A Secure Scheme for Cluster-based 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: Wireless sensor network; security; clustering; OKS; multi-dimension

Abstract. A strategy for wireless sensor network security is presented through dividing sensing multi-dimension hypercube into clusters and using the overlap key sharing (OKS) concept in this paper. The multi-dimension sensing hypercube is divided into a number of small same dimension hypercubes called cells, some of which are comprised of a cluster called logical group. The overlap key sharing protocol creates long bit clusters as the key cluster pools and distributes a sub-group to every sensor as key cluster. Analysis and comparison demonstrate this scheme enhances the WSN security, realizes the flexile secure grades for WSN, and has good network connection.

Introduction

Guaranteeing the WSN secure is an of importance issue. Key management scheme is an efficient way to assure wireless sensor networks secure.

A. Perrig et al.[1] proposed that the base station sends the pairwise key encrypted with the two shared keys to two nodes respectively if they need to set up a pairwise key. Although this scheme has good resilience, it has poor scalability because the base station has to send keys to the related sensors. To solve the shortage, L. Eschenauer and V. D. Gligor[2]proposed that communication keys are set up through three steps: key predistribution, shared-key discovery, and path-key establishment. In the first phase, a large key pool is generated, and some distinct keys are drawn out of the pool and stored into sensor memory. In the second phase, each sensor in WSNs finds its neighbors with its shared keys in its wireless communication range. In the last phase, those sensors that do not share common keys are connected by two or more links.

This scheme divides sensing multi-dimension hypercube into the same dimension small hypercubes called cells, 2^{n_d} cells of which consist of a n_d -dimension cluster called logical group and uses the overlap key sharing (OKS) concept, which creates long bit clusters as the key cluster pools and distributes a sub-group to every sensor as key cluster. Analysis and comparison show that this scheme enhances the resilience of WSNs, provides the flexile secure grades for WSN, and has good network connection.

The rest of this paper is organized as follows. In section two, location-based pairwise key establishment is given. Performance analysis for WSNs is given in the section three. The conclusion of this paper is in section four.

Location-based pairwise key establishment

Bit cluster group establishment and sensing hypercube division.

In this paper, the sensing space is a n_d dimension, $D_1, D_2, \cdots, D_{n_d-1}$, and D_{n_d}, hypercube denoted as V_{hc} and the nodes are equally distributed in V_{hc} in this scheme. We introduce the key cluster concept in paper [3]. In [3], the overlap key sharing protocol creates long bit clusters as the key cluster pools and distributes a sub-group to every sensor as key cluster. The sensors employ the overlap sections as the sharing keys with their neighbor sensors.

The overlap key sharing protocol creates n_d $\left(\sqrt[n_d]{m}-1\right)$ bit clusters denoted as GID_{D_1} , GID_{D_2} , $\cdots$, $\mathrm{GID}_{D_{n_d-1}}$ and $\mathrm{GID}_{D_{n_d}}$, where, $D_1 = 0,1,\cdots,\left(\sqrt[n_d]{m}-3\right),\left(\sqrt[n_d]{m}-2\right)$, $D_2 = 0,1,\cdots,\left(\sqrt[n_d]{m}-3\right),\left(\sqrt[n_d]{m}-2\right)$, $\cdots$, $D_{n_d-1} = 0,1,\cdots,\left(\sqrt[n_d]{m}-3\right),\left(\sqrt[n_d]{m}-2\right)$ and $D_{n_d} = 0,1,\cdots,\left(\sqrt[n_d]{m}-3\right),\left(\sqrt[n_d]{m}-2\right)$. The setup server randomly generates $\left(\sqrt[n_d]{m}-1\right)^{n_d}$ bit cluster groups $\mathrm{G}'_{D_1D_2\cdots D_{n_d-1}D_{n_d}}$ through picking a bit cluster from GID_{D_1} , GID_{D_2} , $\cdots$, $\mathrm{GID}_{D_{n_d-1}}$ and $\mathrm{GID}_{D_{n_d}}$ respectively. $\mathrm{G}'_{D_1D_2\cdots D_{n_d-1}D_{n_d}}$ includes $\mathrm{G}'_{00\cdots00}$, $\mathrm{G}'_{00\cdots01}$, $\cdots$, $\mathrm{G}'_{00\cdots0D_1}$, $\cdots$, $\mathrm{G}'_{00\cdots0(\sqrt[n_d]{m}-3)}$, $\mathrm{G}'_{00\cdots0(\sqrt[n_d]{m}-2)}$, $\mathrm{G}'_{00\cdots10}$, $\mathrm{G}'_{00\cdots11}$, $\cdots$, $\mathrm{G}'_{00\cdots1D_1}$, $\cdots$, $\mathrm{G}'_{00\cdots1(\sqrt[n_d]{m}-3)}$, $\mathrm{G}'_{00\cdots1(\sqrt[n_d]{m}-2)}$, $\cdots$, $\mathrm{G}'_{00\cdots D_20}$, $\mathrm{G}'_{00\cdots D_21}$, $\cdots$, $\mathrm{G}'_{00\cdots D_2D_1}$, $\cdots$, $\mathrm{G}'_{00\cdots D_2(\sqrt[n_d]{m}-3)}$, $\mathrm{G}'_{00\cdots D_2(\sqrt[n_d]{m}-2)}$, $\cdots$, $\mathrm{G}'_{00\cdots(\sqrt[n_d]{m}-2)0}$, $\mathrm{G}'_{00\cdots(\sqrt[n_d]{m}-2)1}$, $\cdots$, $\mathrm{G}'_{00\cdots(\sqrt[n_d]{m}-2)D_1}$, $\cdots$, $\mathrm{G}'_{00\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-3)}$, $\mathrm{G}'_{00\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)}$, $\cdots$, $\mathrm{G}'_{0(\sqrt[n_d]{m}-2)\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)}$, $\cdots$, $\mathrm{G}'_{(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)}$.

The sensing hypercube V_{hc} in the wireless sensor networks is divided into m same hypercube cells, denoted as $\mathrm{C}'_{00\cdots00}$, $\mathrm{C}'_{00\cdots01}$, $\cdots$, $\mathrm{C}'_{00\cdots0D_1}$, $\cdots$, $\mathrm{C}'_{00\cdots0(\sqrt[n_d]{m}-2)}$, $\mathrm{C}'_{00\cdots0(\sqrt[n_d]{m}-1)}$, $\mathrm{C}'_{00\cdots10}$, $\mathrm{C}'_{00\cdots11}$, $\cdots$, $\mathrm{C}'_{00\cdots1D_1}$, $\cdots$, $\mathrm{C}'_{00\cdots1(\sqrt[n_d]{m}-2)}$, $\mathrm{C}'_{00\cdots1(\sqrt[n_d]{m}-1)}$, $\cdots$, $\mathrm{C}'_{00\cdots D_20}$, $\mathrm{C}'_{00\cdots D_21}$, $\cdots$, $\mathrm{C}'_{00\cdots D_2D_1}$, $\cdots$, $\mathrm{C}'_{00\cdots D_2(\sqrt[n_d]{m}-2)}$, $\mathrm{C}'_{00\cdots D_2(\sqrt[n_d]{m}-1)}$, $\cdots$, $\mathrm{C}'_{00\cdots(\sqrt[n_d]{m}-1)0}$, $\mathrm{C}'_{00\cdots(\sqrt[n_d]{m}-1)1}$, $\cdots$, $\mathrm{C}'_{00\cdots(\sqrt[n_d]{m}-1)D_1}$, $\cdots$, $\mathrm{C}'_{00\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-2)}$, $\mathrm{C}'_{00\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$, $\cdots$, $\mathrm{C}'_{0(\sqrt[n_d]{m}-1)\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$, $\cdots$, $\mathrm{C}'_{(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$. Where, $D_1 = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$, $D_2 = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$, $\cdots$, $D_{n_d-1} = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$ and $D_{n_d} = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$, according to their geographical locations.

Cells based on location and logical groups.

There are N sensor nodes in the sensing hypercube V_{hc}. Those nodes are divided into m same groups denoted as $\mathrm{C}_{00\cdots00}$, $\mathrm{C}_{00\cdots01}$, $\cdots$, $\mathrm{C}_{00\cdots0D_1}$, $\cdots$, $\mathrm{C}_{00\cdots0(\sqrt[n_d]{m}-2)}$, $\mathrm{C}_{00\cdots0(\sqrt[n_d]{m}-1)}$, $\mathrm{C}_{00\cdots10}$, $\mathrm{C}_{00\cdots11}$, $\cdots$, $\mathrm{C}_{00\cdots1D_1}$, $\cdots$, $\mathrm{C}_{00\cdots1(\sqrt[n_d]{m}-2)}$, $\mathrm{C}_{00\cdots1(\sqrt[n_d]{m}-1)}$, $\cdots$, $\mathrm{C}_{00\cdots D_20}$, $\mathrm{C}_{00\cdots D_21}$, $\cdots$, $\mathrm{C}_{00\cdots D_2D_1}$, $\cdots$, $\mathrm{C}_{00\cdots D_2(\sqrt[n_d]{m}-2)}$, $\mathrm{C}_{00\cdots D_2(\sqrt[n_d]{m}-1)}$, $\cdots$, $\mathrm{C}_{00\cdots(\sqrt[n_d]{m}-1)0}$, $\mathrm{C}_{00\cdots(\sqrt[n_d]{m}-1)1}$, $\cdots$, $\mathrm{C}_{00\cdots(\sqrt[n_d]{m}-1)D_1}$, $\cdots$, $\mathrm{C}_{00\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-2)}$, $\mathrm{C}_{00\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$, $\cdots$, $\mathrm{C}_{0(\sqrt[n_d]{m}-1)\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$, $\cdots$, $\mathrm{C}_{(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)\cdots(\sqrt[n_d]{m}-1)(\sqrt[n_d]{m}-1)}$ .Where, $D_1 = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$, $D_2 = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$, $\cdots$, $D_{n_d-1} = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$ and $D_{n_d} = 0,1,\cdots,\left(\sqrt[n_d]{m}-2\right),\left(\sqrt[n_d]{m}-1\right)$. The sensor nodes in group $\mathrm{C}'_{D_1D_2\cdots D_{n_d-1}D_{n_d}}$ are deployed in cell $\mathrm{C}_{D_1D_2\cdots D_{n_d-1}D_{n_d}}$. Prior to the deployment, the key setup server forms the logical groups and then distributes a bit cluster group to each of them. There are $\left(\sqrt[n_d]{m}-1\right)^{n_d}$ logical groups denoted as $\mathrm{G}_{00\cdots00}$, $\mathrm{G}_{00\cdots01}$, $\cdots$, $\mathrm{G}_{00\cdots0D_1}$, $\cdots$, $\mathrm{G}_{00\cdots0(\sqrt[n_d]{m}-3)}$, $\mathrm{G}_{00\cdots0(\sqrt[n_d]{m}-2)}$, $\mathrm{G}_{00\cdots10}$, $\mathrm{G}_{00\cdots11}$, $\cdots$, $\mathrm{G}_{00\cdots1D_1}$, $\cdots$, $\mathrm{G}_{00\cdots1(\sqrt[n_d]{m}-3)}$, $\mathrm{G}_{00\cdots1(\sqrt[n_d]{m}-2)}$, $\cdots$, $\mathrm{G}_{00\cdots D_20}$, $\mathrm{G}_{00\cdots D_21}$, $\cdots$, $\mathrm{G}_{00\cdots D_2D_1}$, $\cdots$, $\mathrm{G}_{00\cdots D_2(\sqrt[n_d]{m}-3)}$, $\mathrm{G}_{00\cdots D_2(\sqrt[n_d]{m}-2)}$, $\cdots$, $\mathrm{G}_{00\cdots(\sqrt[n_d]{m}-2)0}$, $\mathrm{G}_{00\cdots(\sqrt[n_d]{m}-2)1}$, $\cdots$, $\mathrm{G}_{00\cdots(\sqrt[n_d]{m}-2)D_1}$, $\cdots$, $\mathrm{G}_{00\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-3)}$, $\mathrm{G}_{00\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)}$, $\cdots$, $\mathrm{G}_{0(\sqrt[n_d]{m}-2)\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)}$, $\cdots$, $\mathrm{G}_{(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)\cdots(\sqrt[n_d]{m}-2)(\sqrt[n_d]{m}-2)}$. Where, $D_1 = 0,1,\cdots,\left(\sqrt[n_d]{m}-3\right),\left(\sqrt[n_d]{m}-2\right)$, $D_2 = 0,1,\cdots,\left(\sqrt[n_d]{m}-3\right),\left(\sqrt[n_d]{m}-2\right)$, $\cdots$, $D_{n_d-1} = 0,1,\cdots,\left(\sqrt[n_d]{m}-3\right),\left(\sqrt[n_d]{m}-2\right)$

and $D_{n_d} = 0,1, \cdots, \left(\sqrt[n_d]{m}-3\right), \left(\sqrt[n_d]{m}-2\right)$, each of which consists of 2^{n_d} cells. Therefore, each logical group $G_{D_1 D_2 \cdots D_{n_d-1} D_{n_d}}$ has $\frac{2^{n_d} N}{m}$ sensor nodes.

Pairwise key establishment.

We introduce the grid-based key predistribution scheme in [4]. In our strategy we form $2\sqrt[n_d]{\frac{N}{m}} \times 2\sqrt[n_d]{\frac{N}{m}} \times \cdots \times 2\sqrt[n_d]{\frac{N}{m}}$ hyper grid denoted by a n_d-dimension hyper coordinate system in the logical group $G_{D_1 D_2 \cdots D_{n_d-1} D_{n_d}}$. In the hyper coordinate system, those hyper axes are bit clusters $\mathrm{GID}_{D_1}, \mathrm{GID}_{D_2}, \cdots, \mathrm{GID}_{D_{n_d-1}}$ and $\mathrm{GID}_{D_{n_d}}$. Each of bit clusters GID_{D_1} includes $2\sqrt[n_d]{\frac{N}{m}}$ sub bit clusters denoted as $\mathrm{GID}_{D_1} \| \mathrm{NID}_{D_1^{'}}$, where, $D_1^{'} = 0,1,\cdots,\left(2\sqrt[n_d]{\frac{N}{m}}-2\right), \left(2\sqrt[n_d]{\frac{N}{m}}-1\right)$. In hyper axis GID_{D_1}, $0,1,\cdots,\left(2\sqrt[n_d]{\frac{N}{m}}-2\right), \left(2\sqrt[n_d]{\frac{N}{m}}-1\right)$ denote $\mathrm{GID}_{D_1} \| \mathrm{NID}_0$, $\mathrm{GID}_{D_1} \| \mathrm{NID}_1$, … , $\mathrm{GID}_{D_1} \| \mathrm{NID}_{2\sqrt[n_d]{\frac{N}{m}}-2}$, $\mathrm{GID}_{D_1} \| \mathrm{NID}_{2\sqrt[n_d]{\frac{N}{m}}-1}$ respectively. In the same way, for those hyper axes $\mathrm{GID}_{D_2}, \cdots, \mathrm{GID}_{D_{n_d-1}}$ and $\mathrm{GID}_{D_{n_d}}$ there are similar results. In logical group $G_{D_1 D_2 \cdots D_{n_d-1} D_{n_d}}$, 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 sensor node, where ID is the hyper grid-based index of the node. 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 paper assumes all sensor nodes in the logical group $G_{D_1 D_2 \cdots D_{n_d-1} D_{n_d}}$ are at the intersections. It is clear that different nodes at different intersections have different hyper grid-based indexes. The setup server then 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.

Suppose node S_0 is in the logical group $G_{D_1 D_2 \cdots D_{n_d-1} D_{n_d}}$ 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 deployment of nodes, node S_0 broadcasts its message $\left\{\left\langle D_{1_{S_0}}^{'}, D_{2_{S_0}}^{'}, \cdots, D_{(n_d-1)_{S_0}}^{'}, D_{(n_d)_{S_0}}^{'} \right\rangle, \mathrm{GID}_{D_1} \| \mathrm{NID}_{D_{1_{S_0}}^{'}}, \mathrm{GID}_{D_2} \| \mathrm{NID}_{D_{2_{S_0}}^{'}}, \cdots, \mathrm{GID}_{D_{(n_d-1)}} \| \mathrm{NID}_{D_{(n_d-1)_{S_0}}^{'}}, \mathrm{GID}_{D_{n_d}} \| \mathrm{NID}_{D_{(n_d)_{S_0}}^{'}}\right\}$ 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 $D_1^{'}$. For the $\mathrm{GID}_{D_2} \| \mathrm{NID}_{D_{2_{S_0}}^{'}}, \cdots, \mathrm{GID}_{D_{(n_d-1)}} \| \mathrm{NID}_{D_{(n_d-1)_{S_0}}^{'}}, \mathrm{GID}_{D_{n_d}} \| \mathrm{NID}_{D_{(n_d)_{S_0}}^{'}}$, there are similar results.

The new communication connection key $K_{S_0 S_1}^{D_1}$ between S_0 and one node S_1, which have common sub bit cluster $\mathrm{GID}_{D_1} \| \mathrm{NID}_{D_{1_{S_0}}^{'}}$, is generated as follow.

$$K_{S_0 S_1}^{D_1} = \mathrm{hash}\left\{(\mathrm{GID}_{D_1} \| \mathrm{NID}_{D_{1_{S_0}}^{'}}) \oplus \left\langle D_{1_{S_0}}^{'}, D_{2_{S_0}}^{'}, \cdots, D_{(n_d-1)_{S_0}}^{'}, D_{(n_d)_{S_0}}^{'} \right\rangle \oplus \left\langle D_{1_{S_1}}^{'}, D_{2_{S_1}}^{'}, \cdots, D_{(n_d-1)_{S_1}}^{'}, D_{(n_d)_{S_1}}^{'} \right\rangle\right\} \quad (1)$$

where $D_{1_{S_0}}^{'} = D_{1_{S_1}}^{'}$.

We can obtain $K_{S_0S_1}^{D_2},\cdots,K_{S_0S_1}^{D_{(n_d-1)}},K_{S_0S_1}^{D_{n_d}}$ through utilizing formulas similar to formula (1).

$K_{S_0S_1}^{D_1},K_{S_0S_1}^{D_2},\cdots,K_{S_0S_1}^{D_{(n_d-1)}}$ and $K_{S_0S_1}^{D_{n_d}}$ are computed through using exclusive OR based on digit in hash functions, so they are computed rapidly.

In general, the sensor node U in the logical group $\mathrm{G}_{D_1D_2\cdots D_{n_d-1}D_{n_d}}$ can establish a pairwise key with any other sensor node V in the same logical group according to the overlap key sharing concept. If the node U and V share one or more one of $\mathrm{GID}_{D_1}\|\mathrm{NID}_{D_1^{'}},\mathrm{GID}_{D_2}\|\mathrm{NID}_{D_2^{'}},\cdots,$ $\mathrm{GID}_{D_{n_d-1}}\|\mathrm{NID}_{D_{n_d-1}^{'}},\mathrm{GID}_{D_{n_d}}\|\mathrm{NID}_{D_{n_d}^{'}}$, the two nodes can directly establish a pairwise key. If the two nodes share nothing, they also can establish pairwise keys through $n_d!$ midway nodes. Therefore, we can obtain $n_d!$ communication connection keys between U and V.

Addition of new nodes.

If a sensor node $S_{h^{'}}$ will be added to the logical group $\mathrm{G}_{D_1D_2\cdots D_{n_d-1}D_{n_d}}$, the setup server randomly distributes an ID denoted as $\left\langle(2^{n_d}\sqrt{\frac{N}{m}}+D_{1_{add}}^{'})_{S_{h^{'}}},(2^{n_d}\sqrt{\frac{N}{m}}+D_{2_{add}}^{'})_{S_{h^{'}}},\cdots,(2^{n_d}\sqrt{\frac{N}{m}}+D_{(n_d-1)_{add}}^{'})_{S_{h^{'}}},\right.$ $\left.(2^{n_d}\sqrt{\frac{N}{m}}+D_{(n_d)_{add}}^{'})_{S_{h^{'}}}\right\rangle$ and n_d sub bit clusters $\mathrm{GID}_{D_1}\|\mathrm{NID}_{D_1^{'}},\mathrm{GID}_{D_2}\|\mathrm{NID}_{D_2^{'}},\cdots,\mathrm{GID}_{D_{n_d-1}}\|\mathrm{NID}_{D_{n_d-1}^{'}},$ $\mathrm{GID}_{D_{n_d}}\|\mathrm{NID}_{D_{n_d}^{'}}$ to $S_{h^{'}}$, where $\left\langle(2^{n_d}\sqrt{\frac{N}{m}}+D_{1_{add}}^{'})_{S_{h^{'}}},(2^{n_d}\sqrt{\frac{N}{m}}+D_{2_{add}}^{'})_{S_{h^{'}}},\cdots,(2^{n_d}\sqrt{\frac{N}{m}}+D_{(n_d-1)_{add}}^{'})_{S_{h^{'}}},D_{(n_d-1)_{add}}^{'})_{S_{h^{'}}},\right.$ $\left.(2^{n_d}\sqrt{\frac{N}{m}}+D_{(n_d)_{add}}^{'})_{S_{h^{'}}}\right\rangle\neq\left\langle(D_1^{'})_{S_h},(D_2^{'})_{S_h},\cdots,(D_{n_d-1}^{'})_{S_h},(D_{n_d}^{'})_{S_h}\right\rangle$, $0\le h\le 2^{n_d}\sqrt{\frac{N}{m}}-1$, $D_{1_{add}}^{'}=0,1,2,\cdots$, $D_{1_{add}}^{'}=0,1,2,\cdots$, $D_{2_{add}}^{'}=0,1,2,\cdots$, $D_{(n_d-1)_{add}}^{'}=1,2,\cdots$ and $D_{(n_d)_{add}}^{'}=1,2,\cdots$. After added to $\mathrm{G}_{D_1D_2\cdots D_{n_d-1}D_{n_d}}$, $S_{h^{'}}$ broadcasts a message $\left\{\left\langle(2^{n_d}\sqrt{\frac{N}{m}}+D_{1_{add}}^{'})_{S_{h^{'}}},(2^{n_d}\sqrt{\frac{N}{m}}+D_{2_{add}}^{'})_{S_{h^{'}}},\cdots,(2^{n_d}\sqrt{\frac{N}{m}}+D_{(n_d-1)_{add}}^{'})_{S_{h^{'}}},(2^{n_d}\sqrt{\frac{N}{m}}+D_{(n_d)_{add}}^{'})_{S_{h^{'}}}\right\rangle\right.$ $\left.\mathrm{GID}_{D_1}\|\mathrm{NID}_{D_1^{'}},\mathrm{GID}_{D_2}\|\mathrm{NID}_{D_2^{'}},\cdots,\mathrm{GID}_{D_{n_d-1}}\|\mathrm{NID}_{D_{n_d-1}^{'}},\mathrm{GID}_{D_{n_d}}\|\mathrm{NID}_{D_{n_d}^{'}}\right\}$ to other nodes.

The communication connection $K_{S_{h^{'}}S_h}^{D_1}$ between $S_{h^{'}}$ and S_h, $0\le h\le 2^{n_d}\sqrt{\frac{N}{m}}-1$, which have common sub bit cluster $\mathrm{GID}_{D_1}\|\mathrm{NID}_{D_1^{'}}$, is generated by the common section as follow

$$K_{S_{h^{'}}S_h}^{D_1}=\mathrm{hash}\left\{(\mathrm{GID}_{D_1}\|\mathrm{NID}_{D_1^{'}})\oplus\left\langle(2^{n_d}\sqrt{\frac{N}{m}}+D_{1_{add}}^{'})_{S_{h^{'}}},(2^{n_d}\sqrt{\frac{N}{m}}+D_{2_{add}}^{'})_{S_{h^{'}}},\cdots,(2^{n_d}\sqrt{\frac{N}{m}}+D_{(n_d-1)_{add}}^{'})_{S_{h^{'}}},(2^{n_d}\sqrt{\frac{N}{m}}+D_{(n_d)_{add}}^{'})_{S_{h^{'}}}\right\rangle\right.$$
$$\left.\oplus\left\langle(D_1^{'})_{S_h},(D_2^{'})_{S_h},\cdots,(D_{n_d-1}^{'})_{S_h},(D_{n_d}^{'})_{S_h}\right\rangle\right\}\qquad(2)$$

where $D_1^{'}=(D_1^{'})_{S_h}$.

We can obtain $K_{S_{h^{'}}S_h}^{D_2},\cdots,K_{S_{h^{'}}S_h}^{D_{(n_d-1)}},K_{S_{h^{'}}S_h}^{D_{n_d}}$ through utilizing formulas similar to formula (2).

Eviction of nodes.

In wireless sensor network, nodes inevitably are compromised, or, they deplete their energy, so those nodes are deleted in time to guarantee network security. Our scheme can delete those nodes and refresh related keys. According those formulas (1) and (2), new pairwise keys are generated among normal nodes through deleting the indexes of the compromised nodes and their sub bit clusters. Therefore, this scheme realizes key refreshment.

Performance analysis for WSNs

The connectivity in WSNs.

As discussion above, any two sensor node U and V in the same logical group can establish their pairwise keys through using the overlap key sharing concept. Our strategy can guarantee any two sensor node U_0 and U_2, which are not in the same logical group, establish pairwise keys. The minimal number of logical groups between U_0 and U_2 is i. Therefore, U_0 and U_2 can establish $(n_d!)^{i+1}$ pairwise key establishment paths.

Security analysis for WSNs.

$(n_d!)^{i+1}$ random keys, $K_1, K_2, , \cdots, K_{(n_d!)^{i+1}-1}$ and $K_{(n_d!)^{i+1}}$, between node U_0 and U_2 are generated and they are utilized as the pairwise keys between them. The nodes outside the key discovery paths cannot obtain those keys, because it is transmitted through secure connection. Additionally, in this scheme the pairwise keys among sensor nodes still can be established with high probability, even if some sensor nodes are compromised. Therefore, this strategy is resilient to node compromise. According to the concept of the q-composite key pre-distribution scheme in paper [5], our scheme may require node U_0 and U_2 sharing one or more one of $K_1, K_2, , \cdots, K_{(n_d!)^{i+1}-1}$ and $K_{(n_d!)^{i+1}}$ to realize their secure communication. Therefore, this scheme can realize flexible secure grades for wireless sensor networks. Additionally, the pairwise keys in the nodes are generated by using hash functions, therefore, compromised nodes do not reveal pairwise keys in other nodes even though they probably lose their key.

The sub bit clusters stored in nodes determine all the nodes, which can establish pairwise keys with them, so the node replication does not increase other pairwise nodes, and then captures more pairwise keys. This scheme is secure to node replication attacker.

This scheme divides sensing hypercube into small hypercube cells and logical groups and nodes in different logical groups have different bit clusters, so bit clusters are distributed unevenly in entire sensing hypercube. When attackers randomly compromise different nodes without special target, they capture a certain bit cluster with low probability.

Conclusion

The scheme in this paper combines overlap sharing key scheme and the key management strategy based on cells and logical groups. The sensing hypercube is divided into a number of cells and logical groups with same dimension. The sensor nodes are distributed sub bit clusters and establish their pairwise keys through using the OKS concept. This scheme is resilient to compromised node attack, has good network connectivity, and provides flexible security grades for wireless sensor networks.

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] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, J.D. Tygar. “SPINS: security protocols for sensor networks”, In: Proceedings of the 7th annual ACM/IEEE international conference on mobile computing and networking, July 2001, pp.189-199, (2001).

[2] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in Proc. CCS’02: 9th ACM Conference on Computer and Communications Security. New York: ACM Press, Nov. 2002, pp.41-47, (2002).

[3] 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).

[4] D. Liu, P. Ning, “Location-based pairwise key establishments for static sensor networks”, in: ACM Workshop on Security in Ad Hoc and Sensor networks (SASN’03), pp.72-82, (2003).

[5] H. Chan, A. Perrig, D. Song. “Random key predistribution schemes for sensor networks”, Proceedings of the IEEE Syrup. On Research in Security and Privacy, Berkeley, CA, USA, May 11-14 2003, pp.197-213, (2003).