A Security Strategy Based on Multi-Dimension Location for Hierarchical Wireless Heterogeneous Sensor Networks

Yuquan Zhang[1,a], Lei Wei[2,b]

[1]Wireless Sensing Institute, College of Information Science and Engineering, Qilu Normal University, China

[2]College of Physics and Electronic Engineering, Qilu Normal University, China

[a]email:zyczyq@126.com; [b]email:weilei76@126.com

Keywords: Hierarchical wireless heterogeneous sensor network, two-layer, multi-dimension, security, connectivity, lifetime

Abstract. A key management scheme based on multi-dimension location is presented for heterogeneous wireless hierarchical sensor networks. The wireless sensor networks consist of some nodes that have greater power and transmission capability than other sensor nodes. All kinds of nodes are deployed evenly in sensing multi-dimensional hypercube respectively. The sensing hypercube is divided into a number of small same hypercubes for all kinds of nodes and then some of those small same hypercubes consist of a logical group for those heterogeneous nodes. The wireless sensor network has a two-tier structure. The upper layer consists of all cluster heads, namely heterogeneous sensor nodes and the lower layer consists of all ordinary sensors managed by their corresponding cluster heads. This paper investigates how the heterogeneous sensor nodes enhance the performance of wireless sensor networks. Pairwise keys are established between all kinds of nodes through employing the concept of the overlap key sharing and the random key predistribution scheme. Analysis shows the heterogeneous nodes improve the security and connectivity for wireless sensor networks, moreover, they extend the network lifetime.

Introduction

Wireless sensor networks have accepted great attention. Wireless sensor networks comprise numerous sensors dispensed in environments for various purposes[1]. Those WSNs application fields include agriculture, industry, etc[2].

Wireless sensor networks have several architectures including hierarchical architecture, heterogeneous architecture, etc. In hierarchical wireless sensor networks, some powerful nodes can act as the key servers. In heterogeneous wireless sensor networks there are some different kinds of sensors which have different capacities such as communication ability, computing ability, etc[3][4]. Those wireless sensor networks are distributed in antagonistic environment some times, therefore they are easily attacked by opponents.

Key management is an efficient method to ensure WSNs secure. Lai D et al.[5] gave the Overlap-Key-Sharing (OKS) protocol. The protocol generates a bit-string, namely the key-string-pool (KP) of the sensor network, and at random assigns a subset of KP which is stored in each sensor. Sensors utilize the number of bits overlapping between neighbors of the key-strings as the shared secret key with their neighbor nodes.

This paper gives a pairwise key establishment strategy for HWHSNs(heterogeneous wireless hierarchical sensor networks)through exploring how heterogeneous sensor nodes enhance the network performance. The n_d -dimension sensing space is partitioned into many small same hyper-cubes, namely cells, and then 2^{n_d} cells comprise a cluster, namely logical group. All nodes are deployed evenly in sensing space. HWHSNs have a two-tier structure. The upper tier comprises all cluster heads and the lower tier comprises of ordinary sensors. The overlap key sharing protocol creates bit clusters as the key cluster pools and distributes a sub-group to every sensor as key cluster. Pair-wise keys are established between all kinds of nodes by using the concept of the overlap key sharing and the random key pre-distribution scheme. We can prove this scheme enhances the

networks resilience, has good network connectivity and enlarges the network lifetime.

The rest of this paper is organized as the following. In section two, the HWHSNs key scheme is given. HWHSNs performance analysis is given in the section three. The conclusion of this paper is in section four.

Hierarchical Key Management Scheme

This paper presents a key management strategy based on multi-dimension clusters for hierarchical wireless heterogeneous sensor networks. This scheme is a two-layer dynamic key management strategy, which contains the base station, the cluster heads, and the ordinary sensor nodes. The upper layer consists of all cluster heads, namely class 1 sensor nodes, and the lower layer consists of all normal sensors, namely class 0 sensor nodes, managed by their corresponding cluster heads. The scheme can be described in detail as following.

Key generation and distribution.

Class 0 sensor nodes and class 1 sensor nodes are dispensed in the sensing space. The class 0 sensor nodes are normal nodes and the class 1 sensor nodes have more power, including communication range, computing ability, etc, than class 0 sensor nodes. Suppose that the links of between sensors are bi-directional. Let r_i $(0 \le i \le 1)$ express the class i communication range. It is clear that $r_0 < r_1$.

The key generation of the heterogeneous wireless hierarchical sensor networks is based on the random key distribution and the OKS (Overlap-Key-Sharing) protocol. Taking the heterogeneity into account, this paper employs a randomly generated long bit-string as a key pool for all kinds of nodes in each cell.

We divide equally the classes of sensor nodes into J cells, denoted as $C'_{00\cdots00}, C'_{00\cdots01}, \cdots, C'_{00\cdots0d'_1}, \cdots, C'_{00\cdots0\sqrt[n_d]{M}}, \cdots, C'_{00\cdots d'_2\sqrt[n_d]{M}}, \cdots, C'_{0d'_{n_d-1}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}, \cdots, C'_{d'_{n_d}\sqrt[n_d]{M}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}, \cdots, C'_{\sqrt[n_d]{M}\sqrt[n_d]{M}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$, where, $0 \le d'_1 \le \sqrt[n_d]{M}$, $0 \le d'_2 \le \sqrt[n_d]{M}, \cdots, 0 \le d'_{n_d-1} \le \sqrt[n_d]{M}$ and $0 \le d'_{n_d} \le \sqrt[n_d]{M}$. A unique group ID j is assigned to all those cells and $j=0, j=1, \cdots, j=d'_1, \cdots, j=\sqrt[n_d]{M}, \cdots, j=d'_2(\sqrt[n_d]{M}+1)+\sqrt[n_d]{M}, \cdots, j=d'_{n_d-1}(\sqrt[n_d]{M}+1)^{n_d-2}+(\sqrt[n_d]{M}+1)^{n_d-2}-1, j=d'_{n_d}(\sqrt[n_d]{M}+1)^{n_d-1}+(\sqrt[n_d]{M}+1)^{n_d-1}-1, \cdots, j=(\sqrt[n_d]{M}+1)^{n_d}-1$.

The key server engenders I long bit-strings, where a unique key pool ID i is assigned to each long bit-string, S_0, $S_1, \cdots, S_{I-2}, S_{I-1}$, and then takes S_0, denoted as Ω_0, as the key-string-pool for 0 class nodes, the mixture of S_0 and S_1, denoted as Ω_1, as the key-string-pool for 1 class nodes and so on. In this paper, we let $I=2$.

A subset Ω_{ij} of those key-string-pools can be engendered for sensors in class i and group j. Let $\Omega_{ij} = \bigcup_{k=0}^{i} \Omega_{ij}(k)$, where $\Omega_{ij}(k)$ is a subset of Ω_k.

In group j, one class i_1 node and one class i_2 node$(i_1 < i_2)$ will be able to share some bit-strings if $\Omega_{i_1 j}(k_1) \bigcap \Omega_{i_2 j}(k_2) \neq \varnothing$ holds, where $k_1 \le i_1 < i_2$, $k_2 \le i_1 < i_2$, $\Omega_{i_1 j}(k_1) \subset \Omega_{k_1}$, and $\Omega_{i_2 j}(k_2) \subset \Omega_{k_2}$. For example, one class 0 node and one class 1 node will share some bit-strings if $\Omega_{0j}(0) \bigcap \Omega_{1j}(0) \neq \varnothing$ holds, where, $\Omega_{0j}(0) \subset \Omega_0$ and $\Omega_{1j}(0) \subset \Omega_0$.

For the same class i, nodes in groups j_1, j_2 $(j_1 \neq j_2)$ will share some bit-strings if $\Omega_{ij_1}(k_1) \bigcap \Omega_{ij_2}(k_2) \neq \varnothing$ holds, where $k_1 \le i$, $k_2 \le i$, $\Omega_{ij_1}(k_1) \subset \Omega_{k_1}$, and $\Omega_{ij_2}(k_2) \subset \Omega_{k_2}$. Class 0 nodes in different groups may share no common bit-strings, namely, $\Omega_{0j_1}(k_1) \bigcap \Omega_{0j_2}(k_2) = \varnothing$, where $\Omega_{0j_1}(0) \subset \Omega_0$ and $\Omega_{0j_2}(0) \subset \Omega_0$, and class 1 nodes in different groups may share no common bit-strings, namely, $\Omega_{1j_1}(k_1) \bigcap \Omega_{1j_2}(k_2) \neq \varnothing$, where $\Omega_{1j_1}(0) \subset \Omega_0$,

$\Omega_{1_{j_1}}(1) \subset \Omega_1, \Omega_{1_{j_2}}(0) \subset \Omega_0$, and $\Omega_{1_{j_2}}(1) \subset \Omega_1$.

The key server chooses a subset Φ_{ij}^n ($\Phi_{ij}^n \subseteq \Omega_{ij}$) of key-strings for a node n in class i and group j. Next, the key server assigns the node the key-string shares of these key-strings.

Location-based grids.

The sensing space V is a n_d dimension, $D_1, D_2, \cdots, D_{n_d-1}$, and D_{n_d}, hypercube and all kinds of nodes are equally distributed in V in this scheme. The sensing hypercube V is equally divided into $(\sqrt[n_d]{M}+2)^{n_d}$, denoted as $C_{00\cdots00}$, $C_{00\cdots01}$, $\cdots$, $C_{00\cdots0d_1}$, $\cdots$, $C_{00\cdots0(\sqrt[n_d]{M}+1)}$, $\cdots$, $C_{00\cdots d_2(\sqrt[n_d]{M}+1)}$, $\cdots$, $C_{00\cdots(\sqrt[n_d]{M}+1)(\sqrt[n_d]{M}+1)}$, $\cdots$, $C_{0d_{n_d-1}\cdots(\sqrt[n_d]{M}+1)(\sqrt[n_d]{M}+1)}$, $\cdots$, $C_{0(\sqrt[n_d]{M}+1)\cdots(\sqrt[n_d]{M}+1)(\sqrt[n_d]{M}+1)}$, $\cdots$, $C_{(\sqrt[n_d]{M}+1)(\sqrt[n_d]{M}+1)\cdots(\sqrt[n_d]{M}+1)(\sqrt[n_d]{M}+1)}$, where, $0 \le d_1 \le \sqrt[n_d]{M}+1$, $0 \le d_2 \le \sqrt[n_d]{M}+1$, $\cdots$, $0 \le d_{n_d-1} \le \sqrt[n_d]{M}+1$ and $0 \le d_{n_d} \le \sqrt[n_d]{M}+1$, small hypercubes called cells. A cluster consists of 2^{n_d-1} cells. $(\sqrt[n_d]{M}+1)^{n_d}$ clusters are denoted as $G_{00\cdots00}$, $G_{00\cdots01}$, $\cdots$, $G_{00\cdots0d_1'}$, $\cdots$, $G_{00\cdots0\sqrt[n_d]{M}}$, $\cdots$, $G_{00\cdots d_2'\sqrt[n_d]{M}}$, $\cdots$, $G_{00\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$, $\cdots$, $G_{0d_{n_d-1}'\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$, $\cdots$, $G_{0\sqrt[n_d]{M}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$, $\cdots$, $G_{\sqrt[n_d]{M}\sqrt[n_d]{M}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$, where, $0 \le d_1' \le \sqrt[n_d]{M}$, $0 \le d_2' \le \sqrt[n_d]{M}$, $\cdots$, $0 \le d_{n_d-1}' \le \sqrt[n_d]{M}$ and $0 \le d_{n_d}' \le \sqrt[n_d]{M}$. The sensor nodes in group $C'_{d_{n_d}'d_{n_d-1}'\cdots d_2'd_1}$ are deployed in cluster $G_{d_{n_d}'d_{n_d-1}'\cdots d_2'd_1}$.

Suppose N_0 class 0 nodes and one class 1 node locate in each cluster and they are evenly distributed in their cluster respectively.

Pair-wise key establishment.

To establish pair-wise keys between the sensor nodes, we utilize three steps, namely, initialization, direct key setup, and (optional) path key setup. Firstly, the initialization step is finished in a key setup center before all the node deployment. The setup server distributes a subset of the key-string-pool to different sensor nodes. Secondly, any two nodes try to establish a pair-wise key; of course, they always first attempt to do so via direct key establishment. If the second step is successful, the third step is omitted. Otherwise, these sensor nodes start path key setup to establish a pair-wise key with the help of other nodes.

The performance analysis for hierarchical wireless heterogeneous sensor network

The function of heterogeneous nodes in network security.

From the above discussion, we know that all the key-string-pools for i ($i = 0,1,\cdots,I\text{-}1$) classes of sensor nodes contain the long bit-strings S_0 and all the key-string-pools for i ($i = 1,2,\cdots,I\text{-}1$) classes of sensor nodes contain the long bit-strings S_0 and S_1, and so on. Therefore, the same subset of key-strings will generate multiple keys at different nodes and the total number of the keys, which a class 0 node will share with all powerful nodes, is the summation of the number of all shared subset of key-strings between the class 0 node and each of the more powerful nodes.

Let $I = 2$ and S be the size of the key-string-pool Ω_1. Suppose that P_0 and P_1 be the number of subset of key-strings that can be stored in a class 0 node and a class 1 node respectively. In a certain logical group, we calculate the probability, $p(\alpha)$, that a class 0 node shares α sub key-strings with a class 1 node as follows

$$p(\alpha) = \frac{\binom{S}{\alpha}\binom{S-\alpha}{P_0-\alpha}\binom{S-P_0}{P_1-\alpha}}{\binom{S}{P_0}\binom{S}{P_1}}. \quad (1)$$

Suppose a class 1 node only can establish secure connection with those class 1 nodes that are close to it in different logical groups. For example, in Fig.1, the class 1 node in G_{11} only can establish secure connection with all those class 1 nodes in G_{00}, G_{01}, G_{10} and so on. We calculate the

probability, $p(\beta)$, that two class 1 nodes in different groups share β sub key-strings as follows

$$p(\beta) = \frac{\binom{S}{\beta}\binom{S-\beta}{P_1-\beta}\binom{S-P_1}{P_1-\beta}}{\binom{S}{P_1}^2} \tag{2}$$

Letting G_0 denote class 0 nodes and G_1 denote the class 1 nodes. We define that a G_1 node is the neighborhood of a G_0 node if it can directly receive a broadcast message sent from the G_1 node. Namely, the G_0 node can obtain bit-string pool information sent by the G_1 node without help of other sensor nodes. To simplify the issue, we assume that a G_0 node can send data to any G_1 in its neighborhood through either a one-hop link if the distance between them is small enough, or a multi-hop if the distance is larger than a threshold.

We give an example to illustrate this strategy in Fig. 1, where node A, X_0 and Y_0 are G_0 nodes, and node X_1 is a G_1 node. In this case, node X_0, Y_0 and X_1 are the only neighbor nodes of the node A. Additionally, node A share key $\mathrm{K1}_i (i = 0,1)$ with X_i $(i = 0,1)$ respectively, similarly, node A share key $\mathrm{K2}_0$ and $\mathrm{K3}_0$ with node Y_0. In this scenario, if node A sends messages to the sink node, certainly, it will first choose the key $\mathrm{K1}_1$. If the distance from node A to node X_1 is larger than a threshold, moreover, in the path from node A to node X_1, there are compromised nodes, the node A will not connect with it. In the same way, the node A will try to connect with a class 0 node, X_0 or Y_0, until its data transmit to the sink node. Obviously, in the WSNs with heterogeneous nodes, the communication is more resilient.

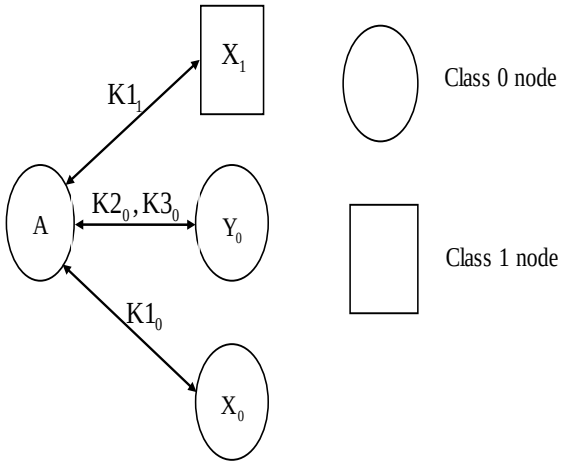

Fig. 1. An example in the scheme

Generally, if a class 0 node is captured and compromised by enemy in a certain logical group, it will not reveal any information of class 0 nodes in other cells, because it share no key with them. Additionally, the class 1 in the same cell is difficult to be compromised because the class 1 nodes are more powerful to attack than class 0 nodes. Therefore, the scheme improves the security for WSNs.

The heterogeneous node function for the network connectivity.

Any a class 0 node and a class 1 node can establish secure connection if they share a key, therefore, from equation (1), the scheme can guarantee that the class 0 node and a class 1 node

establish secure connection if $\sum_{1}^{p_0} p(\alpha) \geq 1$ holds. We can obtain this result through choosing reasonable S, P_0 and P_1. From equation (2), the scheme can guarantee that any two class 1 nodes establish secure connection if $\sum_{1}^{p_1} p(\beta) \geq 1$ holds. We can obtain this result through choosing reasonable S and P_1. Therefore, the scheme can guarantee that all nodes including class 0 nodes and class 1 nodes can establish secure connections with any other node, if $\sum_{1}^{p_0} p(\alpha) \geq 1$ and $\sum_{1}^{p_1} p(\beta) \geq 1$ hold, through selecting reasonable S, P_1 and P_2.

The heterogeneous node function for the network lifetime.

All class 0 nodes in a certain logical group send their information to the class 1 node that is their cluster head, and the class 1 node transmits it to the next cluster head or the base station directly after receiving and aggregating the information. It is clear the cluster heads spend much more energy than cluster sensor nodes. If class 0 nodes act as the cluster heads, they will spend energy more quickly than class 1 nodes because class 1 nodes have more energy than class 0 nodes. Therefore, the network lifetime extends by employing class 1 nodes as the cluster heads.

The conclusion

Key management is of importance to assure wireless sensor networks secure and it has been researched recently. However, in most existing wireless sensor networks, all sensor nodes are supposed to have same capability including battery energy, communication range etc. this paper presents a key management scheme for hierarchical wireless heterogeneous sensor networks through investigating how heterogeneous nodes enhance the performance of wireless sensor networks. The sensing hypercube is divided into a number of small same hypercubes, 2^{n_d} cells of which consist of a n_d-dimension logical group. The structure in this scheme is a two-tier structure. The upper layer consists of all cluster heads and the lower layer consists of all ordinary sensors. All kinds of nodes including heterogeneous nodes are deployed evenly in entire sensing hypercube and they establish their pairwise keys through employing the concept of the overlap key sharing and the random key predistribution scheme. With the help of heterogeneous sensor nodes, this scheme is resilient to compromised node attack, has good network connectivity and prolongs the network lifetime.

Acknowledgements

This work was supported by the Project of Shandong Province Higher Educational Science and Technology Program, and the project number is J13LN05.

References

[1] Mohammad Shokouhifar, Ali Jalali. A new evolutionary based application specific routing protocol for clustered wireless sensor networks. International Journal of Electronics and Communications (AEÜ) 69(2015) 432-441.

[2] Samira Chouikhi, Inès El Korbi, Yacine Ghamri-Doudane, Leila Azouz Saidane. Asurvey on fault tolerance in small and large scale wireless sensor networks. Computer Communications 000(2015)1-16.

[3] J. Szurley, A. Bertrand, M. Moonen. Disytibuted adaptive node-specific signal estimation in heterogeneous and mixed-topology wireless sensor networks. Signal Processing 117 (2015) 44-60.

[4] Min-Yi Wang, Jie Ding, Wan-Pei Chen, and Wen-Qiang Guan. SEARCH: A Stochastic Election Approach for Heterogeneous Wireless Sensor Networks. IEEE COMMUNICATIONS LETTERS, VOL.19, NO.3, MARCH 2015.

[5] D. Lai, Hwang S. Kim, I. Verbauehrde. “Reducing Radio Energy Consumption of Key Management Protocols for Wireless Sensor Networks”, Proceedings of ACM/ IEEE International Symposium on Low Power Electronics and Design (ISLPED’04), 2004, pp.351-356, (2004).