A Security Scheme based on Location for Wireless Sensor Networks

Yuquan Zhang, Lihua Sun and Min You

1, 2School of Information Technology, Shandong Women’s University, Jinan 250300, China
3Provincial Hospital Affiliated to Shandong University, Jinan 250021, China

Abstract: A pairwise key pre-distribution scheme based on the concept of the Overlap Key Sharing (OKS) and clusters for wireless sensor networks is proposed. This strategy divides the sensing area into square cells and logical groups and distributes key information to the sensor nodes by employing the OKS scheme. Sensor nodes establish their secure communication through using their keys. Analysis and comparison demonstrate that this scheme has good network connectivity, effectively reduces storage cost and enhances the security for WSNs and provides flexible security grades.

Keywords: Network security, pairwise key, overlap key sharing, wireless sensor networks

INTRODUCTION

A Wireless Sensor Network (WSN) is a wireless network that consists of numerous spatially deployed tiny autonomous devices cooperatively monitoring environmental conditions and sending the collected data to a command center through wireless channels. Various feasible applications are introduced including industrial sensor networks (Lakshman, et al., 2005), volcano monitoring networks (Werner-Allen et al., 2006), habitat monitoring (Ning, 2003), health monitoring and home automation etc.

The security and reliability for wireless sensor networks face many challenges because of the wireless nature of communications, resource limitations of sensor nodes, generally very large and dense networks, unknown network topology prior to deployment and the high risk of physical attacks on unattended sensors (Tolle and Culler, 2005; Shin and Cha, 2006).

In order to protect sensitive sensing data and communications between sensor nodes in WSNs, security capacity of wireless sensor networks, including availability, authorization, authentication, confidentiality, integrity, non-repudiation and freshness, is required. The key management is extremely of importance to assure WSN security. This study presents a key management strategy based on location for wireless sensor networks.

Key management, a key issue in security for wireless sensor networks, has been investigated widely and some approaches have been proposed for distributed wireless sensor networks (Eschenauer and Gligor, 2002; Chan et al., 2003; Blundo et al., 1992; Liu and Ning, 2003a). Eschenauer and Gligor (2002) introduced a probabilistic key pre-distribution scheme recently for key establishment. The chief idea is to let each sensor node randomly pick 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. (2003), namely, a q-composite key pre-distribution 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 pair wise 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.

Blundo et al. (1992) archived key distribution for dynamic conferences by using bivariate polynomials. In order to establish a pairwise key between two nodes, the key setup server randomly generates a t-degree bivariate polynomial over a finite field. The desired symmetric property can be obtained through choosing appropriate coefficient. This study guarantees that this strategy is unconditionally secure and t-collusion resistant. The constraint in this study is that the scheme can only tolerate no more than t compromised nodes, where the value of t is limited by the memory available in sensor nodes. Obviously, the larger a wireless sensor network is, the more likely an attacker comprises more than t sensor nodes.

LOCATION-BASED PAIRWISE KEY ESTABLISHMENT

We introduce the key cluster concept in study (Lai et al., 2004). In Lai et al. (2004), the overlap key sharing protocol creates long bit clusters as the key cluster pool and distributes a sub-group to every sensor as the key cluster. The sensors employ the overlap sections as the
sharing keys with their neighbor sensors. In this study, the overlap key sharing protocol creates \( m \) bit clusters denoted as GLD\(_{i}\), where \( i = 0, 1, ..., (m-2), (m-1) \), namely, \( 0 \leq i \leq m-1 \).

**Cells based on location and logical groups:** In Fig. 1, there are \( N \) sensor nodes in the sensing area \( S \). Those nodes are divided into \( m \) same groups denoted as \( C_0, C_1, \cdots, C_{(m-2)} \) and \( C_{(m-1)} \), where \( 0 \leq I \leq m-1 \). The sensing area \( S \) in the wireless sensor networks is divided into \( m \) same cells, denoted as \( C_0, C_1, \cdots, C_{l} \) and \( C_{l+1} \), where \( 0 \leq I \leq m-1 \), according to their geographical locations. The sensor nodes in group \( C_I \) are deployed in cell \( C_I \). Prior to the deployment, the key setup server distributes GID\(_I\) to those sensor nodes in \( C_I \) and forms the logical groups. There are \( m-1 \) logical groups denoted as \( G_0, G_1, \cdots, G_{l}, G_{l+1}, \cdots, G_{(m-2)} \) and \( G_{(m-1)} \), where \( 0 \leq I \leq m-2 \), each of which consists of two cells. Namely, the logical group \( G_I \) comprises cell \( C_I \) and \( C_{I+1} \), where \( 0 \leq I \leq m-2 \) and then the logical \( G_I \) has \( 2N/m \) sensor nodes.

**Pairwise key establishment in a logical group:** Utilizing the concept in paper (Chan \textit{et al}., 2003; Liu and Ning, 2003b), the setup server randomly generates \( \left\lceil \frac{2N}{m} \right\rceil \) sub bit clusters in GID\(_I\) NID\(_{I} \) and GID\(_{I+1}\) NID\(_{I} \) for logical group \( G_I \) respectively, where \( J_r = 0, 1, \cdots, (\left\lceil \frac{2N}{m} \right\rceil -2), (\left\lceil \frac{2N}{m} \right\rceil -1) \) and \( J_r = 0, 1, \cdots, (\left\lceil \frac{2N}{m} \right\rceil -2), (\left\lceil \frac{2N}{m} \right\rceil -1) \). The setup server divides all nodes in a logical group into \( \sqrt{2N/m} \) small groups denoted as \( c_0, c_1, \cdots, c_{i}, \cdots \) and \( c_{i+1} \) where \( i = 0, 1, \cdots, (\left\lceil \frac{2N}{m} \right\rceil -2), (\left\lceil \frac{2N}{m} \right\rceil -1) \) and assigns GID\(_I\) NID\(_{I} \) to all nodes in \( c_0 \), GID\(_I\) NID\(_{I} \) to all nodes in \( c_1 \), GID\(_I\) NID\(_{I} \) to all nodes in \( c_{i} \), and GID\(_I\) NID\(_{I} \) to all nodes in \( c_{i+1} \) respectively. Therefore, any node in a cluster has a certain GID\(_{I} \) NID\(_{I} \), \( J_r = 0, 1, \cdots, (\left\lceil \frac{2N}{m} \right\rceil -2), (\left\lceil \frac{2N}{m} \right\rceil -1) \)

\[ \text{hash}(\text{GID}_I \oplus \text{NID}_I) \oplus (J_r)_S \oplus (J_r)_S \oplus (J_r)_S \oplus (J_r)_S \]
For GID_{j+1}NID_{j+1}, the communication connection key $K'_{S_0,S_1}$ between node $S_0$ and $S_1$ is generated by the common section GID_{j+1}NID_{j+1} and the indexes of the node $S_0$ and $S_1$ as follows:

$$K'_{S_0,S_1} = \text{hash}\left\{(\text{GID}_{j+1} \cap \text{NID}_{j+1}) \oplus (J_r)_{S_0} (J_r)_{S_1}\right\}$$

(3)

where, $(J_r)_{S_0} = (J_r)_{S_1}$.

Obviously, GID_{j+1}NID_{j+1} is shared by $\sqrt{2N/m}$ sensor nodes including $S_0$ and $S_1$, therefore, we can obtain the communication connection key $K'_{S_0-S_1}$ between $S_0$ and $S_1$ as follows:

$$K'_{S_0-S_1} = \text{hash}\left\{(\text{GID}_{j+1} \cap \text{NID}_{j+1}) \oplus (J_r)_{S_0} (J_r)_{S_1}\right\}$$

(4)

where, $(J_r)_{S_0} = (J_r)_{S_1} = \cdots (J_r)_{S_i}$.

$K'_{S_0-S_1}, K'_{S_0-S_2}, K'_{S_2-S_1}$ and $K'_{S_0-S_1}$ are computed quickly through exclusive OR based on digit in hash functions.

In general, the sensor node $U$ in the logical group $G_j$ can establish a pair wise key with any other sensor node $V$ in the same logical group according to the overlap key sharing concept. If the node $A$ and $B$ share GID_{j}NID_{j} or GID_{j+1}NID_{j+1}, the two nodes can directly establish a pair wise key. If the two nodes share nothing, they also can establish a pair wise key through a midway node $W$. We will describe in detail as follows.

Let $C_U, C_V, C_W, R_U, R_V$, and $R_W$ stand for the sub bit cluster in GID_{j}NID_{j} and GID_{j+1}NID_{j+1} of node $U, V$ and $W$ respectively. If $C_U = C_V$ or $R_U = R_V$, they can establish a pair wise key directly by using the common sub bit cluster. $W$ can directly establish a pair wise key with $U$ if $C_U = C_W$ or $R_U = R_W$. In the same way, $W$ can directly establish a pair wise key with $V$ if $C_V = C_W$ or $R_V = R_W$. So, if $C_U \neq C_V$ and $R_U \neq R_V$, they still can establish a pair wise key through a midway node $W$. The pair wise key establishment path is $U \rightarrow W \rightarrow V$ or $V \rightarrow W \rightarrow U$. We can obtain the communication connection keys between node $U$ and $V$ respectively as follows:

$$K_{U,V} = \text{hash}\left\{(\text{GID}_{j+1} \cap C_U) \oplus (\text{GID}_{j+1} \cap C_V) \oplus (C_U, R_U) \oplus (C_V, R_V) \oplus (C_W, R_W)\right\}$$

(5)

$$K_{V,U} = \text{hash}\left\{(\text{GID}_{j+1} \cap C_U) \oplus (\text{GID}_{j+1} \cap C_V) \oplus (C_U, R_U) \oplus (C_V, R_V) \oplus (C_W, R_W)\right\}$$

(6)

**Addition of new node:** If a sensor node $S_i$ will be added to the logical group $G_j$, the setup server randomly distributes an ID denoted as:

$$\left\{\left(\frac{2N}{m} + J_r\right)_{S_i}, \left(\frac{2N}{m} + J_r\right)_{S_i}\right\}$$

and two sub bit clusters GID_{i}NID_{j} to $S_i$, where,

$$\left\{\left(\frac{2N}{m} + J_r\right)_{S_i}, \left(\frac{2N}{m} + J_r\right)_{S_i}\right\} \neq (J_r)_{S_i}, (J_r)_{S_i}$$

$$0 \leq h \leq \left\lfloor \frac{2N}{m} \right\rfloor - 1$$

$J_r = 0, 1, 2, \ldots, J_r = 1, 2, \ldots$

After added to $G_j$, $S_i$ broadcasts a message $\{\{\left(\frac{2N}{m} + J_r\right)_{S_i}\}$ to other nodes. The communication connection key $K'_{S_i-S_i}$ between $S_i$ and $S_i$, $0 \leq h \leq \left\lfloor \frac{2N}{m} \right\rfloor - 1$, which have common sub bit cluster GID_{i}NID_{j}, is generated by the common section as follows:

$$K'_{S_i-S_i} = \text{hash}\left\{(\text{GID}_{j+1} \cap \text{NID}_{j+1}) \oplus \left(\frac{2N}{m} + J_r\right)_{S_i}\right\}$$

(7)

where, $(J_r)_{S_i} = (J_r)_{S_i}$.

In the same way, The communication connection key $K'_{S_i-S_i}$ between $S_i$ and $S_i$, $0 \leq h \leq \sqrt{2N/m} - 1$, which have common sub bit cluster GID_{j}NID_{j}, is generated as follows:

$$K'_{S_i-S_i} = \text{hash}\left\{(\text{GID}_{j+1} \cap \text{NID}_{j+1}) \oplus \left(\frac{2N}{m} + J_r\right)_{S_i}\right\}$$

(8)

where, $(J_r)_{S_i} = (J_r)_{S_i}$.

**Eviction of node:** In wireless sensor networks, nodes inevitably are compromised, or, they deplete their energy, so those nodes ought to be deleted in time to guarantee network security. Our scheme can delete those nodes and refresh related keys. According those formulas (1-8), 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

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

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

According to the concept of the q-composite key pre-distribution scheme in study (Chan et al., 2003), our scheme may require node $S_0$ and $S_1$ sharing $K_{S_0S_1}$ and $K_{S_0S_1}$ simultaneously or one of them to realize their secure communication. Therefore, this scheme can realize flexible secure grades for wireless sensor networks. Additionally, the pair wise keys in the nodes are generated by using hash functions; therefore, compromised nodes do not reveal pair wise keys in other nodes even though they probably lose their keys.

The storage expense of WSNS: Each node in the logical groups is distributed a node index and two single sub bit clusters in our scheme and each node in Xiao-Yu et al. (2008) stores seven sub bit clusters. It is clear that the storage cost in this scheme greatly reduces than that in study (Xiao-Yu et al., 2008).

The connectivity in WSNS: As discussion above, any two sensor node $U$ and $V$ in the same logical group can establish their pair wise key through using the overlap key sharing concept. Our strategy can guarantee any two sensor node $U_0$ and $U_3$, which are not in the same logical group, establish a pair wise key. In Fig. 2, $U_0$ is in the logical group $G_j$ consisting of cell $C_j$ and $C_{j+1}$ and $U_3$ is in $G_{j+2}$ consisting of cell $C_{j+2}$ and $C_{j+3}$. In general, suppose that $C_{U_0} \neq C_{U_1}$ and $R_{U_0} \neq R_{U_1}$, where $C_{U_0}$, $C_{U_1}$, $R_{U_0}$ and $R_{U_1}$ stand for the sub bit cluster in GID, NID, and GID, NID, of the node $V_0$, $W_0$, so, the node $U_0$ and $U_1$ can always establish a pairwise key through employing intermediate node $V_0$ or $W_0$. In the same way, the node $U_1$ and $U_2$ can always establish a pairwise key by using intermediate node $V_1$ or $W_1$ in the logical group $G_{j+1}$ and the node $U_3$ and $U_4$ can always establish a pairwise key by using intermediate node $V_3$ or $W_3$ in the logical group $G_{j+2}$. In Fig. 2, the key discovery paths include:

- $V_0 \rightarrow U_0 \rightarrow V_0 \rightarrow U_1 \rightarrow V_1 \rightarrow U_2 \rightarrow V_2 \rightarrow U_1 \rightarrow V_1 \rightarrow U_0 \rightarrow V_0 \rightarrow U_0 \rightarrow V_0 \rightarrow U_1 \rightarrow V_1 \rightarrow U_2 \rightarrow V_2 \rightarrow U_3 \rightarrow U_0 \rightarrow V_0$.

random key $K$ is generated and it is utilized as the pair wise key between node $U_0$ and $U_3$ that is in different logical groups and has no common sub bit cluster. The $K$ can be transmitted through any one of the key discovery paths. The nodes outside the key discovery paths can not obtain the $K$, because it is transmitted through secure connection. Additionally, in this scheme the pair wise 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.

CONCLUSION

The scheme in this study combines overlap sharing key scheme and the key management strategy based on cells and logical groups. The sensing area is divided in a number of cells and logical groups. The sensor nodes are distributed sub bit clusters and establish their pair wise keys through using the OKS concept. This scheme effectively reduces storage cost, has good network connectivity, improves the security for WSNS and provides flexible security grades.

REFERENCES


