Research Journal of Applied Sciences, Engineering and Technology 5(20): 4920-4924, 2013
DOI:10.19026/rjaset.5.4343
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: September 30, 2012 Accepted: December 02, 2012 Published: May 15, 2013

Research Article

A Security Scheme based on Location for Wireless Sensor Networks

[1]Yuquan Zhang, [2]Lihua Sun and [3]Min You
[1, 2]School of Information Technology, Shandong Women's University, Jinan 250300, China
[3]Provincial Hospital Affiliated to Shandong University, Jinan 250021, China

Abstract: A pair wise 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, pair wise 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 pair wise 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 pair-wise 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

Corresponding Author: Yuquan Zhang, School of Information Technology, Shandong Women's University, Jinan 250300, China

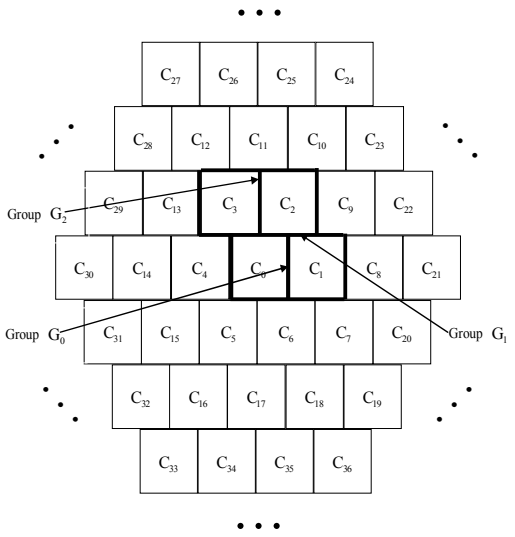

Fig. 1: Location-based cells and logical groups

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,$0 \le I \le$ 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 $C_0^{'}, C_1^{'}, \cdots, C_I^{'}, \cdots, C_{(m-2)}^{'}$ and $C_{0(m-1)}^{'}$, where $0 \le I \le m$-1. The sensing area S in the wireless sensor networks is divided into m same cells, denoted as C_0, C_1, C_I, $C_{(m-2)}$ and C_{m-1}, where $0 \le I \le m$-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, …, G_2, G_I, …, $G_{(m-3)}$ and G_{m-2}, where $0 \le I \le m$-2, each of which consists of two cells. Namely, the logical group G_I comprises cell C_I and $C_{(I+1)}$, where $0 \le I \le m$-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 *et al*., 2003; Liu and Ning, 2003b), the setup server randomly generates $\sqrt{\frac{2N}{m}}$ sub bit clusters in $GID_I\ NID_{Jc}$ and $GID_{I+1}\ NID_{Jr}$ for logical group G_I respectively, where J_c = 0, 1, …, ($\sqrt{\frac{2N}{m}}$ -2), ($\sqrt{\frac{2N}{m}}$ - 1) and J_r = 0, 1, …, ($\sqrt{\frac{2N}{m}}$ -2), ($\sqrt{\frac{2N}{m}}$ - 1). The setup server divides all nodes in a logical group into √2N/m small groups denoted as c_0, c_1, …, c_i, …, $c\sqrt{\frac{2N}{m}}$ -1where i = 0, 1,…, ($\sqrt{\frac{2N}{m}}$ -2), ($\sqrt{\frac{2N}{m}}$ -1) and assigns $GID_I\ NID_0$ to all nodes in c_0, $GID_I\ NID_1$ to all nodes in c_1, …, $GID_I\ NID_1$ to all nodes in c_i,…and $GID_I\ NID_{\sqrt{2N/m}-1}$ to all nodes in $c\sqrt{\frac{2N}{m}}$ -1 respectively and assigns $GID_{I+1}NID_0$, … , $GID_{I+1}NID_1$ …, $GID_{I+1}NID_{Jr}$,…, $GID_{I+1}\ NID_{\sqrt{2N/m}-1}$to the different nodes in group c_0, c_1, …, c_i, …, $c\sqrt{\frac{2N}{m}}$ - 1 respectively. Therefore, any node in a cluster has a certain $GID_{I+1}NID_{Jc}$, J_c = 0, 1,.., ($\sqrt{\frac{2N}{m}}$ -2), ($\sqrt{\frac{2N}{m}}$ -1) and a certain $GID_{I+1}NID_{Jr}$, J_r = 0, 1, …, ($\sqrt{\frac{2N}{m}}$ -2), ($\sqrt{\frac{2N}{m}}$ -1). Let ID, denoted as (J_c, J_r), be the index of the sensor nodes, which is distributed $GID_I\ NID_{Jc}$ and $GID_{I+1}NID_{Jr}$. It is clear that different nodes have different indexes. The setup server then distributes {(J_c, J_r)} GID_INID_{Jr}, $GID_{I+1}NID_{Jr}$} to each sensor. If two nodes have a common sub bit cluster, they can establish pair wise keys and then can communicate securely. It is clear that a certain sub bit cluster is shared by √2N/m nodes in a certain cluster and a node can directly establish communication keys with 2($\sqrt{\frac{2N}{m}}$ -1) sensor nodes.

Suppose node S_0 is in the logical group G_I and its index is $[(J_c)_{S0}, (J_r)_{S0}]$. After deployment of nodes, node S_0 broadcasts its message {$[(J_c)_{S0}, (J_r)_{S0}]$, GID_I, NID_{Jc}, GID_{I+1}, NID_{Jr}} to discover nodes, which have common sub bit clusters with it. The common sub bit clusters shared by nodes with it are $GID_I NID_{Jc}$ or $GID_{I+1}NID_{Jr}$.

For $GID_I NID_{Jc}$, the communication connection key $K_{S_0S_1}^c$ between node S_0 and S_1 is generated by the common section $GID_I NID_{Jc}$ and the indexes of the node S_0 and S_1 as follows:

$$K_{S_0S_1}^c = \text{hash}\left\{(\text{GID}_I \| \text{NID}_{J_c}) \oplus \left\langle (J_c)_{S_0}, (J_r)_{S_0} \right\rangle \oplus \left\langle (J_c)_{S_1}, (J_r)_{S_1} \right\rangle\right\} \quad (1)$$

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

Obviously, $GID_I NID_{Jc}$ is shared by √2N/m sensor nodes including S_0 and S_1, therefore, we can obtain the communication connection key $K_{S_0-S_1}^c$ between S_0 and S_1 as follows:

$$K_{S_0-S_1}^c = \text{hash}\left\{(\text{GID}_I \| \text{NID}_{J_c}) \oplus \left\langle (J_c)_{S_0}, (J_r)_{S_0} \right\rangle \oplus \left\langle (J_c)_{S_1}, (J_r)_{S_1} \right\rangle \oplus \left\langle (J_c)_{S_2}, (J_r)_{S_2} \right\rangle \cdots \oplus \left\langle (J_c)_{S_{\sqrt{\frac{2N}{m}}-1}}, (J_r)_{S_{\sqrt{\frac{2N}{m}}-1}} \right\rangle\right\} \quad (2)$$

where,

$$(J_c)_{S_0} = (J_c)_{S_1} = (J_c)_{S_2} = \cdots = (J_c)_{S_{\sqrt{\frac{2N}{m}}-1}}$$

For $GID_{I+1}NID_{Jr}$, the communication connection key $K^r_{S_0S_1}$ between node S_0 and S_1 is generated by the common section $GID_{I+1}NID_{Jr}$ and the indexes of the node S_0 and S_1 as follows:

$$K^r_{S_0S_1} = \text{hash}\left\{(\text{GID}_{I+1} \| \text{NID}_{J_r}) \oplus \left\langle (J_c)_{S_0}, (J_r)_{S_0} \right\rangle \oplus \left\langle (J_c)_{S_1}, (J_r)_{S_1} \right\rangle\right\} \quad (3)$$

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

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

$$K^r_{S_0-S_1} = \text{hash}\left\{(\text{GID}_{I+1} \| \text{NID}_{J_r}) \oplus \left\langle (J_c)_{S_0}, (J_r)_{S_0} \right\rangle \oplus \left\langle (J_c)_{S_1}, (J_r)_{S_1} \right\rangle \oplus \left\langle (J_c)_{S_2}, (J_r)_{S_2} \right\rangle \oplus \cdots \oplus \left\langle (J_c)_{S_{\sqrt{\frac{2N}{m}}-1}}, (J_r)_{S_{\sqrt{\frac{2N}{m}}-1}} \right\rangle\right\} \quad (4)$$

where, $(J_r)_{S_0} = (J_r)_{S_1} = (J_r)_{S_2} = \cdots (J_r)_{S_{\sqrt{\frac{2N}{m}}-1}}$

$K^c_{S_0S_1}$, $K^c_{S_0-S_1}$, $K^r_{S_0S_1}$ and $K^r_{S_0-S_1}$ are computed quickly through exclusive OR based on digit in hash functions.

In general, the sensor node U in the logical group G_I 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_INID_{Jc} or $GID_{I+1}NID_{Jr}$, 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 $GID_I\,NID_{Jc}$ and $GID_{I+1}\,NID_{Jr}$, 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:

$$K_{UV} = \text{hash}\left\{(\text{GID}_I \| C_U) \oplus (\text{GID}_{I+1} \| C_V) \oplus \left\langle C_U, R_U \right\rangle \oplus \left\langle C_V, R_V \right\rangle \oplus \left\langle C_W, R_W \right\rangle\right\} \quad (5)$$

$$K_{VU} = \text{hash}\left\{(\text{GID}_I \| C_V) \oplus (\text{GID}_{I+1} \| C_U) \oplus \left\langle C_U, R_U \right\rangle \oplus \left\langle C_V, R_V \right\rangle \oplus \left\langle C_W, R_W \right\rangle\right\} \quad (6)$$

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

$$\left\langle \left(\sqrt{\frac{2N}{m}} + J_c^{'}\right)_{S_{h'}}, \left(\sqrt{\frac{2N}{m}} + J_r^{'}\right)_{S_{h'}} \right\rangle$$

and two sub bit clusters $GID_I\,NID_{Jc}$ to S_h, where,

$$\left\langle \left(\sqrt{\frac{2N}{m}} + J_c^{'}\right)_{S_{h'}}, \left(\sqrt{\frac{2N}{m}} + J_r^{'}\right)_{S_{h'}} \right\rangle \neq \left\langle (J_c)_{S_h}, (J_r)_{S_h} \right\rangle \quad 0 \le h \le \sqrt{\frac{2N}{m}} - 1$$

$J_c^{'} = 0,1,2,\cdots$, $J_r^{'} = 1,2,\cdots$

After added to G_I, $S_{h'}$ broadcasts a message $\{[(\sqrt{\frac{2N}{m}} + J_{c)}\ S_h]\}\ \{[(\sqrt{\frac{2N}{m}} + J_{c)} S_h]\}$, GID_I, NID_{Jc}, GID_{I+1}, $NID_{Jr}\}$ to other nodes. The communication connection key K^c_{ShSh} between S_h and S_h, $0 \le h \le \sqrt{\frac{2N}{m}} - 1$, which have common sub bit cluster $GID_I\,NID_{Jr}$, is generated by the common section as follows:

$$K^c_{S_{h'}S_h} = \text{hash}\left\{(\text{GID}_I \| \text{NID}_{J_c}) \oplus \left\langle \left(\sqrt{\frac{2N}{m}} + J_c^{'}\right)_{S_{h'}}, \left(\sqrt{\frac{2N}{m}} + J_r^{'}\right)_{S_{h'}} \right\rangle \oplus \left\langle (J_c)_{S_h}, (J_r)_{S_h} \right\rangle\right\} \quad (7)$$

where, $J_c = (J_c)_{S_h}$.

In the same way, The communication connection key $K^r_{S_{h'}S_h}$ between $S_{h'}$ and S_h, $0 \le h \le \sqrt{2N/m} - 1$, which have common sub bit cluster $GID_{I+1}NID_{Jr}$, is generated as follows:

$$K^r_{S_{h'}S_h} = \text{hash}\left\{(\text{GID}_{I+1} \| \text{NID}_{J_r}) \oplus \left\langle \left(\sqrt{\frac{2N}{m}} + J_c^{'}\right)_{S_{h'}}, \left(\sqrt{\frac{2N}{m}} + J_r^{'}\right)_{S_{h'}} \right\rangle \oplus \left\langle (J_c)_{S_h}, (J_r)_{S_h} \right\rangle\right\} \quad (8)$$

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

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 $K^c_{S_0S_1}$ and $K^r_{S_0S_1}$ 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_I consisting of cell C_I and C_{I+1} and U_3 is in G_{I+2} consisting of cell C_{I+2} and C_{I+3}. In general, suppose that $C_{U0} \neq C_{U1}$ and $R_{U0} \neq R_{U1}$, where C_{U0}, C_{U1}, R_{U0} and R_{U1} stand for the sub bit cluster in $GID_I\,NID_{Jc}$ and $GID_I\,NID_{Jr}$ of the node V_0 and 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_{I+1} and the node U_2 and U_3 can always establish a pairwise key by using intermediate node V_2 or W_2 in the logical group G_{I+2}. In Fig. 2, the key discovery paths include:

$$U_0 \to V_0 \to U_1 \to V_1 \to U_2 \to V_2 \to U_3, U_0 \to V_0 \to$$
$$U_1 \to V_1 \to U_2 \to W_2 \to U_3, U_0 \to W_0 \to U_1 \to$$

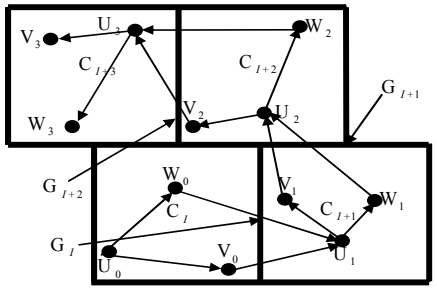

Fig. 2: The sensor node connection

$$V_1 \to U_2 \to V_2 \to U_3, U_0 \to W_0 \to U_1 \to V_1 \to$$
$$U_2 \to W_2 \to U_3, U_0 \to V_0 \to U_1 \to W_1 \to U_2 \to$$
$$V_2 \to U_3, U_0 \to V_0 \to U_1 \to W_1 \to U_2 \to W_2$$
$$\to U_3, U_0 \to W_0 \to U_1 \to W_1 \to U_2 \to V_2 \to U_3,$$
$$U_0 \to W_0 \to U_1 \to W_1 \to U_2 \to W_2 \to U_3 .\ \text{A}$$

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

Blundo, C., A.D. Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, 1992. Perfectly-secure key distribution for dynamic conferences. Proceeding of 12th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'92), Springer-Verlag , London, pp: 471-486.

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. Proceeding of IEEE Symposium on Research in Security and Privacy, Berkeley, CA, USA, May 11-14, pp: 197-213.

Eschenauer, L.V. and D. Gligor, 2002. A key-management scheme for distributed sensor networks. Proceeding of 9th ACM Conference on Computer and Communications Security (CCS'02), ACM Press, New York, pp: 41-47.

Lai, B.C.C., D.D. Hwang S.P. Kim and I. Verbauehrde, 2004. 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), pp: 351-356.

Lakshman, K., A. Robert, B. Phil, C. Jasmeet, F. Mick, K. Nandakishore, N. Lama and Y. Mark, 2005. Design and deployment of industrial sensor networks: Experiences from a semiconductor plant and the North Sea. Proceeding of the 3rd International Conferences on Embedded Networked Sensor Systems (SenSys '05), ACM Press, pp: 64-75.

Liu, D. and P. Ning, 2003a. Establishing pairwise keys in distributed sensor networks. Proceeding of 10th ACM Conference on Computer and Communications Security (CCS'03), New York, pp: 52-61.

Liu, D. and P. Ning, 2003b. Location-based pairwise key establishments for static sensor networks. Proceeding of ACM Workshop on Security in Ad Hoc and Sensor networks (SASN'03), pp: 72-82.

Ning, X., 2003. A Survey of Sensor Network Applications. University of Southern California. Retrieved from: http://enl.usc.edu/~ningxu /papers/survey. pdf.

Shin, H. and H. Cha, 2006. Supporting application-oriented kernel functionality for resource constrained wireless sensor nodes. Lect. Notes Comput. Sc., 4325: 748-759.

Tolle, G. and D. Culler, 2005. Design of an application cooperative management system for wireless sensor networks. Proceedings of the 2nd European Workshop on Wireless Sensor Networks (EWSN), Istanbul, Turkey, pp: 121-132.

Werner-Allen, G., K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees and M. Welsh, 2006. Deploying a wireless sensor network on an active volcano. IEEE Internet Comput., 10(2): 18-25.

Xiao-Yu, D., L. Jian-Wei and S. Ding-Rong, 2008. Pairwise keys predistribution scheme based on OKS for wireless sensor networks. Chin. J. Sensor. Actuator., 21(9): 1590-1594.