A SECURE SCHEME FOR HETEROGENEOUS WIRELESS SENSOR NETWORKS

[1]YUQUAN ZHANG
[1]Lecturer, School of Information Technology, Shandong Women's University, Jinan, China
E-mail: [1]zyczyq@126.com

ABSTRACT

A secure scheme for heterogeneous wireless sensor networks is presented. The wireless sensor networks have some sensor nodes and heterogeneous sensor nodes that have greater power and transmission capability than other nodes have. All kinds of sensor nodes are evenly distributed respectively in entire sensing area that is divided into a number of same cells and logical groups evenly. The pairwise keys between nodes including all kinds of nodes are set up through employing the concept of the overlap key sharing, the grid-based key predistribution scheme, and the random key predistribution scheme. The two-dimensional sensing square is divided into a number of small squares called cells, four of which are comprised of a cluster called logical group for class 1 nodes. Analysis shows that both the security and the connectivity of wireless sensor networks have been enhanced evidently with some heterogeneous nodes.

Keywords: *Heterogeneous Wireless Sensor Networks, Security, Connectivity, OKS*

1. INTRODUCTION

The recent advances in wireless communications, integrated electronics, and microelectromechanical systems (MEMS) technology have facilitated the development of wireless sensor networks[1]. A wireless sensor network can be considered a especial type of ad hoc network composed by a large number of tiny, cheap and highly resource constrained sensor nodes, known as motes[2]. Typically, a sensor node is a tiny device that includes three basic components: a sensing subsystem for data acquisition from the physical surrounding environment, a processing subsystem for local data processing and storage, and a wireless communication subsystem for data transmission. All sensor nodes have constraints on resource, including energy, memory, computation speed, and bandwidth because of their constraints on size and cost.

Wireless sensor networks have received tremendous attention in recent years because of their potential various applications in many fields, such as healthcare[3], greenhouse monitoring[4], and forest fires and plant fires monitoring[5] etc.

The unique constraints of sensor nodes and the requirements of wireless sensor networks have spurred considerable investigation into the security issue for wireless sensor network.

As an important issue for WSNs security, key management has been investigated widely and some approaches have been proposed for wireless sensor networks. Eschenauer and Gligor[6] introduced a probabilistic key pre-distribution scheme recently for key establishment. The chief idea is to let each sensor node randomly picks a set of keys from a key pool before deployment so that any two sensor nodes have a certain probability to share at least one common key. The strategy has further been improved by Chan et al[7], namely, a q-composite key pre-distribution scheme a random pairwise key scheme. The q-composite key pre-distribution also uses a key pool but requires two nodes compute a pairwise key from at least q pre-distributed keys that they share. The random pairwise key scheme randomly picks pairs of sensor nodes and assigns each pair a unique random key. Both schemes improve the security over the basic probabilistic key pre-distribution scheme. But, they can not scale to large sensor networks. [8] and [9] are proposed as extensions of the scheme in [6] to make it even more secure and reliable. [10] presented peer intermediaries for key establishment in sensor network called "PIKE". In this scheme, the key establishment between two sensor nodes is based on the common trust of a third node. For any two nodes of A and B, there is a node C that shares a key with both A and B simultaneously. D. Liu and P. Ning[11] ensured that two nodes set up their key through using the grid-based key predistribution scheme. Cungang Yang, Celia Li, Jie Xiao[12] guarantee that any two nodes establish their pairwise key in the case there are no compromised node. In addition, Lai D et al.[13] presented the OKS (Overlap-Key-Sharing) protocol. The scheme generates a long bit-string to be the key-string-pool (KP) of the sensor network, and randomly assigns a subset of the key-string-pool to be the key-string stored in each sensor. Sensors in OKS protocol use the overlap intervals (number of bits overlapping between neighbors) of the key-strings as the shared secret key with their neighbor nodes.

This paper proposes a secure key management strategy for heterogeneous wireless sensor networks through utilizing the random key predistribution scheme, the overlap key sharing (OKS) concept, the grid-based key predistribution scheme, and dividing sensing area into two-dimensional clusters. The scheme investigates how the heterogeneous nodes affect the distributed wireless sensor networks. The overlap key sharing protocol creates long bit clusters as the key cluster pools and randomly distributes a sub-group to store every sensor as key cluster. The two-dimensional sensing square is divided into a number of small same squares called cells. In a certain cell, there are some class 0 nodes and a class 1 node, and all class 0 nodes are evenly distributed 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. In a certain logical group, the setup server generates and then distributes keys to all class 1 nodes to guarantee that any two class 1 nodes can establish a pairwise key. Analysis and comparison demonstrated in this strategy heterogeneous nodes improve the resilience of HWSNs, and enhance the network connectivity.

The rest of this paper is organized as follows. In section two, the distributed key management scheme for WSNs with heterogeneous nodes is given. The scheme contains classes of nodes, key generation and distribution for all kinds of nodes, location-based grids, and pair-wise key establishment among all kinds of nodes. The section three discusses the performance for wireless heterogeneous sensor network. The conclusion of this paper is in section four.

2. DISTRIBUTED KEY MANAGEMENT SCHEME

In this paper, I present a key management strategy in distributed peer-to-peer wireless sensor networks that are composed of heterogeneous sensor nodes. The scheme can be described in detail as follows.

2.1 Classes Of Nodes

We propose that there are I classes of sensor nodes in the WSNs, with Class 0 being the least powerful nodes, and Class $I-1$ the most powerful nodes, in terms of their power. Particularly, we make some assumptions.

(1) There are bi-directional links among sensor nodes.

(2) Let r_i ($0 \le i \le I-1$) denotes the communication range of class i nodes, we always have $r_{i_1} < r_{i_2}$ if $i_1 < i_2$.

Where, in this paper, we let $I = 2.$

We ought to differ the heterogeneous WSNs from the hierarchical WSNs. In the former, the communications among all different classes of nodes are still on distributed peer-peer basis, although the higher class nodes have more powerful computing processing capacity, communication capacity, and energy than the lower ones. On the other hand, in the latter, the clusters (or the base stations) are centralized nodes.

2.2 Key Generation And Distribution

The key generation of the heterogeneous distributed wireless sensor networks is based on the random key distributions, the grid-based key predistribution scheme, 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 and employs 2 m_k t -degree bivariate polynomials as the key pool for all class 1 nodes in each logical group.

For all kinds of nodes in each cell, one of the challenging tasks in this strategy is how to distribute bit-string shares into different classes of nodes, we will firstly deal with the issue in this section.

Firstly, we divide equally the classes of sensor nodes into J groups, denoted as C'_{00} , $\cdots$, $\mathrm{C}'_{0j'}$, $\cdots$ $\mathrm{C}'_{0J'}$, 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 $J = I'(J'+1) + J'+1$. An 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, the setup server generates I long bit-strings, where a unique key pool ID i is assigned to each long bit-string, denoted as 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 of sensor nodes, the combination of S_0 and S_1, denoted as Ω_1, as the key-string-pool for 1 class of sensor nodes and so on. In this paper, we let $I=2$.

Thirdly, a subset of those key-string-pools, denoted as Ω_{ij}, can be created for nodes in class i and group j. Particularly, we let

$$\Omega_{ij}=\bigcup_{k=0}^{i}\Omega_{ij}(k), \qquad (1)$$

Where $\Omega_{ij}(0)\subseteq\Omega_0,\Omega_{ij}(1)\subseteq\Omega_1$, $\Omega_{ij}(2)\subseteq\Omega_2,\cdots,\Omega_{ij}(k)\subseteq\Omega_k$, namely, $\Omega_{ij}(k)$ is a subset of the key-string-pool that is selected from Ω_k.

From (1), we can see that in group j, two classes i_1 and i_2 ($i_1<i_2$) will be able to share some common bit-strings if there exists k_1, k_2 ($k_1\le i_1<i_2$) ($k_2\le i_1<i_2$) such that

$$\Omega_{i_1 j}(k_1)\bigcap\Omega_{i_2 j}(k_2)\neq\varnothing \qquad (2)$$

Where $\Omega_{i_1 j}(0)\subset\Omega_0,\Omega_{i_1 j}(1)\subset\Omega_1$, $\Omega_{i_1 j}(2)\subset\Omega_2,\cdots,\Omega_{i_1 j}(k_1)\subset\Omega_{k_1}$, namely $\Omega_{i_1 j}(k_1)\subset\Omega_{k_1};\Omega_{i_2 j}(0)\subset\Omega_0,\Omega_{i_2 j}(1)\subset\Omega_1$, $\Omega_{i_2 j}(2)\subset\Omega_2,\cdots,\Omega_{i_2 j}(k_2)\subset\Omega_{k_2}$, namely $\Omega_{i_2 j}(k_2)\subset\Omega_{k_2}$.

In this paper, two classes 0 and 1 in the same group will be able to share some common bit-strings if

$$\Omega_{0j}(0)\bigcap\Omega_{1j}(0)\neq\varnothing \qquad (3)$$

Where $\Omega_{0j}(0)\subset\Omega_0$ and $\Omega_{1j}(0)\subset\Omega_0$.

Similarly, for the same class i, nodes in two different groups $j_1\neq j_2$ will be able to share common bit-strings if there exists two different k_1 and k_2 ($k_1\le i$) ($k_2\le i$) such that

$$\Omega_{ij_1}(k_1)\bigcap\Omega_{ij_2}(k_2)\neq\varnothing \qquad (4)$$

Where $\Omega_{ij_1}(0)\subset\Omega_0,\Omega_{ij_1}(1)\subset\Omega_1$, $\Omega_{ij_1}(2)\subset\Omega_2,\cdots,\Omega_{ij_1}(k_1)\subset\Omega_{k_1}$, namely $\Omega_{ij_1}(k_1)\subset\Omega_{k_1};\Omega_{ij_2}(0)\subset\Omega_0,\Omega_{ij_2}(1)\subset\Omega_1$, $\Omega_{ij_2}(2)\subset C_2,\cdots,\Omega_{ij_2}(k_2)\subset\Omega_{k_2}$, namely $\Omega_{ij_2}(k_2)\subset\Omega_{k_2}$.

In this paper, class 0 nodes in different groups share nothing, 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 some common keys, namely, $\Omega_{1j_1}(k_1)\bigcap\Omega_{1j_2}(k_2)\neq\varnothing$, where $\Omega_{1j_1}(0)\subset\Omega_0$, $\Omega_{1j_1}(1)\subset\Omega_1$, $\Omega_{1j_2}(0)\subset\Omega_0$, $\Omega_{1j_2}(1)\subset\Omega_1$.

At last, the setup server picks up a subset of key-strings, denoted as Φ_{ij}^n ($\Phi_{ij}^n\subseteq\Omega_{ij}$) for a node n in class i and group j, and then assigns the key-string shares of these key-strings to the node.

2.3 Location-Based grids

In Fig. 1, The sensor area S_{area} is divided into $(I'+1)(J'+1)$ same cells, denoted as C_{00}, C_{01}, $\cdots$, $\mathrm{C}_{0j'}$, $\cdots$, $\mathrm{C}_{0(J'\text{-}1)}$, $\mathrm{C}_{0J'}$, C_{10}, C_{11}, $\cdots$ $\mathrm{C}_{1j'}$, $\cdots$, $\mathrm{C}_{1(J'\text{-}1)}$, $\mathrm{C}_{1J'}$, $\cdots$, $\mathrm{C}_{i'0}$, $\mathrm{C}_{i'1}$, $\cdots$, $\mathrm{C}_{i'j'}$, $\cdots$, $\mathrm{C}_{i'(J'\text{-}1)}$, $\mathrm{C}_{i'J'}$, $\cdots$, $\mathrm{C}_{I'0}$, $\mathrm{C}_{I'1}$, $\cdots$, $\mathrm{C}_{I'j'}$, $\cdots$, $\mathrm{C}_{I'(J'\text{-}1)}$, $\mathrm{C}_{I'J'}$, where $0\le i'\le I'$ and $0\le j'\le J'$, according to their geographical locations. The sensor nodes in group $C'_{i'j'}$ are deployed in cell $C_{i'j'}$. A logical group consists of four cells. For example, in Fig. 1, cluster $G_{(I'-1)(J'-1)}$ consists of cell $C_{I'J'}$, $C_{I'(J'-1)}$, $C_{(I'-1)J'}$ and $C_{(I'-1)(J'-1)}$. If $I' = J'$, there are $(I'-1)^2 = (J'-1)^2$ logical groups.

Suppose that N_0 class 0 nodes are evenly distributed in each cell and a class 1 node is in the center of each cell.

2.4 Pair-Wise Key Establishment

To establish pair-wise keys between the sensor nodes, we also utilize the three steps, namely, initialization, direct key setup, and (optional) path key setup, as the previous papers did. Firstly, the initialization step is finished in a key setup center before the deployment of all the sensor nodes. The setup server distributes a subset of the key-string-pool to different sensor nodes. Secondly, any two sensor nodes try to establish a pair-wise key; of course, they always firstly attempt to do so via direct key establishment in a distributed peer-peer manner. 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. In this paper, the third step can be disabled because of the heterogeneity.

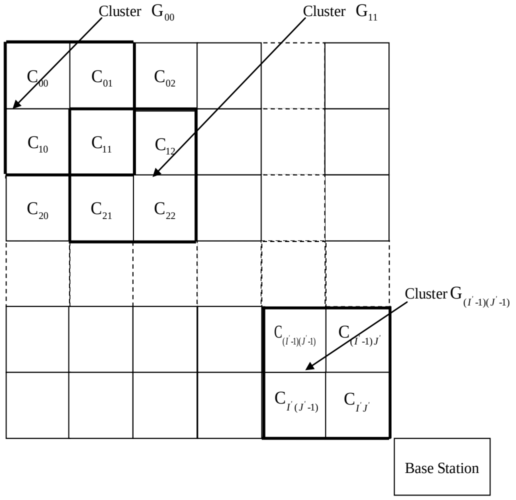

Figure 1. Location-Based Cells And Clusters

3. THE PERFORMANCE ANALYSIS FOR WIRELESS HETEROGENEOUS SENSOR NETWORK

3.1 The Importance Of Heterogeneous Nodes In Node Connectivity

In Fig.1, two kinds of nodes, class 0 nodes and class 1 nodes, are distributed evenly in the sensing area. Suppose that the cell is a a by a square, the communication range of class 0 nodes is $\frac{\sqrt{2}a}{2}$, and the communication range of class 1 nodes is $\sqrt{2}a$.

We investigate a WSN with heterogeneity that is utilized to collect data in a distributed peer-to-peer case. In this scenario, sensor nodes should transmit their observation to the base station via the wireless sensor network, as shown in Fig. 2, where there are two types of sensor nodes and there are four class 0 nodes, namely $N_0 = 4$, in each group. Obviously, lower class nodes employ the links between themselves and the higher-class nodes to transmit their observations because the higher nodes have a larger transmission range. For example, in Fig. 2, class 0 node A will tend to use the path “A-B-C-D-Base Station” to transmit its data, instead of sending the message by class 0 nodes (the dash line). The class 0 node A chooses the class 1 node B as it’s the first hop node, instead of using class 0 nodes, even though the class 0 node is closer than the class 1 node B. Next, the class 1 node B chooses the class 1 node C as the second hop node. Therefore, a higher class node will more likely be chosen as the next hop node candidate to relay data. The connection between a lower node and a higher node is more possible and more important than between two lower class nodes.

In this section, we present several analytical models to evaluate the connection performance of the key manage strategy, in which probability theoretical method will be utilized because we randomly generated or selected keys. From the above discussion, for simpleness, we consider a special key distribution scheme. In the case, there are two classes of the heterogeneous sensor nodes and there are *J* groups.

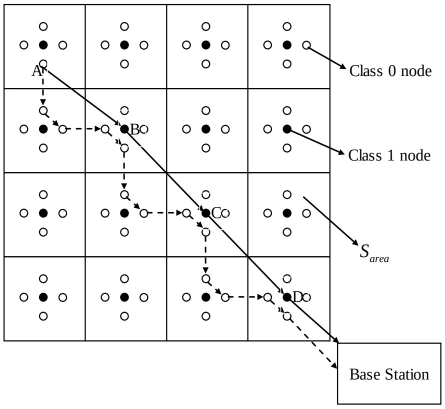

Figure 2. An Example For Wireless Heterogeneous Sensor Network

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 ($i = 1,2,\cdots,\text{I-}1$) 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 group, we calculate the probability, denoted as $p(\alpha)$, that a class 0 node shares α sub key-strings with a class 1 node as follows

$$p(\alpha) = \frac{\binom{S}{\alpha}\binom{S-\alpha}{P_0-\alpha}\binom{S-P_0}{P_1-\alpha}}{\binom{S}{P_0}\binom{S}{P_1}} \qquad (5)$$

Any a class 0 node and a class 1 node can establish secure connection if they share a key, therefore, the scheme can guarantee that the class 0 node and a class 1 node establish secure connection if $\sum_{1}^{P_0} p(\alpha) \geq 1$. We can obtain this result through choosing reasonable S , P_0 and P_1.

The setup server[11] randomly generates 2 m_k t -degree bivariate polynomials $F = \left\{ f_{i^c}^{c}(x,y), f_{i^c}^{r}(x,y) \right\}_{i^c=0,1,\ldots,m_k-1}$ over a finite field F_q for all class 1 nodes in each logical group, where $m_k = \sqrt{N_1}$, here N_1 is the total sensor node number in the group. Then, the setup server assigns $\left\{ ID, f_{i^c}^{c}(j^r,x), f_{j^r}^{r}(i^c,x) \right\}$ for each class 1 node where ID is the grid-based index of the class 1 node. The ID of the class 1 node at the intersection of column coordinate i^c and row coordinate j^r is denoted as $\left\langle i^c, j^r \right\rangle$ (see Fig.3).

Generally, there are two nodes S^1 and S^2 in a logical group which will establish a pairwise key. S^1 checks if $c_{S^1} = c_{S^2}$ or $r_{S^1} = r_{S^2}$ where c_{S^1} , c_{S^2} , r_{S^1} and r_{S^2} are the column and row coordinates of node S^1 and node S^2 respectively. If $c_{S^1} = c_{S^2}$ or $r_{S^1} = r_{S^2}$, node S^1 and node S^2 share common polynomial key $f_{c_{S^{1,2}}}^{c}(x,y)$ or $f_{r_{S^{1,2}}}^{r}(x,y)$ where $f_{c_{S^1}}^{c}(x,y) = f_{c_{S^2}}^{c}(x,y) = f_{c_{S^{1,2}}}^{c}(x,y)$, $f_{r_{S^1}}^{r}(x,y) = f_{r_{S^2}}^{r}(x,y) = f_{r_{S^{1,2}}}^{r}(x,y)$, they can directly establish a pairwise key by utilizing the polynomial-based key predistribution scheme. Otherwise, if $c_{S^1} \neq c_{S^2}$ and $r_{S^1} \neq r_{S^2}$, nodes S^1 and node S^2 can still establish pairwise key via

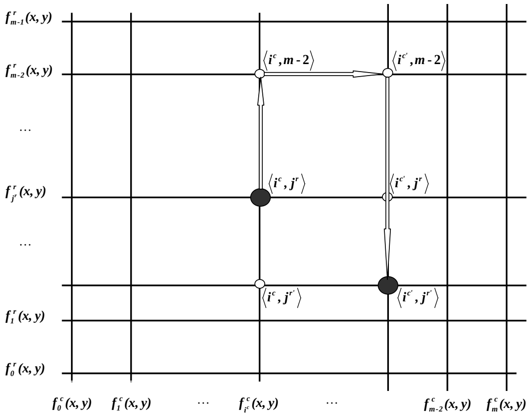
$f_{m-1}^{r}(x,y)$
$f_{m-2}^{r}(x,y)$
…
$f_{j^r}^{r}(x,y)$
…
$f_{1}^{r}(x,y)$
$f_{0}^{r}(x,y)$
$\left\langle i^c, m-2 \right\rangle$
$\left\langle i^{c'}, m-2 \right\rangle$
$\left\langle i^c, j^r \right\rangle$
$\left\langle i^{c'}, j^r \right\rangle$
$\left\langle i^c, j^{r'} \right\rangle$
$\left\langle i^{c'}, j^{r'} \right\rangle$
$f_{0}^{c}(x,y)$
$f_{1}^{c}(x,y)$
…
$f_{i^c}^{c}(x,y)$
…
$f_{m-2}^{c}(x,y)$
$f_{m}^{c}(x,y)$

Figure 3. Grid-Based Key Distribution

an intermediate node S^{12} with column c_{S^1} and row r_{S^2} or node S^{21} with column c_{S^2} and row r_{S^1}.

Obviously, the strategy guarantees that each pair of class 1 nodes can set up a pairwise key if the two sensors can communicate with each other and that the information can be sent to the base station safely. Additionally, in each cell, the class 1 nodes can establish a pairwise key with each of class 0 nodes. Therefore, our scheme guarantees that all nodes, including class 0 nodes and class 1 nodes are connective and can set up secure communication.

3.2 The Importance Of Heterogeneous Nodes In Information Security

We denote G_0 as the class 0 nodes and G_1 as 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 the 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 manner if the distance is larger than a threshold.

We give an example to illustrate this strategy in Fig. 4, 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* shares key $K1_i\,(i=0,1)$ with $X_i\ (i=0,1)$ respectively, similarly, node *A* shares key $K2_0$ and $K3_0$ with node Y_0. In this scenario, if node *A* sends messages to the sink node, certainly, it will firstly choose the key $K1_1$. If the distance from node *A* to node X_1 is larger then 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.

Generally, If a class 0 node is captured and compromised by enemy in a certain cell, it will not reveal any information of class 0 nodes in other cells, because it shares 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.

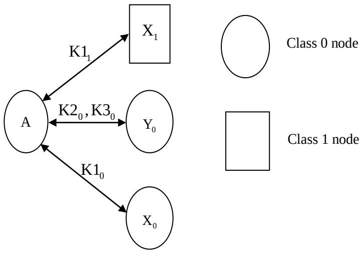

Figure 4. An Example In The Scheme

4. CONCLUSION

Key management is of importance to guarantee wireless sensor networks secure and it has been investigated recently. In most existing wireless sensor networks, however, all sensor nodes are assumed to have same capability. This paper research how heterogeneous nodes effect the performance including security and connectivity for WSNs. All kinds of sensor nodes are distributed evenly in sensing area that is divided into a number of same cells. For class 1 nodes, four of cells consist of a logical group. The pairwise keys between nodes including all kinds of nodes are established by employing the concept of the overlap key sharing, the grid-based key predistribution scheme, and the random key predistribution strategy. Analysis and comparison show some heterogeneous nodes improve both the security and connectivity effectively. Generally, it is difficult to improve the security and connectivity simultaneously in homogeneous wireless sensor networks, so this scheme deals with some WSNs limitations and has more applications including military and civilian fields.

REFRENCES:

[1] E. Callaway, P. Gorday, L. Hester, J. A. Gutiérrez, M. Naeve, B. Heile, and V. Bahl. Home networking with IEEE 802.15.4: a development standard for low-rate wireless

personal area networks. IEEE Communications Magazine, 2002, 40(8): 70-77.

[2] J. Yick, B. Mukherjee, D. Ghosal. Wireless sensor network survey. Computer Networks, 2008, 52(12): 2292-2330.

[3] J. Yoo, L Yan, S. Lee, Y. Kim, H.-J. Yoo. A 5.2 mw self-configured wearable body sensor network controller and a 12 w wirelessly powered sensor for a continuous health monitoring system. IEEE Journal of Solid-State Circuits, 2010, 45(1):178-188.

[4] M. Mancuso, F. Bustaffa. A Wireless Sensors Network for Monitoring Environmental Variables in a Tomato Greenhouse. at 6th IEEE International Workshop on Factory Communication Systems in Torino, Italy, June 28-30,2006, 2006, 107-110.

[5] A. S. Tanenhaum, C. Gamage, C. Crispo. Taking Sensor Networks from the Lab to the Jungle. IEEE Computer, 2006, 39(8):98-100.

[6] L. Eschenauer. 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, 41-47.

[7] H. Chan, A. Perrig, D. Song. Random key predistribution schemes for sensor networks. in Proc. IEEE Symposium on Research in Security and Privacy, May 2003, 197-213.

[8] P. Ning, R. Li, D. Liu, establishing pairwise keys in distributed sensor networks, ACM Transactions on Information and System Security, 2005, 8(1): 41-77.

[9] M.F. Younis, K. Ghumman, M. Eltoweissy, Location-aware combinatorial key management scheme for clustered sensor networks, IEEE Transactions on Parallel and Distributed Systems, 2006, 17(8): 865-882.

[10] H. Chan, A. Perrig. PIKE: peer intermediaries for key establishment in sensor networks. In: Proceedings of the 24th annual joint conference of the IEEE Computer and communications societies (INFOCOM’05), Miami, FL, USA, March 2005, 524-35.

[11] 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),2003,72-82.

[12] Y. Cungang, L. Celia, X. Jie. Location-based design for secure and efficient wireless sensor networks. Computer networks, 2008,52:3119-3129.

[13] 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, 351-356.