A Key Management Scheme for 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: Wireless sensor networks; heterogeneous; security; connectivity

Abstract. A key management strategy is presented for heterogeneous wireless sensor networks. The wireless sensor networks have some sensor nodes that are more powerful than other nodes. Both ordinary nodes and heterogeneous nodes are evenly distributed respectively in a sensing area that is divided into a number of same equilateral hexagons. The pairwise keys between nodes are established through utilizing the concept of the overlap key sharing and the random key pre-distribution scheme. Analysis demonstrates that the connectivity and security of wireless sensor networks have been improved obviously with some heterogeneous nodes.

1. Introduction

WSNs (Wireless sensor networks) consist of numerous sensors dispensed in various environments for monitoring environmental and physical phenomena[1]. Generally, the WSNs architectures can be organized into different categories according to different standards. Those architectures can be homogeneous, heterogeneous, hierarchical, distributed, etc[2]. In distributed wireless sensor networks, sensors employ pre-distributed keys which are generated by using keying materials[3]. In heterogeneous wireless sensor networks, sensors may have different capabilities, including computing ability, communication ranges, storages, etc[4].

WSNs are dispensed in hostile environments at times to finish some applications. Sensors have some limitations including low computing ability, limited storages, etc. Wireless sensor networks are likely to be attacked. Therefore, guaranteeing WSNs security is of importance.

Key management schemes are utilized to ensure wireless sensor networks secure. Lai D et al.[5] gave the Overlap-Key-Sharing protocol. The strategy generates a bit-string as the WSNs key-string-pool (KP), and randomly allocates its a subset as the key-string. It is stored in each sensor. The overlap intervals of the key-strings among sensors are their shared secret keys.

This paper presents a key scheme for heterogeneous distributed wireless sensor networks through using the idea in paper [5]. The rest of this paper is organized as follows. Section 2 gives the distributed key management strategy. The WSNs performance analysis is in section 3. The conclusion is in section 4.

2. Distributed key management strategy

2.1 Generating and distributing keys

Two class sensors, class 0 sensors and class 1 sensors, are distributed in the sensing area. The class 0 sensors are ordinary nodes and the class 1 sensors are more powerful than class 0 sensors in capacities including communication range, computing ability, etc. Assume that the links among sensors are bi-directional. Let r_i $(0 \le i \le 1)$ express the class i communication range. It is obvious that $r_0 < r_1$.

Through using the OKS protocol and the random key distribution, the key generation for

HDWSNs functions. This scheme utilizes a randomly generated long bit-string as the key pool for ordinary sensors and heterogeneous sensors.

Firstly, the classes of sensors are divided equally into J groups, namely $\mathrm{C}_0^{'}$, $\mathrm{C}_1^{'}$, $\cdots$, $\mathrm{C}_j^{'}$, $\cdots$, $\mathrm{C}_{J\text{-}2}^{'}$ and $\mathrm{C}_{J\text{-}1}^{'}$, where $0 \le j \le J-1$. A unique group ID j is assigned to each of all those groups.

Secondly, I long bit-strings, S_0, $S_1, \cdots, S_{I-2}, S_{I-1}$, are generated and a unique key pool ID i is assigned to each of them. We take S_0, denoted as Ω_0, as the key-string-pool of 0 class sensors, and the combination of S_0 and S_1, denoted as Ω_1, as the key-string-pool of 1 class sensor nodes, etc.

Thirdly, Ω_{ij}, a subset of those key-string-pools, can be created for nodes 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. Therefore, class i_1 and class i_2 $(i_1 < i_2)$ may share 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 $\Omega_{i_2 j}(k_2) \subset \Omega_{k_2}$.

There are two class sensors in this scheme. They may share some common bit-strings if $\Omega_{0j}(0) \bigcap \Omega_{1j}(0) \neq \varnothing$ exists, where $\Omega_{0j}(0) \subset \Omega_0$ and $\Omega_{1j}(0) \subset \Omega_0$. In the same way, for the same class i, sensors in two different groups j_1, j_2, $j_1 \neq j_2$, may share common bit-strings, if $\Omega_{ij_1}(k_1) \bigcap \Omega_{ij_2}(k_2) \neq \varnothing$ 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 strategy, $\Omega_{0j_1}(k_1) \bigcap \Omega_{0j_2}(k_2) = \varnothing$, where $\Omega_{0j_1}(0) \subset \Omega_0$, and $\Omega_{0j_2}(0) \subset \Omega_0$. Namely, class 0 sensors in different groups share nothing. Similarly, in this scheme, $\Omega_{1j_1}(k_1) \cap \Omega_{1j_2}(k_2) \neq \varnothing$, where $\Omega_{1j_1}(0) \subset \Omega_0$, $\Omega_{1j_1}(1) \subset \Omega_1$, $\Omega_{1j_2}(0) \subset \Omega_0$, $\Omega_{1j_2}(1) \subset \Omega_1$. Namely, class 1 nodes in different groups may share some common keys.

At last, the setup server chooses a subset of key-strings, Φ_{ij}^{n} ($\Phi_{ij}^{n} \subseteq \Omega_{ij}$), for a sensor n in class i and group j, and then allocates the sensor the key-string shares of these key-strings.

2.2 Location-based grids

In Fig.1, the sensing area, denoted as S_{area}, is divided into J same equilateral hexagon cells, C_0, C_1, $\cdots$, C_j, $\cdots$, $\mathrm{C}_{J\text{-}2}$ and $\mathrm{C}_{J\text{-}1}$, where $0 \le j \le J-1$. The sensor nodes located in $\mathrm{C}_I^{'}$ are dispensed in C_I. Assume that N_0 class 0 nodes locate in each cell evenly, and that a class 1 node locates in the cell center.

2.3 Establishing pair-wise keys

To set up pair-wise keys among sensor nodes, this scheme employs three phases including initialization, direct key setup, and (optional) path key setup. The first step is finished in a key setup center before all sensors, class 0 sensors and class 1 sensors, are distributed. The setup server allocates different sensor nodes a subset of the key-string-pool. In the second step, any two sensors attempt to set up a pair-wise key; obviously, they always first try to do so via direct key establishment by using a distributed peer-peer manner. If the second phase succeeds, the third phase is omitted. Otherwise, they start path key setup to set up a pair-wise key through using other nodes. In this strategy, the last step can be disabled because of the heterogeneity.

3. The HWSNs performance analysis

3.1 The function of heterogeneous nodes in network connectivity

In Fig.1, class 0 nodes and class 1 nodes are dispensed evenly in the sensing area. We make an assumption that the equilateral hexagon side length is a, the communication range of class 0 nodes is $\frac{\sqrt{3}\mathrm{a}}{2}$, and the communication range of class 1 nodes is $\sqrt{3}\mathrm{a}$.

This scheme utilizes heterogeneity to collect data in a distributed peer-to-peer case. Sensors transmit their observation to the base station through the HDWSNs, as shown in Fig. 2, where one class 1 node and six class 0 nodes locate in each group. 0 class nodes use the links between themselves and the 1 class nodes to forward their observations because the 1 class nodes have a larger transmission range than 0 class nodes. Therefore, in Fig. 2, class 0 node A tends to use the route “A-B-C-D-Base Station” to forward its data, instead of forwarding the data through class 0 nodes (the dash line). Node A selects the class 1 node B as it’s the first hop sensor, instead of employing class 0 nodes, even though the class 0 node is as near as the class 1. Next, the node B selects the class 1 node C as its second hop sensor. Therefore, a 1 class node is more likely to be chosen as the next hop sensor candidate to relay information. The path between a 0 class node and a 1 class node is more important than that between two 0 class nodes.

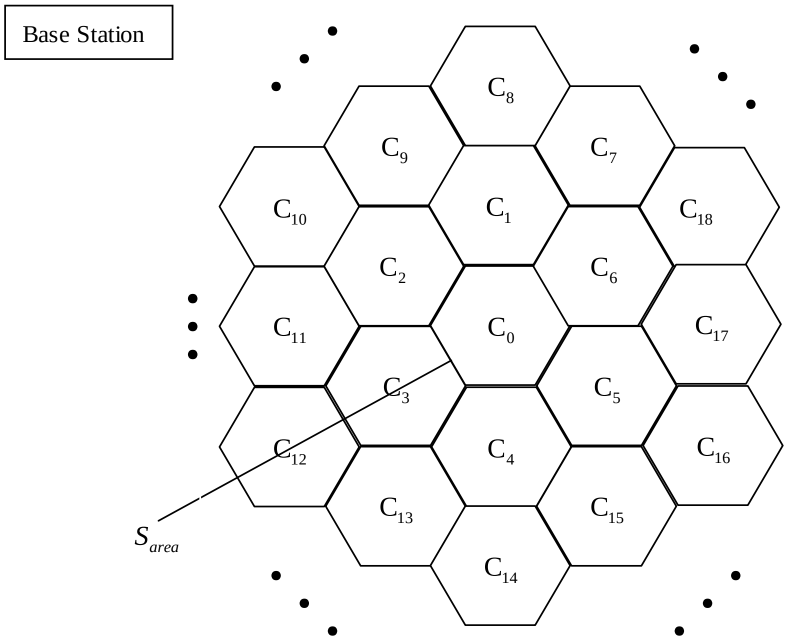

Fig.1 The hexagon sensing area

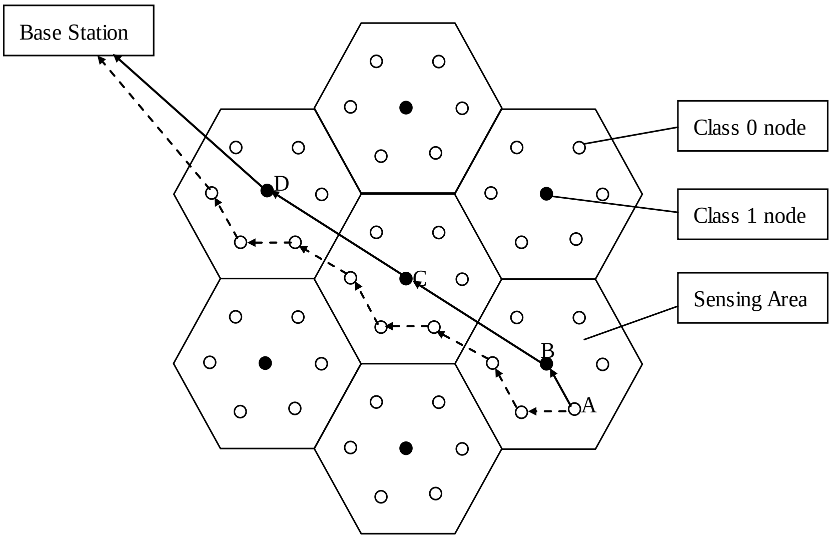

Fig.2 An example for wireless heterogeneous sensor network

This scheme presents several analytical models to evaluate the connection performance, in which probability theoretical methods are utilized because keys are randomly generated or selected. For simplicity, this paper discusses a special key distribution scheme in which there are two classes sensors and there are J groups.

All the key-string-pools for i ($i = 0,1,\cdots,I-1$) classes of sensors contain the S_0 and all the key-string-pools for i ($i = 1,2,\cdots,\mathrm{I}-1$) classes of sensors contain the S_0 and S_1, and so on. Therefore, the same subset of key-strings can create 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 sensor and each of the more powerful sensors.

We let $I = 2$ and S be the size of Ω_1. Assume that P_0 and P_1 are the numbers of subset of key-strings that can be stored in a class 0 sensor and a class 1 sensor respectively. In a certain group, the probability, $p(\alpha)$, that a class 0 sensor shares α sub key-strings with a class 1 sensor 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 connection if they share a key. Therefore, the scheme ensures that the class 0 sensor and a class 1 sensor set up secure connection if $\sum_{1}^{p_0} p(\alpha) \ge 1$. Through choosing reasonable S, P_0 and P_1, this result can be obtained.

We make an assumption that a class 1 sensor only can set up safe connection with those class 1 sensors which are the closest to it in different groups. For instance, in Fig.1, the class 1 sensor in C_0 only can set up safe connection with all class 1 nodes in $\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3, \mathrm{C}_4, \mathrm{C}_5$ and C_6. The probability, $p(\beta)$, that two class 1 nodes in different groups share β sub key-strings is calculated as follows

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

The scheme can assure that any two class 1 sensors set up safe connection if $\sum_{1}^{p_1} p(\beta) \ge 1$. We can get this result through selecting reasonable S and P_1.

From above discussion, the scheme guarantees that all sensors including class 0 sensors and class 1 sensors can set up secure 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.

3.2 The function of heterogeneous nodes in network security

Let G_0 denote the class 0 nodes and G_1 denote the class 1 nodes. A G_1 node is the neighborhood of a G_0 node which can accept a broadcast message directly transmitted from the G_1 node. In other word, the G_0 node gets bit-string pool messages transmitted by the G_1 on its own account. To simplify the topic, we suppose that a G_0 node can transmit data to any G_1 in its neighborhood through either a one-hop manner if the distance between them is small enough, or a multi-hop manner if the distance is larger than a threshold.

In Fig. 3, node A, X_0 and Y_0 are G_0 nodes, and node X_1 is a G_1 node. Node X_0, Y_0 and X_1 are the only neighbor sensors of the node A. In addition, sensor A shares key $\mathrm{K1}_i (i = 0,1)$ with X_i ($i = 0,1$) respectively, similarly, sensor A shares key $\mathrm{K2}_0$ and $\mathrm{K3}_0$ with nodes Y_0. If node A forwards data to the sink node, it will select the key $K1_1$ firstly. If the distance from A to X_1 is larger than a threshold, furthermore, in the path from A to X_1, there are compromised sensors, A will not connect with it. Similarly, A will try to link a class 0 node, X_0 or Y_0, until its message transmits to the sink node. It is clear that, in the WSNs with heterogeneous sensors, the communication is more resilient.

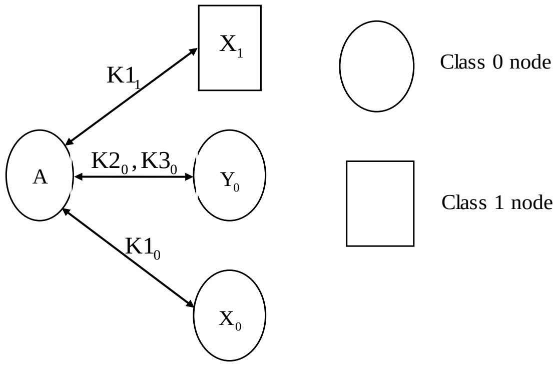

Fig.3 An example in the scheme

In general, if a class 0 node is attacked and compromised by opponents in a certain group, it will reveal no information of class 0 sensors in other groups, because it has no common key with them. Additionally, compromising the class 1 sensors in the same group is of difficulty because they are more powerful than class 0 nodes. Therefore, the scheme improves the security for WSNs.

4. The conclusion

As a topic in the security for WSNs, key management has been investigated recently. This paper investigates HWSNs in which some nodes are more powerful than other nodes. Ordinary nodes and heterogeneous nodes are dispensed evenly in sensing area which is divided into many groups evenly. The pairwise keys between nodes are set up through utilizing the concept of the overlap key sharing and the random key pre-distribution scheme. Analysis and comparison demonstrate that the connectivity and security of wireless sensor networks have been improved obviously with the help of some heterogeneous nodes.

References

[1] Tarek Alskaif, Manel Guerrero Zapata, Boris Bellalta. Game theory for energy efficiency in Wireless Sensor Networkss:Latest trends. Journal of Network and Computer Applications 54(2015) 33-61.

[2] 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.

[3] D. Liu, P. Ning, R. Li. Establishing. Pair-wise Keys in Distributed Sensor Networks. ACM Trans., Inf. Syst. Secur., 2005, 8(1):41-77.

[4] 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.

[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, 351-356.