A Secure Scheme Based on Three-Dimension Location for Hierarchical Wireless Heterogeneous Sensor Networks

Yuquan Zhang\textsuperscript{1,2,a}, Lei Wei\textsuperscript{3,b}

\textsuperscript{1}Shandong Women University, China
\textsuperscript{2}Wireless Sensing Institute, College of Information Science and Engineering, Qilu Normal University, China
\textsuperscript{3}College of Physics and Electronic Engineering, Qilu Normal University, China

\textsuperscript{a}email:zyczyq@126.com; \textsuperscript{b}email:weilei76@126.com

Keywords: Hierarchical wireless heterogeneous sensor network, two-layer, three-dimension, connectivity, lifetime

Abstract. A pairwise key establishment strategy based clusters for hierarchical wireless heterogeneous sensor networks (HWHSNs) is presented in this paper through investigating how heterogeneous sensor nodes enhance network performance. The HWHSNs have some sensor nodes that have greater power and transmission capability than other nodes. All kinds of nodes are evenly deployed in sensing cube respectively. The three-dimension sensing cube is divided into a number of small same cubes for all kinds of nodes and then eight of those small cubes comprise a logical group for heterogeneous nodes. The structure of HWHSNs is a two-layer structure. The upper layer contains all cluster heads, namely heterogeneous sensor nodes, and the lower layer contains all ordinary sensors managed by corresponding cluster heads. The pairwise keys between all kinds of nodes are set up through utilizing the concept of the overlap key sharing and the random key predistribution scheme. Analysis shows the heterogeneous nodes improve both the security and connectivity of the wireless sensor networks and prolong the WSNs lifetime.

Introduction

Nowadays, wireless sensor networks which consist of a number of sensor nodes have obtained a growing consideration from the researchers\textsuperscript{[1]}. Generally, wireless sensor networks architectures include hierarchical architecture, heterogeneous architecture, etc. In hierarchical wireless sensor networks, some trusted nodes, for example base stations or clusters, function as the key center because they are more powerful than ordinary sensors. In heterogeneous wireless sensor networks, there are two kinds of sensors at least; different kinds of sensor have different capacities in communication, computation, storage, etc. They are utilized in many fields although sensors have some limitations including low computing capacity, limited storage, etc. Wireless sensor networks usually are distributed in unfriendly or even hostile environments for those applications\textsuperscript{[2]}. Therefore, they easily are attacked by adversaries\textsuperscript{[3]}.

Key management is of importance in order to ensure WSNs secure and it has been researched recently. In paper \textsuperscript{[4]}, the OKS (Overlap-Key-Sharing) protocol is given. The scheme creates a long bit-string which acts as the key-string-pool (KP) of the sensor network, and randomly allots each sensor a subset of the key-string-pool which acts as the key-string. Sensors utilize the overlap intervals of the key-strings as their common secret key. In paper \textsuperscript{[5]}, Zhang, et al. gave a secure strategy for three-dimension heterogeneous wireless sensor networks. In the scheme, the sensing space is partitioned into a number of same small cubes.

This paper presents a pairwise key establishment scheme through using the methods in paper \textsuperscript{[5]}, the concept of the overlap key sharing and the random key pre-distribution scheme. The scheme researches how the heterogeneous sensors improve the HWHSNs performance. Analysis shows heterogeneous nodes improve the resilience and connectivity for HWHSNs and enlarge the network lifetime.

The paper is outlined as the following. The introduction is in the section 1. The hierarchical key...
Hierarchical Key Management Strategy

This paper presents a key management strategy based on three-dimension clusters for hierarchical wireless heterogeneous sensor networks. The scheme is a two-layer dynamic key management strategy, which contains the base station, the cluster heads, and the ordinary sensor nodes. The upper layer consists of all cluster heads, namely class 1 sensor nodes, and the lower layer consists of all normal sensors, namely class 0 sensor nodes, managed by their corresponding cluster heads.

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 \( r_i \) (\( 0 \leq i \leq 1 \)) express the class \( i \) communication range. It is clear that \( r_0 < r_1 \).

The key generation of the HWHSNs is based on the random key distribution and the OKS protocol. Taking the heterogeneity into account, this paper employs a randomly generated long bit-string as a key pool for all kinds of nodes.

We divide equally the classes of sensor nodes into \( J \) cells, denoted as \( C_{00}^i, \ldots, C_{00}^l, \ldots, C_{0l}^i, \ldots, C_{0l}^l, \ldots, C_{1i}^i, \ldots, C_{1i}^l, \ldots, C_{1l}^i, \ldots, C_{1l}^l, \ldots, C_{jk}^i, \ldots, C_{jk}^l, \ldots, C_{kl}^i, \ldots, C_{kl}^l, \ldots \), where \( 0 \leq j_c^i \leq \sqrt[3]{M} \), \( 0 \leq k_c^i \leq \sqrt[3]{M} \) and \( 0 \leq l_c^i \leq \sqrt[3]{M} \). A unique group ID \( j \) is assigned to all those cells and \( j = 0, \ldots, j = l_c^i, \ldots, j = \sqrt[3]{M}, j = \sqrt[3]{M} + 1, \ldots, j = \sqrt[3]{M} + l_c^i, \ldots, j = 2\sqrt[3]{M} + 1, \ldots, j = k_c^i(\sqrt[3]{M} + 1), \ldots, j = k_c^i(\sqrt[3]{M} + 1) + l_c^i, \ldots, j = k_c^i(\sqrt[3]{M} + 1) + \sqrt[3]{M}, \ldots, j = k_c^i(\sqrt[3]{M} + 1) + \sqrt[3]{M} + 1, \ldots, j = (\sqrt[3]{M} + 1)(\sqrt[3]{M} + 1) + \sqrt[3]{M} + 1, \ldots, j = (\sqrt[3]{M} + 1)(\sqrt[3]{M} + 1) + \sqrt[3]{M} + 1 + \sqrt[3]{M} + 1 \).

The key server engenders \( I \) long bit-strings, where a unique key pool ID \( i \) is assigned to each long-bit-string, \( S_0, S_1, \ldots, S_{i-2}, S_{i-1} \), and then takes \( S_0 \), denoted as \( \Omega_0 \), as the key-string-pool for 0 class nodes, the mixture of \( S_0 \) and \( S_1 \), denoted as \( \Omega_1 \), as the key-string-pool for 1 class nodes and so on. In this paper, we let \( I = 2 \).

A subaggregate of those key-string-pools, denoted as \( \Omega_j \), can be engendered for sensors in class \( i \) and group \( j \). Let \( \Omega_j = \bigcup_{k=0}^{i} \Omega_j(k) \), where \( \Omega_j(k) \) is a subaggregate of \( \Omega_j \).

In group \( j \), one class \( i_1 \) node and one class \( i_2 \) node\((i_1 < i_2)\) will be able to share some bit-strings if \( \Omega_{i_1}(k_1) \bigcap \Omega_{i_2}(k_2) \neq \emptyset \) come into existence, where \( k_1 \leq i_1 < i_2, k_2 \leq i_2, \Omega_{i_1}(k_1) \subset \Omega_{i_2} \), and \( \Omega_{i_2}(k_2) \subset \Omega_{i_1} \). For example, one class 0 node and one class 1 node will share some bit-strings if \( \Omega_{i_1}(0) \bigcap \Omega_{i_2}(0) \neq \emptyset \) come into existence, where \( \Omega_{i_1}(0) \subset \Omega_0 \) and \( \Omega_{i_2}(0) \subset \Omega_1 \).

For the same class \( i \), nodes in two different groups \( j_1, j_2 \) will share some bit-strings if \( \Omega_{i_1}(k_1) \bigcap \Omega_{i_2}(k_2) \neq \emptyset \) come into existence, where \( k_1 \leq i_1, k_2 \leq i_2, \Omega_{i_1}(k_1) \subset \Omega_{i_2} \), and \( \Omega_{i_2}(k_2) \subset \Omega_{i_1} \). Class 0 nodes in different groups may share no common bit-strings, namely, \( \Omega_{i_1}(k_1) \bigcap \Omega_{i_2}(k_2) = \emptyset \), where \( \Omega_{i_1}(0) \subset \Omega_0 \) and \( \Omega_{i_2}(0) \subset \Omega_1 \), and class 1 nodes in different groups may share no common bit-strings, namely, \( \Omega_{i_1}(k_1) \bigcap \Omega_{i_2}(k_2) \neq \emptyset \), where \( \Omega_{i_1}(0) \subset \Omega_0 \),
\[ \Omega_{ij}^{(1)} \subseteq \Omega_i, \Omega_{ij}^{(0)} \subseteq \Omega_0, \text{ and } \Omega_{ij}^{(1)} \subseteq \Omega_j. \]

The key server chooses a subset of key-strings, \( \Phi_n^{\theta} (\Phi_n^{\theta} \subseteq \Omega_j) \), for a node \( n \) in class \( i \) and group \( j \). Next, the key server assigns the node the key-string shares of these key-strings.

Location-based Grids.

The sensing space \( V \) has three dimensions, \( x, y, \) and \( z \), and all nodes are evenly distributed in the sensing space in Fig. 1. \( V \) is equally divided into \( (\sqrt[3]{M} + 2)^3 \), \( C_{000}, C_{001}, \ldots, C_{001}, \ldots, C_{001} \), \( C_{010}, C_{011}, \ldots, C_{011}, \ldots, C_{011} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ldots, C_{0k1} \), \( C_{0k0}, C_{0k1}, \ldots, C_{0k1}, \ld ...
each of the more powerful nodes.

Let \( I = 2 \) and \( S \) be the size of \( \Omega \). Suppose \( P_0 \) and \( P_1 \) be the number of subcollection of key-strings that can be stored in a class 0 node and a class 1 node respectively. In a certain logical group, the probability \( p(\alpha) \) that a class 0 node shares \( \alpha \) sub key-strings with a class 1 node is calculated as follows

\[
p(\alpha) = \frac{S(S-a)(S-P_0)}{P_0(P_0-\alpha)(P_1-\alpha)}.
\]

Suppose a class 1 node only can establish safe links with those class 1 nodes close to it in different logical groups. For example, in Fig. 1, the class 1 node in \( G_{11} \) only can establish safe links 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 share \( \beta \) sub key-strings is calculated as follows

\[
p(\beta) = \frac{S(S-\beta)(S-P_1)}{P_1(P_1-\beta)}.
\]

Let \( G_0 \) express the class 0 nodes and \( G_i \) express the class 1 nodes. Define a \( G_i \) node is the vicinage of a \( G_0 \) node if it can directly accept a broadcast message transmitted from the \( G_i \) node. Namely, the \( G_0 \) node can get bit-string pool information transmitted by the \( G_i \) node without help of other nodes. For simplicity, we make an assumption a \( G_0 \) node can transmit data to any \( G_i \) in its vicinage through either a one-hop manner if the distance between them is small enough, or a multi-hop manner if the distance is more than a threshold.

In Fig. 2, 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 vicinage nodes of the node \( A \). Additionally, \( A \) shares key \( K_{1i} \) \((i = 0, 1)\) with \( X_i \) \((i = 0, 1)\) respectively, similarly, \( A \) shares key \( K_{20} \) and \( K_{30} \) with node \( Y_0 \). If \( A \) sends messages to the sink node, certainly, it will first select the key \( K_{1i} \). If the distance from \( A \) to \( X_1 \) is more than a threshold, moreover, there are compromised nodes in the path from \( A \) to \( X_1 \), \( A \) will not connect with it. In the same way, \( A \) 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 compromised, it will not disclose any information of class 0 nodes in other cells, because the node 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 defend attacks than class 0 nodes. Therefore, the scheme improves the security for WSNs.

**The Function of Heterogeneous Nodes for the Network Connectivity.**

A class 0 node and a class 1 node can establish a safe link if they share a key, therefore, the scheme can ensure the class 0 node and a class 1 node establish a safe link if \( \sum \alpha \geq 1 \). This result can be obtained through choosing reasonable \( S_0 \) and \( P_0 \). The scheme can ensure any two class 1 nodes establish a safe link if \( \sum \beta \geq 1 \). This result can be obtained through choosing reasonable \( S \) and \( P_1 \). Therefore, the scheme can ensure all nodes including class 0 nodes and class 1 nodes can establish a safe link with any other node, if \( \sum \alpha \geq 1 \) and \( \sum \beta \geq 1 \), through selecting reasonable \( S, P_1 \) and \( P_2 \).

**The Function of Heterogeneous Nodes for the Network Lifetime.**

In Fig. 3, the cluster head locates in the center and has eight cluster nodes, which locate in eight cell centers respectively. All class 0 nodes, namely cluster sensors, in transmit their information to the class 1 node, namely their cluster head, and the class 1 node sends it to the next cluster head or the base station directly after receiving and aggregating those information. It is obvious the cluster heads spend much more energy than cluster nodes. If class 0 nodes function as the cluster heads, they will spend their energy more quickly than class 1 nodes because class 1 nodes have more energy than class 0 nodes. Therefore, the network lifetime enlarges by employing class 1 nodes as the cluster heads.

**The Conclusion**

In most existing wireless sensor networks, all sensor nodes are supposed to have same capabilities including battery energy, communication range, etc. This paper investigates how heterogeneous nodes improve the performance of hierarchical wireless sensor networks. The sensing cube is divided into a number of small same cubes, eight of which are comprised of a logical group. This scheme has a two-tier structure for WSNs. The upper tier consists of all cluster heads, namely heterogeneous sensor nodes, and the lower tier consists of ordinary sensors in all clusters. All kinds of nodes are distributed in entire sensing cube and they can establish their pairwise keys through employing the concept of the overlap key sharing and the random key predistribution scheme. With the help of heterogamous sensor nodes, the HWHSN is more resilient to compromised node attack and has better network connectivity than wireless sensor networks. Moreover, they prolong the network lifetime.
Acknowledgements

This work was supported by the Project of Shandong Province Higher Educational Science and Technology Program, and the project number is J13LN05.

References


