A Key Management Scheme Based on Multi-Dimension Location for Clustered Heterogeneous Wireless 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: Heterogeneous wireless sensor network; security; connectivity; multi-dimension

Abstract. A key scheme based on multi-dimension location is presented for heterogeneous wireless sensor networks (HWSNs). 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 space. The sensing space is divided into a number of small same hypercubes for all kinds of nodes and then some of them consist of a logical group for those heterogeneous nodes. This paper researches 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, the grid-based key pre-distribution scheme, and the random key pre-distribution scheme. Analysis shows the heterogeneous nodes improve the security and connectivity for wireless sensor networks.

1. Introduction

A wireless sensor network consists of a number of sensor nodes. Heterogeneous wireless sensor networks consist of different sensor nodes, some of which have more powerful capabilities, including computing ability, communication ranges, storages, etc, than other sensor nodes[1]. WSNs have obtained a great deal of research attention because they have various applications[2]. WSNs are sometimes distributed in unfriendly, or even hostile environments, moreover, sensors have some limitations including low storage, limited communication range, etc. Therefore, wireless sensor networks are vulnerable to be attacked[3]. Guaranteeing wireless sensor networks secure is one of importance issue. Lai D et al.[4] gave the OKS (Overlap-Key-Sharing) protocol. The strategy creates a long bit-string and it acts as the WSNs key-string-pool (KP). Next, the strategy randomly allocates each node a subset of the key-string-pool. Sensors in this scheme employ the overlap intervals of the key-strings which act as the shared secret key with their neighbor sensors. Zhang[5] gave a safe scheme in which the sensing space consist of clusters each of which consists of some cells.

This paper gives a pairwise key establishment scheme for HWSNs through researching how the heterogeneous sensors improve the WSNs performance. The sensing hyperspace is divided into numerous cells and logical groups. Heterogeneous nodes and ordinary nodes are evenly deployed in sensing space. The overlap key sharing protocol generates bit clusters which act as the key cluster pools. Next, it allocates each sensor a sub-group. Through employing the grid-based key pre-distribution strategy and the concept of the overlap key sharing, pairwise keys are set up between nodes including heterogeneous nodes and ordinary nodes. We can prove that this scheme enhances the WSNs resilience and has good network connectivity.

The structure of this paper is as follows. The distributed key management strategy is given in section two. Performance analysis for HWSNs is presented in the section three. The conclusion of this paper is in section four.

2. Distributed key management strategy

2.1 Generating and distributing keys

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 $r_0 < r_1$.

By utilizing the OKS protocol, the random key distribution method, the grid-based key pre-distribution scheme, the key generation for HDWSNs works. This scheme employs a randomly generated bit-string as the key pool for all kinds of sensors.

This scheme partitions equally the classes of sensor nodes into J cells, expressed 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 identifier j is allocated to each of 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 setup server generates I bit-strings, where a unique key pool identifier i is allocated to each of them, expressed as $S_0, S_1, \cdots, S_{I-2}, S_{I-1}$, and then takes S_0, expressed as Ω_0, as the key-string-pool for 0 class sensors, the combination of S_0 and S_1, expressed as Ω_1, as the key-string-pool for 1 class sensor nodes, etc.

A subset of those key-string-pools, expressed as Ω_{ij}, may be generated for nodes in class i and group j. Allowing $\Omega_{ij} = \bigcup_{k=0}^{i} \Omega_{ij}(k)$, where $\Omega_{ij}(k)$ is a subset of Ω_k.

In group j, two classes i_1 and $i_2 (i_1 < i_2)$ will be able to have some common bit-strings if $\Omega_{i_1 j}(k_1) \bigcap \Omega_{i_2 j}(k_2) \neq \varnothing$ 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 $\Omega_{i_2 j}(k_2) \subset \Omega_{k_2}$. For example, two classes 0 and 1 will be able to have some common bit-strings if $\Omega_{0j}(0) \bigcap \Omega_{1j}(0) \neq \varnothing$, where, $\Omega_{0j}(0) \subset \Omega_0$ and $\Omega_{1j}(0) \subset \Omega_0$.

In another condition, for the same class i, sensors in two different groups $j_1, j_2 (j_1 \neq j_2)$ will be able to have some common bit-strings if $\Omega_{ij_1}(k_1) \bigcap \Omega_{ij_2}(k_2) \neq \varnothing$, 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 have 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 have no common bit-strings, namely, $\Omega_{1j_1}(k_1) \bigcap \Omega_{1j_2}(k_2) \neq \varnothing$, where $\Omega_{1j_1}(0) \subset \Omega_0$, $\Omega_{1j_1}(1) \subset \Omega_1, \Omega_{1j_2}(0) \subset \Omega_0$, and $\Omega_{1j_2}(1) \subset \Omega_1$.

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

2.2 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. All nodes are scattered in V equally. V is equally partitioned into $(\sqrt[n_d]{M}+1)^{n_d}$, $C_{00\cdots00}$, $C_{00\cdots01}$, $\cdots$, $C_{00\cdots0d_1}$, $\cdots$, $C_{00\cdots0\sqrt[n_d]{M}}$, $\cdots$, $C_{00\cdots d_2\sqrt[n_d]{M}}$, $\cdots$, $C_{00\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$,

$\cdots, C_{0d_{n_d-1}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}, \cdots, C_{0\sqrt[n_d]{M}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}, \cdots, C_{\sqrt[n_d]{M}\sqrt[n_d]{M}\cdots\sqrt[n_d]{M}\sqrt[n_d]{M}}$, 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 $0 \le d_{n_d} \le \sqrt[n_d]{M}$, cells. The sensor nodes of $C'_{d'_{n_d}d'_{n_d-1}\cdots d'_2 d_1}$ are deployed in $C_{d_{n_d}d_{n_d-1}\cdots d_2 d_1}$. A cluster includes 2^{n_d-1} cells. M clusters are expressed as $G_{00\cdots00}$, $G_{00\cdots01}$, $\cdots$, $G_{00\cdots0d'_1}$, $\cdots$, $G_{00\cdots0(\sqrt[n_d]{M}-1)}$, $\cdots$, $G_{00\cdots d'_2(\sqrt[n_d]{M}-1)}$, $\cdots$, $G_{00\cdots(\sqrt[n_d]{M}-1)(\sqrt[n_d]{M}-1)}$, $\cdots$, $G_{0d'_{n_d-1}\cdots(\sqrt[n_d]{M}-1)(\sqrt[n_d]{M}-1)}$, $\cdots$, $G_{0(\sqrt[n_d]{M}-1)\cdots(\sqrt[n_d]{M}-1)(\sqrt[n_d]{M}-1)}$, $\cdots$, $G_{(\sqrt[n_d]{M}-1)\sqrt[n_d]{M}-1)\cdots(\sqrt[n_d]{M}-1)(\sqrt[n_d]{M}-1)}$. 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 $0 \le d'_{n_d} \le \sqrt[n_d]{M}-1$. We make an assumption that N_0 class 0 nodes and N_1 class 1 nodes are in each cell and they are distributed evenly.

2.3 Establishing pair-wise keys

This strategy employs three steps including initialization, direct key setup, and (optional) path key setup, in order to set up pair-wise keys among sensor nodes. The initialization is fulfilled in a key setup center before class 0 sensors and class 1 sensors are dispensed. The setup server allocates different sensor nodes a subset of the key-string-pool. In the direct key setup, any two sensors attempt to set up their pair-wise key; it is clear that they firstly try to finish this step via direct key establishment through a distributed peer-peer manner. If the second phase is successful, the third phase is omitted. Otherwise, they begin path key setup to set up a pair-wise key by using their intermediate nodes. In this scheme, the path key setup can be disabled because this scheme uses the heterogeneity.

3. The HWSNs performance analysis

3.1 The function of heterogeneous nodes in HWSNs connectivity

Probability theoretical method will be employed because this scheme generates or chooses keys randomly in this section. For simplicity, we consider a special case which has two classes of the sensor nodes and has *J* groups.

All the key-string-pools for i ($i = 0,1,\cdots,I\text{-}1$) classes of nodes include the bit-strings S_0 and all the key-string-pools for i ($i = 1,2,\cdots,\mathrm{I}\text{-}1$) classes of nodes include the bit-strings S_0 and S_1, etc. Therefore, the same subset of key-strings will originate multiple keys at different sensors 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 Ω. Assume that P_0 and P_1 be the number of subset of key-strings that can be kept in a class 0 node and a class 1 node respectively. The probability $p(\alpha)$ that a class 0 node shares α sub key-strings with a class 1 node is calculated as follows

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

A class 0 node and a class 1 node can set up secure path if they have a shared key, therefore, the strategy can ensure that they set up secure path if $\sum_{1}^{p_0} p(\alpha) \ge 1$. This result can be obtained through selecting reasonable S, P_0 and P_1.

This scheme forms $2\sqrt[n_d]{\frac{N_1}{2}} \times 2\sqrt[n_d]{\frac{N_1}{2}} \times \cdots \times 2\sqrt[n_d]{\frac{N_1}{2}}$ hyper grid denoted by a n_d-dimension hyper coordinate system in $G_{D_1D_2\cdots D_{n_d-1}D_{n_d}}$ in which those hyper axes are bit clusters GID_{D_1}, GID_{D_2}, $\cdots$,

$\mathrm{GID}_{D_{n_d-1}}$ and $\mathrm{GID}_{D_{n_d}}$. Each of bit clusters GID_{D_1} consist of $2\sqrt[n_d]{\frac{N_1}{2}}$ sub bit clusters $\mathrm{GID}_{D_1} \| \mathrm{NID}_{D_1^{'}}$, where, $D_1^{'} = 0,1,\cdots,\left(2\sqrt[n_d]{\frac{N_1}{2}}-2\right)$, $\left(2\sqrt[n_d]{\frac{N_1}{2}}-1\right)$. In GID_{D_1}, $0,1,\cdots,\left(2\sqrt[n_d]{\frac{N_1}{2}}-2\right)$, $\left(2\sqrt[n_d]{\frac{N_1}{2}}-1\right)$ express $\mathrm{GID}_{D_1} \| \mathrm{NID}_0$, $\mathrm{GID}_{D_1} \| \mathrm{NID}_1$, $\cdots$, $\mathrm{GID}_{D_1} \| \mathrm{NID}_{2\sqrt[n_d]{\frac{N_1}{2}}-2}$, $\mathrm{GID}_{D_1} \| \mathrm{NID}_{2\sqrt[n_d]{\frac{N_1}{2}}-1}$ respectively. Similarly, for GID_{D_2}, $\cdots$, $\mathrm{GID}_{D_{n_d-1}}$ and $\mathrm{GID}_{D_{n_d}}$ there are similar results. In $\mathrm{G}_{D_1 D_2 \cdots D_{n_d-1} D_{n_d}}$, the setup server distributes $\left\{\mathrm{ID}, \mathrm{GID}_{D_1} \| \mathrm{NID}_{D_1^{'}}, \mathrm{GID}_{D_2} \| \mathrm{NID}_{D_2^{'}}, \cdots, \mathrm{GID}_{D_{n_d-1}} \| \mathrm{NID}_{D_{n_d-1}^{'}}, \mathrm{GID}_{D_{n_d}} \| \mathrm{NID}_{D_{n_d}^{'}}\right\}$ to each class 1 node, where ID is the class 1 node hyper grid-based index. If the node is at the intersection of hyper axes, namely, bit clusters $\mathrm{GID}_{D_1}, \mathrm{GID}_{D_2}, \cdots, \mathrm{GID}_{D_{n_d-1}}$ and $\mathrm{GID}_{D_{n_d}}$, the ID of the node is denoted as $\left\langle D_1^{'}, D_2^{'}, \cdots, D_{n_d-1}^{'}, D_{n_d}^{'} \right\rangle$. This scheme supposes all class 1 nodes in the logical group $\mathrm{G}_{D_1 D_2 \cdots D_{n_d-1} D_{n_d}}$ are at the intersections. It is obvious that different nodes at different intersections have different hyper grid-based indexes. Next, The setup server distributes $\left\{\left\langle D_1^{'}, D_2^{'}, \cdots, D_{n_d-1}^{'}, D_{n_d}^{'} \right\rangle, \mathrm{GID}_{D_1} \| \mathrm{NID}_{D_1^{'}}, \mathrm{GID}_{D_2} \| \mathrm{NID}_{D_2^{'}}, \cdots, \mathrm{GID}_{D_{n_d-1}} \| \mathrm{NID}_{D_{n_d-1}^{'}}, \mathrm{GID}_{D_{n_d}} \| \mathrm{NID}_{D_{n_d}^{'}}\right\}$ to each sensor at intersection.

Assume class 1 node S^0 is in $\mathrm{G}_{D_1 D_2 \cdots D_{n_d-1} D_{n_d}}$ and its index is $\left\langle D_{1_{S^0}}^{'}, D_{2_{S^0}}^{'}, \cdots, D_{(n_d-1)_{S^0}}^{'}, D_{(n_d)_{S^0}}^{'} \right\rangle$. After node deployment, S^0 broadcasts its message $\left\{\left\langle D_{1_{S^0}}^{'}, D_{2_{S^0}}^{'}, \cdots, D_{(n_d-1)_{S^0}}^{'}, D_{(n_d)_{S^0}}^{'} \right\rangle, \mathrm{GID}_{D_1} \| \mathrm{NID}_{D_{1_{S^0}}^{'}}, \right.$ $\left. \mathrm{GID}_{D_2} \| \mathrm{NID}_{D_{2_{S^0}}^{'}}, \cdots, \mathrm{GID}_{D_{(n_d-1)}} \| \mathrm{NID}_{D_{(n_d-1)_{S^0}}^{'}}, \mathrm{GID}_{D_{n_d}} \| \mathrm{NID}_{D_{(n_d)_{S^0}}^{'}} \right\}$ in order to discover nodes, which have common sub bit clusters with it. The common sub bit cluster $\mathrm{GID}_{D_1} \| \mathrm{NID}_{D_{1_{S^0}}^{'}}$ is shared by nodes whose GID_{D_1} coordinate is $D_1^{'}$. There are similar results for the $\mathrm{GID}_{D_2} \| \mathrm{NID}_{D_{2_{S^0}}^{'}}, \cdots, \mathrm{GID}_{D_{(n_d-1)}} \| \mathrm{NID}_{D_{(n_d-1)_{S^0}}^{'}}, \mathrm{GID}_{D_{n_d}} \| \mathrm{NID}_{D_{(n_d)_{S^0}}^{'}}$.

If S^1 and S^2 share one or more of $\mathrm{GID}_{D_1} \| \mathrm{NID}_{D_{1_{S^0}}^{'}}$, $\mathrm{GID}_{D_2} \| \mathrm{NID}_{D_{2_{S^0}}^{'}}, \cdots, \mathrm{GID}_{D_{(n_d-1)}} \| \mathrm{NID}_{D_{(n_d-1)_{S^0}}^{'}}$, and $\mathrm{GID}_{D_{n_d}} \| \mathrm{NID}_{D_{(n_d)_{S^0}}^{'}}$, they can directly set up a pairwise key. Otherwise, if they share nothing, they also can establish pairwise keys through $n_d!$ intermediate nodes.

Therefore, the scheme ensures each pair of class 1 nodes can establish a pairwise key if they can communicate each other and the information can be transmitted to the base station safely. In addition, the class 1 nodes can establish a pairwise key with each of class 0 nodes in each cell. Therefore, this scheme ensures that all nodes are connective and can establish secure communication.

3.2 The function of heterogeneous nodes in HWSNs security

Let G_0 denote the class 0 nodes and G_1 denote the class 1 nodes. If a G_0 can directly receive a broadcast message sent from a G_1 node, the G_1 node is its neighborhood. Namely, the G_0 node can get bit-string pool message forwarded by the G_1 node by itself. For simplicity, this scheme supposes a G_0 node can transmit information to any G_1 in its neighborhood through either a one-hop link manner if the distance between the G_0 node and the G_1 node is small

enough, or a multi-hop manner if the distance is larger than a threshold.

In Fig. 1, A, X_0 , Y_0 and Z_0 are G_0 nodes, and node X_1 , Y_1 and Z_1 are G_1 nodes. X_0, Y_0, Z_0, X_1, Y_1 and Z_1 are the only neighbor sensors of A. In addition, A has common key $K1_i (i = 0,1)$ with X_i $(i = 0,1)$ respectively, has common key $K2_i$ and $K3_i$ with node $Y_i (i = 0,1)$ respectively, and has common key $K4_i$ with node $Z_i (i = 0,1)$. If A transmits messages to the sink node, it will firstly select a key from $K1_1, K2_1, K3_1$ and $K4_1$. If the distances from A to X_1, Y_1 and Z_1 are larger than a threshold, moreover, there are compromised nodes in the routes from *A* to X_1, Y_1 and Z_1, A will not connect with it. Similarly, A will try to connect with a class 0 node, X_0 or Y_0 or Z_0, until its data are transmitted to the sink node. It is clear the communication is more resilient in the WSNs with heterogeneous nodes.

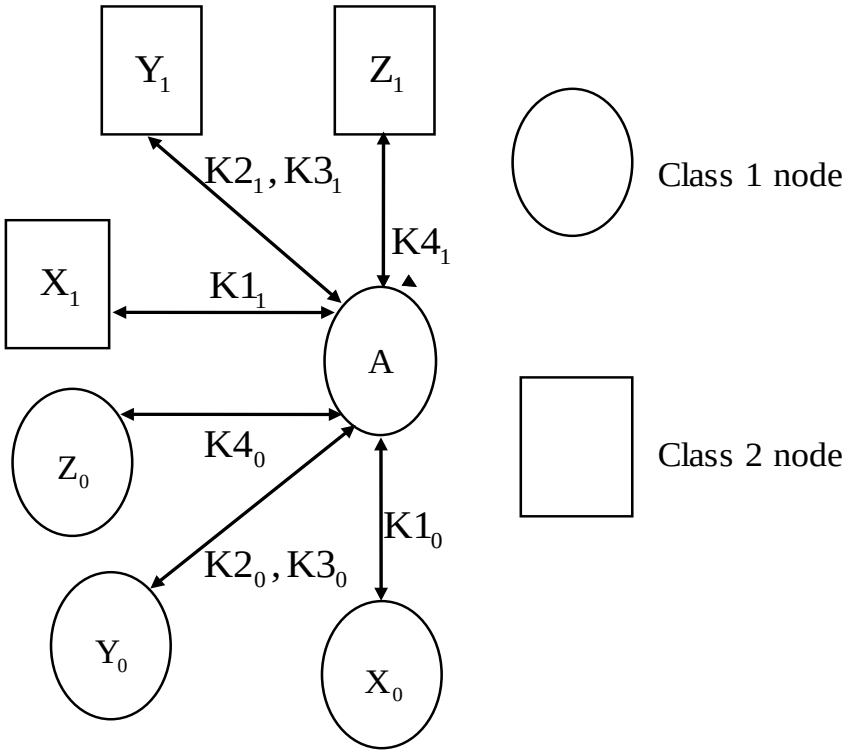

Fig.1 An example in the scheme

In general, if a class 0 node is compromised in a certain cell, it will reveal no information of class 0 nodes in other cells, because it has no common key with them. In addition, compromising the class 1 nodes in the same cell is difficult because they are more powerful to withstand attacks than class 0 nodes. Therefore, the scheme improves the WSNs security.

4. The conclusion

This paper gives a key management scheme for HWSNs through studying how heterogeneous nodes improve the network performance. The sensing space consists of a number of cells and groups. All nodes are deployed evenly in entire sensing space and they establish their common keys through using the random key pre-distribution strategy and the concept of the overlap key sharing. The HWSNs are resilient to compromised node attacks and have good connectivity under the heterogeneous nodes help.

References

[1] Sudeep Tanwar, Neeraj Kumar, Joel J.P.C. Rodrigues. A systematic rewiew on heterogeneous

routing protocals for wireless sensor network. Journal of Network and Computer Applications 53(2015)139-56.

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

[3] Xiao-Jun Tong, Zhu Wang, Yang Liu, Miao Zhang, Lianjie Xu. A novel compound chaotic block cipher for wireless sensor networks. Commun Nonlinear Sci Numer Simulat 22(2015) 120-133.

[4] Lai D, 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.

[5] Yuquan Zhang. A secure based on multi-dimension location for wireless sensor networks. WIT Transaction on Information and Communication Technology, 2014, Vol. 51, pp697-711.