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

Yuquan Zhang[1,2,a] ; Lei Wei[3,b]

[1]Shandong Women University, China

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

[3]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, two-dimension, security, connectivity, lifetime

Abstract. A cluster-based secure strategy for hierarchical wireless heterogeneous sensor networks(HWHSNs) is proposed. The HWHSNs consist of some normal sensor nodes and heterogeneous sensor nodes that have greater power and transmission capability than other normal nodes. Their structure is a two-layer structure. The upper layer consists of all cluster heads, namely heterogeneous sensor nodes, and the lower layer consists of all normal sensors managed by their corresponding cluster heads. All kinds of sensor nodes are evenly distributed respectively in entire sensing area. The two-dimension sensing area is divided into a number of clusters, each of which contains four small squares called cells. The pairwise keys between all kinds of nodes are set up through employing the concept of the overlap key sharing and the random key pre-distribution scheme. Analysis and comparison show this scheme improves the security for HWHSNs, enhances the connectivity for HWHSNs, and prolongs the lifetime of HWHSNs by employing some heterogeneous nodes.

1. Introduction

A wireless sensor network is composed of a number of sensors. The WSNs architectures include heterogeneous architecture, hierarchical architecture, distributed architecture and so on depending on different standards[1]. In hierarchical WSNs, as trusted nodes, cluster heads or base stations can function as the key server center because they have more power than other nodes[2]. In a heterogeneous wireless sensor network, some sensors have more capacities, including sensing ranges, computing ability and son on[3]. WSNs are employed in various fields including battlefield monitoring, biological detection, the sick care, etc[4].

However, WSNs are easily attacked because they are usually distributed in adverse environments. Therefore, security is essential for wireless sensor networks to run smoothly. Lai D et al.[5] presented the OKS protocol. The scheme generates a long bit-string which is the network key-string-pool, and then assigns its subset which is the key-string to each sensor randomly. Sensor nodes employ the overlap intervals of those key-strings as the common key with their neighbor sensors.

Through using the random key pre-distribution strategy and the idea of overlap key sharing (OKS) concept, we present a key management strategy for HWHSNs whose structure is a two-tier structure. The sensing area consists of two-dimensional clusters. The upper tier includes all cluster heads, namely heterogeneous sensor nodes, and the lower tier includes ordinary sensors in all clusters. This paper researches how the heterogeneous sensors improve the HWHSNs performance. The overlap key sharing protocol generates long bit clusters which are the key cluster pools and distributes a sub-group to every node randomly. The sensing square is divided into numerous small same squares called cells. Some class 0 nodes and a class 1 node are in a certain cell, and all class 0 sensors are distributed evenly in the cell and the class 1 node is in the center of the cell. Four of cells are comprised of a cluster called logical group. Analysis and comparison show heterogeneous nodes improve the HWHSNs resilience, enhance the HWHSNs connectivity, and prolong the HWHSNs lifetime.

The rest of this paper is organized as follows. Hierarchical key management scheme is in section two. The section three discusses the HWHSNs performance. The conclusion of this paper is in section four.

2. Hierarchical key management strategy

2.1 Generating and distributing keys

There are two classes of sensor nodes in the HWHSNs, with class 0 being the ordinary nodes, and class 1 being the more powerful nodes. Assume links among sensor nodes are bi-directional and let r_0 denote the communication range of class 0 nodes and r_1 denote the communication range of class 1 nodes. It is clear that $r_0 < r_1$.

The key generation of HWHSNs is based on the OKS (Overlap-Key-Sharing) protocol and the random key distribution. This paper employs a randomly generated long bit-string as a key pool for class 0 nodes and class 1 nodes in each cell.

Firstly, we divide equally the classes of sensor nodes into J groups, denoted as $\mathrm{C}^{'}_{00}, \cdots, \mathrm{C}^{'}_{0j^{'}}, \cdots \mathrm{C}^{'}_{0J^{'}}, \mathrm{C}^{'}_{10}, \cdots,$ $\mathrm{C}^{'}_{1j^{'}}, \cdots, \mathrm{C}^{'}_{1J^{'}}, \cdots, \mathrm{C}^{'}_{i^{'}0}, \cdots, \mathrm{C}^{'}_{i^{'}j^{'}}, \cdots, \mathrm{C}^{'}_{i^{'}J^{'}}, \cdots, \mathrm{C}^{'}_{I^{'}0}, \cdots, \mathrm{C}^{'}_{I^{'}j^{'}},$ $\cdots, \mathrm{C}^{'}_{I^{'}J^{'}}$, where $0 \le i^{'} \le I^{'}$, $0 \le j^{'} \le J^{'}$ and $J = I^{'}(J^{'}+1) + J^{'} + 1$. A unique group ID j is assigned to all those groups and $j = 0$, $\cdots$, $j = j^{'}$, $\cdots$, $j = J^{'}$, $j = J^{'} + 1$, $\cdots$, $j = J^{'} + j^{'} + 1$, $\cdots$, $j = 2J^{'} + 1$, $\cdots$, $j = i^{'}(J^{'}+1)$, $\cdots$, $j = i^{'}(J^{'}+1) + j^{'}$, $\cdots$, $j = i^{'}(J^{'}+1) + J^{'}$, $\cdots$, $j = I^{'}(J^{'}+1)$, $\cdots$, $j = I^{'}(J^{'}+1) + j^{'}, \cdots, j = I^{'}(J^{'}+1) + J^{'}$.

Secondly, I bit-strings including S_0, $S_1, \cdots, S_{I-2}, S_{I-1}$ are created and a sole key pool identifier i is allocated to each of them. We treat S_0, denoted as Ω_0, as the 0 class nodes key-string-pool, and the blend of S_0 and S_1, denoted as Ω_1, as the 1 class sensor nodes key-string-pool, etc.

Thirdly, Ω_{ij}, a subcollection of the key pools, can be formed for nodes in class i and group j. Let $\Omega_{ij} = \bigcup_{k=0}^{i} \Omega_{ij}(k)$, where $\Omega_{ij}(k)$ is a subcollection of Ω_k. Class i_1 and class i_2 $(i_1 < i_2)$ may have some common bit-strings consequently, if $\Omega_{i_1 j}(k_1) \bigcap \Omega_{i_2 j}(k_2) \ne \varnothing$ exists, 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 $\Omega_{i_2 j}(k_2) \subset \Omega_{k_2}$.

This strategy has two class sensors. They may have some joint bit-strings if $\Omega_{0j}(0) \bigcap \Omega_{1j}(0) \ne \varnothing$ exists, where $\Omega_{0j}(0) \subset \Omega_0$ and $\Omega_{1j}(0) \subset \Omega_0$. In another condition, for the same class i, nodes in two different groups j_1, j_2, $j_1 \ne j_2$, may have joint bit-strings if $\Omega_{ij_1}(k_1) \bigcap \Omega_{ij_2}(k_2) \ne \varnothing$ exists, where $k_1 \le i$, $k_2 \le i$, $\Omega_{ij_1}(k_1) \subset \Omega_{k_1}$, and $\Omega_{ij_2}(k_2) \subset \Omega_{k_2}$.

In this scheme, $\Omega_{0j_1}(k_1) \bigcap \Omega_{0j_2}(k_2) = \varnothing$, where $\Omega_{0j_1}(0) \subset \Omega_0$, and $\Omega_{0j_2}(0) \subset \Omega_0$. Namely, class 0 sensors in different groups have no joint keys. Similarly, in this scheme, $\Omega_{1j_1}(k_1) \cap \Omega_{1j_2}(k_2) \ne \varnothing$, where $\Omega_{1j_1}(0) \subset \Omega_0$, $\Omega_{1j_1}(1) \subset \Omega_1$, $\Omega_{1j_2}(0) \subset \Omega_0$, $\Omega_{1j_2}(1) \subset \Omega_1$. Namely, class 1 nodes in different groups may have no joint keys.

At last, the setup server chooses a subcollection of key-strings, Φ^n_{ij} ($\Phi^n_{ij} \subseteq \Omega_{ij}$), for a node n in class i and group j, and then distributes the sensor the key-string shares of these key-strings.

2.2 Location-based grids

In Fig. 1, S_{area} is partitioned into $(I^{'}+2)(J^{'}+2)$ same cells, denoted as $\mathrm{C}_{00}, \mathrm{C}_{01}, \cdots, \mathrm{C}_{0j^{'}}$,

$\cdots, \mathrm{C}_{0J'}, \mathrm{C}_{0(J'+1)}, \mathrm{C}_{10}, \mathrm{C}_{11}, \cdots \mathrm{C}_{1j'}, \cdots, \mathrm{C}_{1J'}, \mathrm{C}_{1(J'+1)}, \cdots, \mathrm{C}_{i'0}, \mathrm{C}_{i'1}, \cdots,$ $\mathrm{C}_{i'j'}, \cdots, \mathrm{C}_{i'J'}, \mathrm{C}_{i'(J'+1)}, \cdots,$ $\mathrm{C}_{(I'+1)0}, \mathrm{C}_{(I'+1)1}, \cdots, \mathrm{C}_{(I'+1)j'}, \cdots, \mathrm{C}_{(I'+1)J'}, \mathrm{C}_{(I'+1)(J'+1)}$, where $0 \le i' \le I' + 1$ and $0 \le j' \le J' + 1$, in the light of their locations. A logical group includes four cells and then S_{area} consists of $(I' + 1)(J' + 1)$ same logical groups, denoted as G_{00}, G_{01}, $\cdots$, $\mathrm{G}_{0j'}$, $\cdots$, $\mathrm{G}_{0(J'-1)}$, $\mathrm{G}_{0J'}$, $\mathrm{G}_{10}, \mathrm{G}_{11}, \cdots \mathrm{G}_{1j'}, \cdots, \mathrm{G}_{1(J'-1)}, \mathrm{G}_{1J'}, \cdots, \mathrm{G}_{i'0}, \mathrm{G}_{i'1}, \cdots,$ $\mathrm{G}_{i'j'}, \cdots, \mathrm{G}_{i'(J'-1)}, \mathrm{G}_{i'J'}, \cdots, \mathrm{G}_{I'0}, \mathrm{G}_{I'1}, \cdots, \mathrm{G}_{I'j'},$ $\cdots, \mathrm{G}_{I'(J'-1)},$ $\mathrm{G}_{I'J'}$, where $0 \le i' \le I'$ and $0 \le j' \le J'$. For example, in Fig. 1, $\mathrm{G}_{I'J'}$ consists of $\mathrm{C}_{I'J'}$, $\mathrm{C}_{I'(J'+1)}$, $\mathrm{C}_{(I'+1)J'}$ and $\mathrm{C}_{(I'+1)(J'+1)}$. If $I' = J'$, there are $(I' + 1)^2 = (J' + 1)^2$ logical groups. The sensor nodes in $\mathrm{C}'_{i'j'}$ are deployed in $\mathrm{G}_{i'j'}$.

We make an assumption that N_0 class 0 nodes are evenly dispensed in each cluster and a class 1 node locates in the center of each cluster.

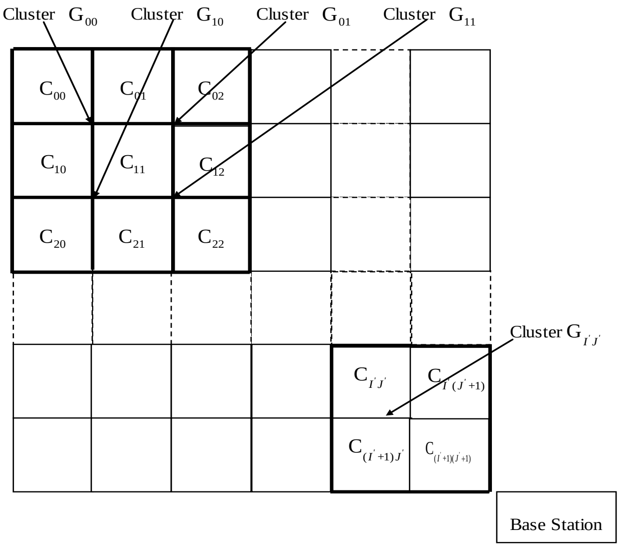

Fig. 1 Location-based cells and clusters

2.3 Establishing pair-wise keys

To establish common keys between the nodes, three steps, namely, initialization, direct key setup, and (optional) path key setup, are utilized. The initialization is completed in a key setup center before all the sensor nodes are deployed. The setup server distributes a subcollection of the key pool to different sensor nodes. Next, any two sensor nodes try to set up a pair-wise key; of course, at first they always make an effort to do so via direct key establishment. If the second step is well-off, the third step leaves out. Otherwise, they start path key setup to set up a common key with the help of other nodes.

3. The performance analysis for WHSNs

3.1 The function of heterogeneous nodes in network security

All the key pools for i ($i = 0,1,\cdots, I$ -1) classes of sensor nodes include the bit-strings S_0 and all the key pools for i ($i = 1,2,\cdots,\mathrm{I}$ -1) classes of sensor nodes include the bit-strings S_0 and S_1, etc. Therefore, the same subcollection of key-strings will create multiple keys at different nodes and the whole number of the keys, which a class 0 node will have with all powerful nodes, is the summation of the number of all shared subcollection of key-strings between the class 0 node and each of the more powerful nodes.

Let $I = 2$ and S be the size of Ω_1. We make an assumption that P_0 and P_1 be the number of subcollection of key-strings which can be saved in a class 0 node and a class 1 node severally. In a certain logical group, we compute the probability $p(\alpha)$ that a class 0 node shares α sub key-strings with a class 1 node as the following

$$p(\alpha)=\frac{\begin{pmatrix}S\\ \alpha\end{pmatrix}\begin{pmatrix}S-\alpha\\ P_0-\alpha\end{pmatrix}\begin{pmatrix}S-P_0\\ P_1-\alpha\end{pmatrix}}{\begin{pmatrix}S\\ P_0\end{pmatrix}\begin{pmatrix}S\\ P_1\end{pmatrix}}.$$

We make an assumption that a class 1 node only can set up safe connection with those class 1 nodes which are close to it in different logical groups. For example, in Fig.1, the class 1 node of G_{11} only can set up safe connections with all those class 1 nodes in G_{00}, G_{01}, G_{10}, etc. The probability $p(\beta)$ that two class 1 nodes in different groups have β sub common key-strings as follows

$$p(\beta)=\frac{\begin{pmatrix}S\\ \beta\end{pmatrix}\begin{pmatrix}S-\beta\\ P_1-\beta\end{pmatrix}\begin{pmatrix}S-P_1\\ P_1-\beta\end{pmatrix}}{\begin{pmatrix}S\\ P_1\end{pmatrix}^2}.$$

G_0 denotes the class 0 nodes and G_1 denotes the class 1 nodes. A G_1 node is the vicinage of a G_0 node if it can accept a broadcast message transmitted from the G_1 node directly. In other word, the G_0 node can gain bit-string pool information transmitted by the G_1 node without help of other sensor nodes. For simplicity, we suppose a G_0 node can forward data to any G_1 in its vicinage through a one-hop link means if the distance between them is small enough, or a multi-hop means if the distance is more than a threshold.

A, X_0 and Y_0 are G_0 nodes, and X_1 is a G_1 node in Fig. 2. X_0, Y_0 and X_1 are the only vicinage nodes of A. In addition, A shares key $\mathrm{K1}_i(i=0,1)$ with X_i $(i=0,1)$ severally. Similarly, A has common key $\mathrm{K2}_0$ and $\mathrm{K3}_0$ with Y_0. If A forwards messages to the sink node, it will firstly select $\mathrm{K1}_1$. If the distance between A and X_1 is more than a threshold, moreover, in the path between A and X_1, there are captured nodes, A will not connect with it. Similarly, A will make an effort to connect with X_0 or Y_0, until its data transmit to the sink node. It is obvious that the communication is more resilient in the WSNs with heterogeneous nodes.

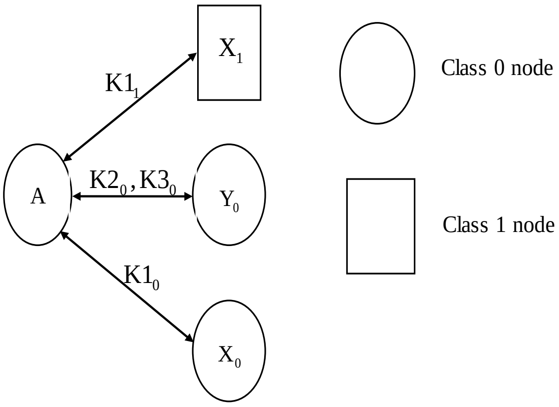

Fig. 2 An example in the scheme

If a class 0 node is compromised by opponents in a certain logical group, it will disclose no information of class 0 nodes in other cells, because it has no common keys with them. Additionally, capturing the class 1 sensors in the same cell is arduous because the class 1 nodes are stronger to shield attacks than class 0 nodes. Therefore, the scheme improves the security for WSNs.

3.2 The function of heterogeneous nodes for the network connectivity

A class 0 node and a class 1 node can set up safe connection if they have a common key. Therefore, the scheme can ensure that the class 0 node and a class 1 node set up secure connection if $\sum_{1}^{p_0} p(\alpha) \ge 1$. We can gain this conclusion by selecting reasonable S, P_0 and P_1. The scheme can ensure any two class 1 nodes set up safe connection if $\sum_{1}^{p_1} p(\beta) \ge 1$. We can gain this conclusion by selecting reasonable S and P_1. Therefore, the scheme can ensure each of all nodes set up safe connections with any other node, if $\sum_{1}^{p_0} p(\alpha) \ge 1$ and $\sum_{1}^{p_1} p(\beta) \ge 1$, through choosing reasonable S, P_1 and P_2.

3.3 The function of heterogeneous nodes for the network lifetime

In Fig. 3, each of all class 0 nodes in $\mathrm{G}_{i'j'}$ forwards its information to the class 1 node which is its cluster head and then the class 1 node transmits it to the next cluster head or the base station directly after accepting and aggregating those information. Obviously, the cluster heads consume much more energy than cluster sensor nodes. If class 0 nodes are the cluster heads, they will consume their battery power more quickly than class 1 nodes because class 1 nodes have more battery power than class 0 nodes. Therefore, the network lifetime enlarges through employing class 1 nodes as the cluster heads.

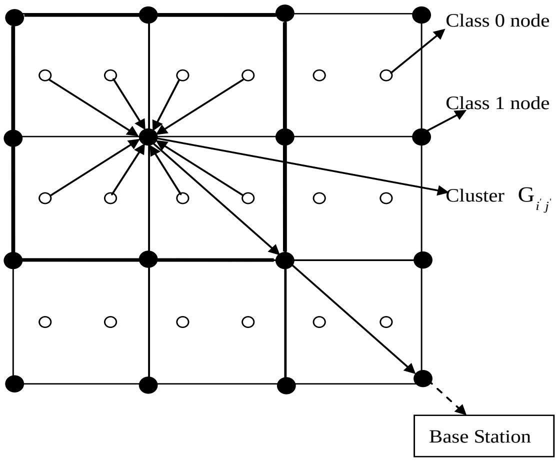

Fig. 3 Sending information in this scheme

4. The conclusion

The paper studies how heterogeneous nodes improve the WSNs security and connectivity, and prolong the network lifetime. All kinds of sensor nodes are dispensed uniformly in sensing area which is partitioned into a number of same cells. Four of cells consist of a logical group for class 1 nodes. This scheme has a two-tier structure. The upper layer consists of all cluster heads and the lower layer consists of all ordinary sensors. The pairwise keys between nodes are established by employing the concept of the overlap key sharing and the random key pre-distribution strategy. Analysis and comparison show heterogeneous nodes improve both the security and connectivity for WSNs and extend the network lifetime.

References

[1] W. Elghazel, J.Bahi, C.Guyeux, M.Hakem, K.Medjaher, H.Zerhouni. Dependability of wireless sensor networks for industrial prognostics and health management. Computers in Industry 68(2015)1-15.

[2] S. Camtepe, B. Yener. “Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks”, ACM Transactions on Networking, 15(2): 346-358, (2007)

[3] K. P. Shih, S.S Wang, P. H. Yang, C. C. Chang. “CollECT: collaborative event detection and tracking in wireless heterogeneous sensor networks”, In: Proceedings of the 11th IEEE symposium on computers and communications (ISCC 2006); June 2006, pp. 935-940, (2006).

[4] Wei Li, Wei Zhang. Coverage hole and boundary nodes detection in wireless sensor networks. Journal of Network and Computer Applications 48(2015) 35-43.

[5] D. Lai, et al. “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).