme based on error-correct coding scheme. This scheme is resilient to $t = (n - k) / 2$ faulty paths with the use of the (n, k) RS codes. But it uses too more redundancy of parity code. Deng and Han [12] decrease the transmission overhead than [15] by sending redundant symbols when necessary.

In ad hoc networks, multi-path routing algorithms are based on the flooding mechanism, and need the centralized processing at the destination node. This flooding mechanism is not appropriate for large-scale sensor networks. Ye et al [10] presented a multi-path algorithm for sensor networks. But, the multi-path is not node-disjoint, and the flooding mechanism is be used. D. Ganesan et al [16] evaluated the relative performance of disjoint and braided multi-paths in sensor networks, but concrete multi-path algorithms are not presented.

III. OUR ALGORITHMS

In this section, we propose our algorithms based on multi-path routes. In our system, we use hexagon-based coordinates as well as grid-based ones. A hexagon-based coordinate system has more advantages over a grid-based one in wireless sensor networks. First, when a sensor node transmits data over wireless links, its signal range would form a circle that is centered around its deployment location with the radius being the distance of signal propagation. And, a hexagon can be used to describe equal distance between two neighboring sensor nodes. In a grid-based coordinate system, the distance between two neighboring sensor nodes differs. When the neighboring node is located directly adjacent or diagonally in the grid-based system, its distance is one unit and square root of two units, respectively.

In our systems, nodes are place in the grid form *n* x *n* as in Fig. 1. We assume that transmission range is two hops for each node. So the number of neighbor nodes within transmission range for each node is 16. Nodes within transmission range for node S is shown in black nodes in Fig. 1. Label of each node is numbered using two dimensional matrixes.

$\{N(i,j) \mid i=0,1,2,\ \dots,\ n-1,\ j=0,1,2,\ \dots,\ n-1\}$
, where, *n* is the size of the network.

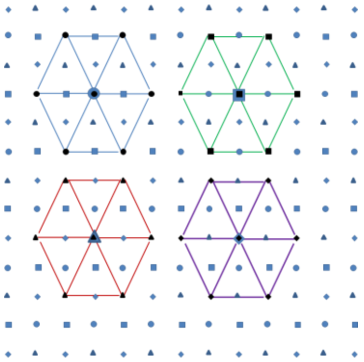


Figure 1. Example of source nodes

Four overlapping networks, G_0, G_1, G_2 and G_3, can be organized using the hexagon-based scheme as follows.

- $G_0 = \{N(i,j) \mid i=0,2,4,\ \dots,\ 2m-2,\ j=0,2,4,\ \dots,\ 2m-2\}$
- $G_1 = \{N(i,j) \mid i=0,2,4,\ \dots,\ 2m-2,\ j=1,3,7,\ \dots,\ 2m-1\}$
- $G_2 = \{N(i,j) \mid i=1,3,7,\ \dots,\ 2m-1,\ j=0,2,4,\ \dots,\ 2m-2\}$
- $G_3 = \{N(i,j) \mid i=1,3,7,\ \dots,\ 2m-1,\ j=1,3,5,\ \dots,\ 2m-1\}$

A node can be identified as a member of G_0, G_1, G_2 and G_3 according to the following rules.

- *i* and *j* value of node *N(i,j)* are all even numbers : a member node of G_0
- *i* and *j* value of node *N(i,j)* are even and odd number, respectively : a member node of G_1
- *i* and *j* value of node *N(i,j)* are odd and even number, respectively : a member node of G_2
- *i* and *j* value of node *N(i,j)* are all odd numbers : a member node of G_3

In Fig. 1, example source nodes of four networks are shown. An example member node in G_0, G_1, G_2 and G_3 is drawn as circle, rectangle, triangle and diamond, respectively. In this figure, an example of hexagon-based routing path is shown for each G_0, G_1, G_2 and G_3, with each source node drawn as big circle, big rectangle, big triangle and big diamond, respectively.

Our scheme has two kinds of hops, one-hop delivery and two-hop delivery. Hexagon-based two-hop delivery is used for the routing where a destination node is more than three hops away. On the other hand, one-hop delivery is used for the distribution of message segments to the neighbor nodes, or final hop of the segments to the destination node. This one-hop is routed using grid-based coordinates.

When a node wants to send some messages to the destination node, we first check the number of nodes (denoted as c) which shares keys with the two-hop range neighbor nodes. Then given message is divided into c segments, i.e. w_0, w_1, …, and w_{c-1}. Each segment except w_0 is delivered to c neighboring nodes. This delivery takes just one hop for each segment. Then each segment is routed to the destination node. This routing is hexagon-based coordinate system and uses two-hop delivery. Fig. 2 shows our routing algorithms.

Step 1. By transmitting hello packets to two-hop range nodes, find the number of nodes (denoted as c) which shares keys with neighbor nodes. Then a given message is divided into c segments, i.e. w_0, w_1, w_2, … , w_{c-1}.

Step 2. Each segment w_i is delivered to its corresponding key sharing node (S_i), which is one-hop or two-hop away neighbor node.

Step 3. When each segment w_i is arrived in the node Si, each segment decides its corresponding G_i (i=0,1,2,3).

Step 4. Each segment is forwarded to the destination node based on hexagon-based routing.

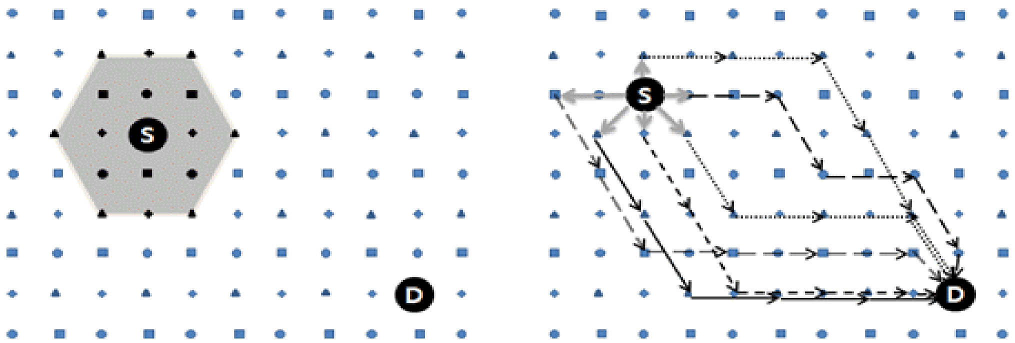
Step 5. When each segment is arrived at the intermediate node, each segment is routed to the next intermediate node according to the pre-determined G_i.

Step 6. As each segment gets closer to the destination node, the last hop may be one-hop or two-hop routing for the destination node depending on the position of that node.

Step 7. After receiving all the segments in the destination node, original messages can be constructed.

Figure 2. Outline of the proposed routing algorithms

Fig. 3 shows an example of our routing. In this example, source node 'S' has some messages for the destination node 'D'. Node S tries to find the neighbor nodes that share the key within two-hop distance. There can be sixteen nodes within two-hop distance. This is shown in Fig. 3(a). Assume the source node found that six neighbor nodes share the key. This is shown in Fig. 3(b). So it divides a message into six segments, and these six segments are forwarded to the neighbor nodes using one-hop or two-hop routing. These six segments are ready to be routed to the destination node using two-hop routing. For the two-hop routing, nodes that share the key are found among two-hop distant neighbor G_i nodes. As two-hop routing is based on the hexagon system, the maximum number of nodes that share the key is six. Among these six nodes, only one node that shares the key is needed for further routings. After finding the node that share the key, current segment message is routed to that node. The final hop to the destination node D may use one-hop delivery. This is shown in Fig. 3(b)



(a) Finding key share **(b) Routing**

Figure 3. Example routing

IV. SIMULATIONS

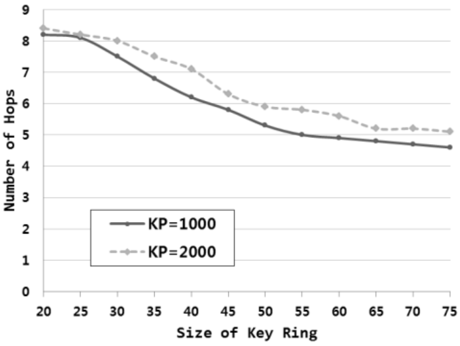
The performance of suggested algorithm is simulated and analyzed in this section. NS-2 is used to perform simulation to compare and analyze performance with the previous works. Performance metrics are message delivery ratio, the quantity of received data in comparison with the consumed energy and overhead of cluster composition. The size of network is 100m × 100m 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. We have performed three simulations to evaluate our protocols as follows.

4.1. Number of hops to reach the destination node for each node

We measured the average number of hops to reach the destination node for each node. As the message for a given node is routed to the intermediate nodes, the number of neighboring node that shares the key is very important. The more the number of key sharing nodes, the less the number of hops to reach the destination node. Fig. 4 shows the results of our algorithms. As the number of key pool(KP) is increased, the number of hops is decreased by about 1 hop. The size of key ring affects the number of hops too. As the number of key ring is increased, the number of hops to reach the destination is decreased by about 2.5 hops.

4.2. Number of available multi-path for a node

The number of multi-path for each node is one of the important factors that affect the performance of the networks. For a given node, the number of neighbor node for two-hop range is 16, which is the maximum number of multi-path. But key-sharing between the neighbors nodes may not be existed, the number of key-sharing is less than this number. We measured the average number of multi-path for a given node. Fig. 5 shows the results. As the number of key pool is increased from 1000 to 2000, the number of multi-path is by about 2. And if we vary the size of key ring, the number of multi-path is increased up to 13(KP=2000).



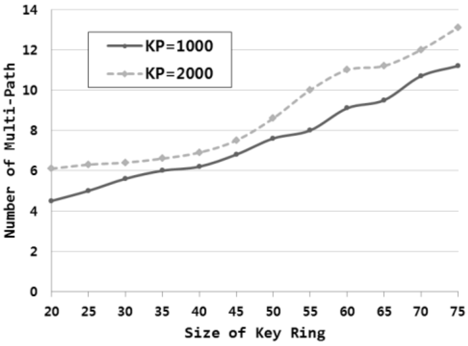


Figure 4. Number of hops

Figure 5. Number of available multi-path

4.3. Message Delivery Ratio

Message delivery ratio of member node to sink was simulated. Packet delivery ratio is the percentage of packets sent by the source which reaches the sink depending on the number of source nodes. 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. 6, Fig. 7 and Fig. 8 show message delivery ratio when the number of message for each node is 20, 40 and 60 and the suggested algorithm was found to have the transmission ratio higher than that of SecLEACH [17] algorithm by about 4%. 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.

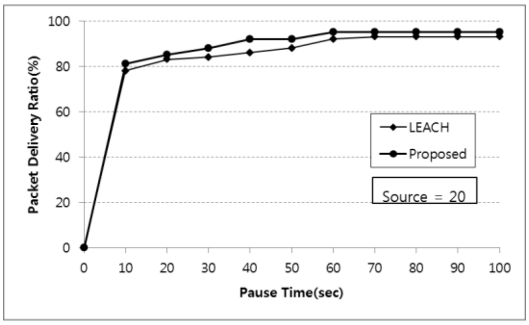


Figure 6. Message Delivery Ratio (sources=20)

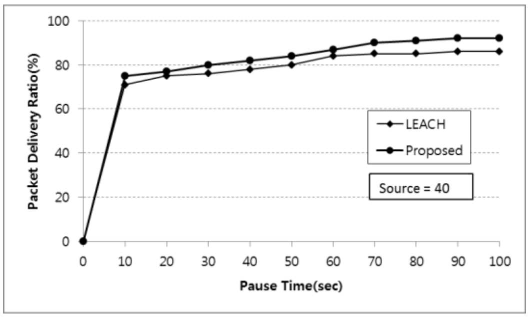


Figure 7. Message Delivery Ratio (sources=40)

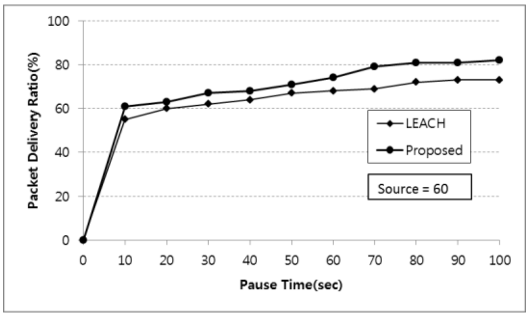


Figure 8. Message Delivery Ratio (sources=60)

V. CONCLUSIONS

Sensor network is limited by the energy resources of sensor node that composes network, computation ability and the memory capacity. This paper suggests key pre-distribution routing algorithm based on multi-path routes in sensor network. Simulation was performed in terms of number of multi-path, average number of hops to reach the destination node and message delivery ratio to compare the performance of suggested algorithm with that of the previous method. Due to the more routing paths, the suggested algorithm shows higher message delivery ratio than that of the existing method by some 4%.

ACKNOWLEDGEMENTS

This work was supported by Kumoh National Institute of Technology, Korea.

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

[3] L. Eschenauer and V. Gligor, “A key management scheme for distributed sensor networks,” in Proc. of the 9th ACM Conf. on Computer and Communications Security, New York: ACM Press, pp. 41-47, 2002.

[4] H. Chan, A. Perrig, and D. Song, “Random Key predistribution schemes for sensor networks”, in IEEE Symposium on Security and privacy, Berkeley, California, May 11-14, 2003, pp. 197-213.

[5] 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. 9, 2, pp. 1-35, 2013.

[6] W. Du, J. Deng, Y. Shan, S. Chen, and P. Varshney, “A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge,” in INFOCOM 2004, Volume 1, 7-11 March, 2004.

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

[8] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks,” ACM Transactions on Information and System Security, Volume 8(1), pp.41-77, 2005.

[9] [y2] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in IEEE Symposium on Research in Security and Privacy, 2003, pp. 197-213.

[10] Ye Ming Lu and Vincent W. S. Wong. 2007. An energy-efficient multipath routing protocol for wireless sensor networks: Research Articles. Int. J. Commun. Syst. 20, 7 (July 2007), 747-766.

[11] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to Leak a Secret. In Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '01), Colin Boyd (Ed.). Springer-Verlag, London, UK, UK, 552-565, 2001.

[12] J. Deng, R. Han, S. Mishra. Limiting DoS Attacks During Multihop Data Delivery In Wireless Sensor Networks. International Journal of Security and Networks, Special Issue on Security Issues in Sensor Networks, vol. 1, nos. 3/4, 2006, pp. 167-176.

[13] Stavrou, Eliana, and Andreas Pitsillides. "A survey on secure multipath routing protocols in WSNs." Computer Networks 54.13 (2010): 2215-2238.

[14] Xin Zhang and Adrian Perrig, "Correlation-Resilient Path Selection in Multi-Path Routing." In Proceedings of the IEEE Global Communications Conference (Globecom), December 2010.

[15] D. Huang and Deep Medhi, “A Byzantine Resilient Multi-Path Key Establishment Scheme and Its Robustness Analysis for Sensor Networks,” in Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS), 2005, pp. 4-8.

[16] Deepak Ganesan, Ramesh Govindan, Scott Shenker, and Deborah Estrin. 2001. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. SIGMOBILE Mob. Comput. Commun. Rev. 5, 4 (October 2001), 11-25.

[17] Leonardo B. Oliveira, Adrian Ferreira, Marco A. Vilaça, Hao Chi Wong, Marshall Bern, Ricardo Dahab, Antonio A.F. Loureiro, SecLEACH—On the security of clustered sensor networks, Signal Processing, Volume 87, Issue 12, December 2007.