International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:2, No:2, 2008

Adaptive Hierarchical Key Structure Generation for Key Management in Wireless Sensor Networks using A*

Jin Myoung Kim, and Tae Ho Cho

***Abstract*—**Wireless Sensor networks have a wide spectrum of civil and military applications that call for secure communication such as the terrorist tracking, target surveillance in hostile environments. For the secure communication in these application areas, we propose a method for generating a hierarchical key structure for the efficient group key management. In this paper, we apply A* algorithm in generating a hierarchical key structure by considering the history data of the ratio of addition and eviction of sensor nodes in a location where sensor nodes are deployed. Thus generated key tree structure provides an efficient way of managing the group key in terms of energy consumption when addition and eviction event occurs. A* algorithm tries to minimize the number of messages needed for group key management by the history data. The experimentation with the tree shows efficiency of the proposed method.

***Keywords*—**Heuristic search, Key management, Security, Sensor network.

I. Introduction

WIRELESS sensor networks (WSNs) have emerged as an innovative class of networked embedded systems due to the union of ever smaller, less costly embedded processor and wireless interfaced with micro-sensors based on micro-mechanical systems (MEMS) technology [1][2]. WSNs are composed of small autonomous devices, or sensor nodes, that are networked together [3][4]. The applications of WSNs widely range from the indoor applications like smart home, health monitoring in a hospital to outdoor applications like highway traffic monitoring, combat field surveillance, security and disaster management [5].

Some of the most important outdoor applications like military surveillance, enemy ship movements and terrorist threats tracking need to keep the privacy and security issues [6][7]. However, the sensor networks are highly vulnerable to security attack since the individual sensor nodes are anonymous and that communication among sensors is made via wireless links [8][9]. One way to implement secure wireless communication in WSNs is through the use of a message encryption [3]. Sensor nodes in the network share a secret encryption key(s) for encrypting messages exchanged among sensor nodes.

The sensor nodes are evicted from the network if sensor nodes are compromised and exhibit malicious behavior in the network [10]. When this eviction occurs, all the keys known to the sensor node must be changed and the new keys must be securely delivered to the remaining sensor nods in order to prevent the evicted node from forging false messages. When the addition of the sensor nodes occurs due to reorganizing the network or complementing more nodes, it is necessary to update all known keys so that newly added nodes cannot understand encrypted messages formed by the current keys [3][7]. This key update is typically accomplished by broadcasting encrypted messages, called re-key messages, containing the new key(s).

In this paper we apply A* algorithm, that exploits a history data of an addition and eviction ratio of a location where sensor node is deployed, in order to generate a hierarchical key structure for the efficient group key management. Thus generated key structure tries to minimize the number of message transmissions needed in the re-key messages. Generally, when a sensor transmits a 1 bit data, an energy consumption of sensor is higher than a computation [11]. The experiment is performed against the logical key hierarchy (LKH) [12]. The result shows that the proposed method is more efficient in terms of energy consumption when addition and eviction event occurs.

This paper is organized follow. Section II describes routing protocols and the key management in WSN, and section III reviews the tree based key management, a re-key scheme and A* algorithm. In section IV, we present a sensor network structure and A* based key tree structure. Section V shows an experiment of our proposed method. Finally, section VI gives a conclusion and future works.

II. Related Works

In WSNs, there are many types of routing protocols. These protocols require a key management for ensuring the security. The key management procedure is an essential constituent of network security. The following subsections present routing protocols and key management in WSNs.

Manuscript received June 30, 2006. 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).

Jin Myoung Kim is with the School of Information and Communication Engineering, Sungkyunkwan University, Suwon, Gyeonggi-do 440-746, Korea (e-mail: kjm77@ece.skku.ac.kr).

Tae Ho Cho is with the School of Information and Communication Engineering, Sungkyunkwan University, Suwon, Gyeonggi-do 440-746, Korea (corresponding author to provide phone: +82-31-290-7221; fax: +82-31-290-7230; e-mail: taecho@ece.skku.ac.kr).

A. Routing Protocols in WSN

In general, routing in WSNs can be classified into three types. These are flat-based routing, clustering-based routing, and direct communication-based routing. In flat-based routing the roles of all nodes are identical, whereas, that of clustering-based routing are different in that the message transmission from the nodes are done through the cluster head. In direct communication-based routing, a sensor node sends data directly to the Base Station (BS) [13][14]. Under this protocol, if the diameter of the network is large, the power of sensor nodes will be drained very quickly. Under flat protocols, when a node needs to send data, it may find a route consisting of several hops to the BS [13]. Clustering-based routing is an efficient way to lower energy consumption within a cluster, performing data aggregation and fusion in order to decrease the number of transmitted messages to the BS [14].

B. Key management in WSNs

To secure WSNs against malicious access, the various keys are needed to encrypt and authenticate the control messages and sensed data. Due to the limited resource of sensor nodes, it is not practical to use asymmetric cryptosystems in WSNs [15]. Therefore, the symmetric key management is mostly adopted in WSNs. LEAP [16] is a key management protocols for sensor networks. It establishes four types of keys for each sensor node. Di Pitro et al. enhance the logical key hierarchy to create a directed diffusion based logical key hierarchy. The logical key hierarchy technique provides mechanisms for nodes joining and leaving groups where the key hierarchy is used to effectively re-key all nodes within the leaving nodes's hierarchy [1]. The logical key hierarchy technique is exploited for the key management within the proposed approach

III. Background

In WSNs, there are many types of key managements. Among them the hierarchical tree based key management provides an efficient re-key mechanism for the addition and eviction. The A* algorithm is exploited for the generation of the hierarchical key tree structure with which efficient key management can be done.

A. Tree based Key Management and Re-keying Scheme

Wallner et. al. proposes a hierarchical keying method called Logical Key Hierarchy (LKH). In the LKH, the key distribution center (KDC) maintains a key tree which will be used for group key update and distribution.

Each internal node in the tree represents a cryptographic symmetric key. The center associates each group member with one terminal node of the tree. Each terminal node knows all the keys from its leaf node up to the root. In the sensor network, the hierarchical technique can be applied in support of other keying protocols such as pre-deployed keying to provide a mechanism to maintain freshness of the shared deployed cryptographic keys [9][14]. In Fig. 1, a cryptographic symmetric keys, e.g. GK, SGK_1, … , SGK_4, SN_1,…,SN_4, are logically distributed in a tree at the KDC.

In [17], Wang et. al. shows a group key management and re-key scheme using key graph. The re-key scheme of our proposal is based on Wang et al's key-oriented re-keying scheme.

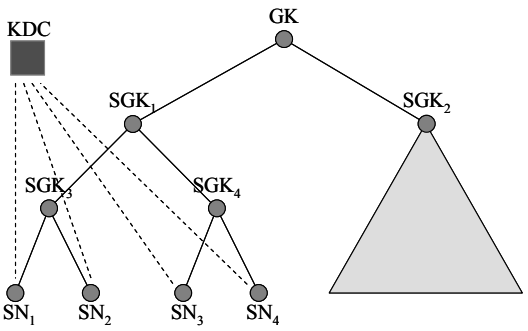

Fig. 1 Logical Key Hierarchy

B. A* algorithm

A* algorithm that is a kind of tree search method uses a heuristic evaluation function [18]. A heuristic evaluation function helps decide which node is the best one to expand next.

Let $h(n)$ is the actual cost of the minimal cost path between node n and a goal node and let $g(n)$ is the cost of a minimal cost path from the start node, n_0, to node n. Then equation is the cost of a minimal cost path from n_0 to a goal node over all paths that are constrained to go through node n.

For each node n, let heuristic factor $h^*(n)$ be some estimate of $h(n)$, and let depth factor $g^*(n)$ be the cost of the lowest-cost path found by A* so far to node n. The estimate of heuristic evaluation is defined:

$$f^*(n) = g^*(n) + h^*(n) \quad (1)$$

In algorithm A* we use equation (1).

IV. A* For Key Tree Structure Generation

In cluster based WSNs, the network is typically organized into clusters, with ordinary cluster members and cluster heads (CHs) playing different roles. For ensuring the security in this organization the tree based key management is used and the key tree structure for the efficient management is generated by applying A* algorithm.

A. Sensor Network Structure

The sensor network is composed of a base station (BS), sensor nodes and cluster heads (CHs) as shown in Fig. 2. CHs have more energy and computation ability than sensor nodes. Those are responsible for data collection and transmission. Also they form a cluster. Clusters can be formed based on many criteria such as communication range, number and type of sensors and geographical location [19]. Every cluster has only one CH. The information gathered from the sensor nodes within a cluster is sent to CH and then it is send to BS [20].

The BS works as the KDC. When sensor nodes makes request of the addition/eviction to CH then the CH notifies BS

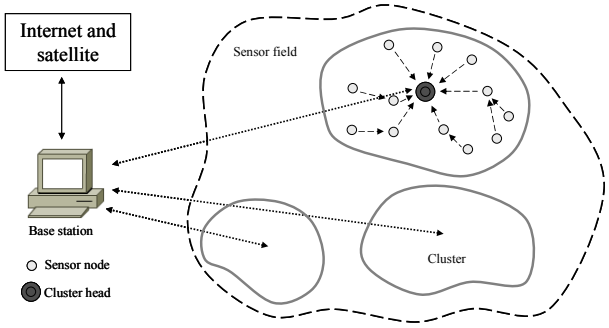

Fig. 2 Sensor Network Structure

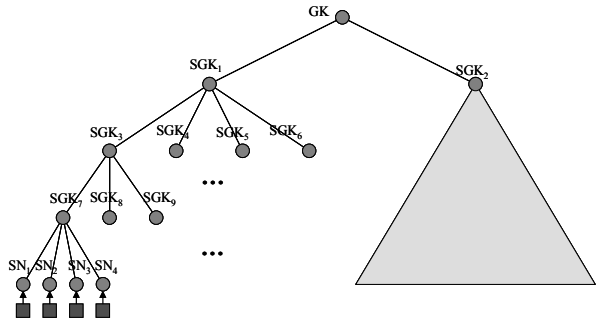

Fig. 3 Proposed A* based key tree structure

to generate and send a new group key(s) to all the sensor nodes (in cluster).

And the new keys are distributed to each sensor node through the CH. The security issue that the current research is concerned with belongs to the message transmissions among CH and sensor nodes in a cluster.

B. A based Key Tree Structure*

In order to reduce the number of re-key messages the branching factor can be different for each level of the proposed A* based tree structure generated for the key management. The collection of the branching factors is represented by *vT* as the sequence below.

$$vT = \{d_0, d_1, ..., d_{h-1}\}$$

In *vT*, d_h represents the branching factor at level *h* of the tree. The branching of the nodes at a particular level is identical, i.e., the branching factor for all the nodes at level 1 is d_1. Also, the elements in *vT* satisfies the following condition.

$$d_0 \cdot d_1 \cdot ... \cdot d_{h-1} = \prod d_i \geq ns \quad where \quad ns : \text{number of sensor snodes} \tag{2}$$

In equation (2), since the terminal nodes of the tree corresponds to the sensor nodes actually deployed in a cluster, the number of the terminal nodes should be greater than or equal to the number of the deployed nodes so that every deployed node can be represented by the terminal nodes used in logical key management.

Fig. 3 shows an example of our proposed key tree structure. In the figure, a circle corresponds to keys and squares correspond to sensor nodes. This structure can be represented in *vT*= {2, 4, 3, 4} which includes 128 sensor nodes.

Above, the addition of sensor and eviction of sensor node denotes the join and leave event respectively.

In [17], when the join/leave event occurs in a cluster, the number of re-key messages by means of key-oriented re-keying scheme is calculated as following equation.

$$\begin{aligned} Join\_MSG &= h \\ Leave\_MSG &= (d-1)(h-1) \end{aligned} \tag{3}$$

In equation (3), *Join_MSG* is the number of re-key messages in join and *Leave_MSG* is the number of re-key messages in leave. *h* is height of the tree which is defined in [17]. And *d* is branching factor in the tree.

When the join/leave event occurs in a cluster, the number of re-key messages needed for the key tree defined by *vT* is calculated as following equations.

$$\begin{aligned} Join\_MSG &= h \\ Leave\_MSG &= \sum d_i - (h-1) \end{aligned} \tag{4}$$

If the join events occur with a ratio of α and the leave events occur with a ratio of $1-\alpha$ then the number of re-key messages *M* in the network is defined as:

$$\begin{aligned} M &= \alpha \cdot Join\_MSG + (1-\alpha) \cdot Leave\_MSG \\ &= \alpha \cdot h + (1-\alpha) \cdot \left\{ \sum_{i=0}^{h-1} d_i - (h-1) \right\} \end{aligned} \tag{5}$$

We assume that α is available for a cluster of sensor nodes. The A* algorithm is applied in finding a degree sequence $\{d_0, d_1, \ldots, d_{h-1}\}$ which minimizes *M*, the number of re-key messages needed.

C. Heuristic Evaluation Function

The history data for the join/leave event of the sensor nodes is different from a cluster to cluster where the sensor nodes are placed. Based on the history data a key structure suitable for the efficient key management is generated with the application of A* algorithm.

In the tree defined by *vT*, $g^*(n_c)$ for an arbitrary node n_c is defined as:

$$g^*(n_c) = \alpha \cdot h_c + (1-\alpha) \cdot \{\sum_{i=0}^{c} d_i - (h_c - 1)\} \quad (6)$$

The evaluation function $g^*(n_c)$ returns the number of re-key messages needed when the join/leave event occurs and h_c is a height of key tree structure. α and d_i are explained section IV-B.

As described by equation (4), the number of re-key messages is minimum when the height of the key tree is minimum. And when the leave event occurs, we knew that a height of the tree vT is maximum and a sum of degree of tree vT is minimum then the number of re-key messages is minimum. So estimate of heuristic factor is defined as:

$$h^*(n_c) = \alpha \cdot \min\_Join\_MSG + (1-\alpha) \cdot \min\_Leave\_MSG \quad (7)$$

Equation (7) calculates the minimum number of expected re-key messages when the join/leave event occurs. The first term and second term in the equation represent the number re-key messages for the join event and that of leave event, respectively. As shown in equation (4) *min_Join_MSG* becomes minimum when the height of the tree is minimum. Thus, *min_Join_MSG* is 1. *min_Leave_MSG* becomes minimum when the height of the key tree is maximum and the sum of d_i is minimum.

$$h^*(n_c) = \alpha + (1-\alpha) \cdot (k-1) \quad (8)$$

Both the maximum height of the tree and minimum d_i are obtained when the key tree is structured as a binary tree. So, the $h^*(n_c)$ can be calculated according to equation (4) as shown in equation (8). Where, k is the height of the binary tree that is calculated as shown below.

From equation (2),

$$d_0 \cdot d_1 \cdots d_c \cdot 2^k \geq ns$$

$$\Leftrightarrow 2^k \geq \left\lceil \frac{ns}{d_0 \cdot d_1 \cdots d_c} \right\rceil$$

$$\Leftrightarrow \log_2 2^k \geq \left\lceil \log_2 \left(\frac{ns}{d_0 \cdot d_1 \cdots d_c}\right) \right\rceil$$

$$\Leftrightarrow k \geq \left\lceil \log_2 \left(\frac{sn}{d_0 \cdot d_1 \cdots d_c}\right) \right\rceil.$$

V. Experimental Result

The experiment is performed under the various history data of leave/join events or history α value. We assume that the maximum number of sensor nodes and minimum number of sensor nodes in the cluster is 120 and 20 respectively and measures the number of messages required for the proposed A* based tree against the ternary tree and binary tree. Our proposed key tree structure for various α are constructed to measure the number of average re-key messages to show how effective the proposed method is.

Fig. 4 shows that the A* based tree needs the number of key-messages less than ($0.5 \leq \alpha \leq 1$) or equal to ($0 \leq \alpha \leq 0.5$) other

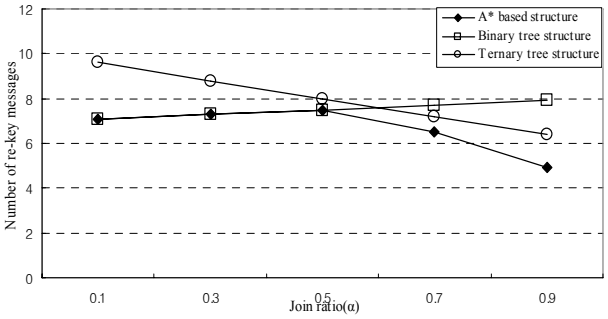

Fig. 4 The number of average re-key messages for the various history data (a) when the number of sensor node is 120 in the cluster

key tree structures when the number of sensor nodes is 120 in the cluster.

Also, Fig. 5 shows that our proposed key tree structure needs the number of re-key messages less than other key tree

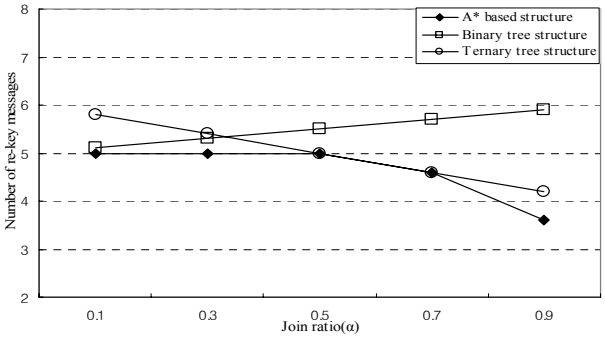

Fig. 5 The number of average re-key messages for the various history data (a) when the number of sensor node is 20 in the cluster

structure.

Accordingly, the experiment result shows that the A* based key structure needs the average number of re-key message less or equal to other key tree structures.

VI. Conclusion

In the various application WSNs enable the monitoring of the target system or area. Especially in the areas such as military, commercial, and privacy applications ensuring security is the important issue. In this paper, we showed how a hierarchical key tree can be generated by exploiting A* algorithm that considers the addition and eviction history data of the target cluster region. Thus generated key tree is effective, when frequent addition and eviction occurs, in that the number of re-key messages for managing the key system is reduced

compared to the existing key tree structures. Future works will reinforce the proposed method by considering the re-key message update cycles. It will also consider the storage issue in managing the hierarchical key structure.

REFERENCES

[1] Pietro, R. D., Mancini, L.V., Jajodia, S., "Providing secrecy in key management protocols for large wireless sensors networks," AdHoc Network 1 (2003) 455-468
[2] Lin Yuan, Gang Qu., "Design Space Exploration for Energy Efficient Secure Sensor Network," IEEE ASAP (2002) 88-97.
[3] Mohamed Eltoweissy, Ashraf Wadaa, Stephan Olariu, Larry Wilson, "Group Key management scheme for large-scale sensor networks," Ad Hoc Network 3 (2005) 668-688.
[4] Laurent Eschenauer, Virgil Gligor, D., "A Key Management Scheme for Distributed Sensor Networks," CCS'02 (2002).
[5] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E., "A Suvey on Sensor Networks," IEEE Communications Magazine 40 (2002) 102-114.
[6] Prasan Kumar Sahoo, Jonathan Jen-Ron Chen, Ping-Tai Sun., "Efficient Security Mechanisms for the Distributed Wireless Sensor Networks," ICITA'50 (2005).
[7] Mohamed Eltoweissy, Mohamed Younis, Kajaldeep Ghumman, "Lightweight Key Management for Wireless Sensor Networks," IEEE International Conference Performance on Computing, and Communications (2004) 813-818.
[8] Carman, D., Kruus, P., Matt, B., "Constraints and approaches for distributed sensor networks security," NAI Technical Report (2000).
[9] Jolly, G., Kuscu, M., Kokate, P., "A hierarchical key management method for low-energy wireless sensor networks," UMBC Online Document. (2002).
[10] Chan, H., Perrig, A., Song, D., "Random key pre-distribution schemes for sensor networks," IEEE 2003 Symposium on Security and Privacy (2003).
[11] Pottie, G. J., Kaiser, W. J., "Wireless Integrated Network Sensors," Communications of the ACM 43 (2000) 51-58.
[12] Wallner, D., Harder, E., Agee, R., "Key management for multicast: Issues and architectures," IETF (1999) RFC 2627.
[13] Jiang, Q., Manivannan, D., "Routing protocols for sensor networks," CCNC (2004) 93 – 98.
[14] Al-Karaki, J.N., Kamal, A.E., "Routing techniques in wireless sensor networks: a survey," Wireless Communications Vol. 11 (2004).
[15] Chien-Chung Su, Ko-Ming Chang, Yau-Hwang Kuo, Mong-Fong Horng, "The new Intrusion Prevention and Detection Approaches for Clustering-based Sensor Network," WCNC (2005) 1927-1932.
[16] Zhu, S., Setia, S., Jajodia, S., "LEAP: efficient security mechanisms for large-scale distributed sensor networks," ACM CCS (2003) 27-31.
[17] Wong, C., Gouda, M., Lam, S., "Secure group communications using key graphs," IEEE/ACM Transactions on Networking 8 (2000) 16–30.
[18] Nils J. Nilsson., "Artificial Intelligence: A new synthesis," Morgan Kaufmann Publishers (1998).
[19] Lin, C., Gerla, M., "Adaptive clustering for mobile wireless networks," Journal on Selected Areas of Communication Vol.15 (1997).
[20] Younis, M., Youssef, M., Arisha K., "Energy-Aware Routing in Cluster-Based Sensor Networks," MASCTS (2002) 129-136.