http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (1): 71-79, 2011
ISSN 1812-5638

An Efficient Scheme Against Node Capture Attacks using Secure Pairwise Key for Sensor Networks

Heng Ren, Xingming Sun, Zhiqiang Ruan and Baowei Wang
School of Computer and Communication, Hunan University, No. 252,
Lushan South Road, Changsha, 410082, China

Abstract: In this study, we aim to design an efficient scheme against node capture attacks using secure pairwise key in Wireless Sensor Networks (WSNs). Prior pairwise key establishment schemes based on random key pre-distribution are vulnerable to node capture attacks. In order to improve the resilience against node capture attacks, we are the first to present the Key Superset (KS) scheme. In this scheme, the entire sensor network is devided into several non-overlapping triangle cells and nodes are separated into groups, each of which is deployed in a cell and each pair of adjacent cells selects randomly a certain number of keys from the key subset which belongs to the key superset. By using deployment knowledge and KS scheme we can restrict the consequence of node capture attacks within a small range and establish pairwise key for each pair of neighboring cells efficiently. Compared to existing schemes, our proposal outperforms others in resilience against node capture attacks and achieves high local connectivity.

Key words: Wireless sensor network, key management, security, key superset, local connectivity

INTRODUCTION

Recent advances in Micro-Electro-Mechanical Systems (MEMS) technology, wireless communications and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances (Akyildiz *et al*., 2002). The resulting Wireless Sensor Networks (WSNs) in recent years have obtained more and more attention. Wireless sensor networks are used for a wide variety of applications: ocean and wildlife monitoring, manufacturing, building safety and earthquake monitoring and many military applications (Perrig *et al*., 2004). When WSNs are deployed in a hostile environment, security becomes extremely important as they are vulnerable to different types of malicious, such as node capture (Conti *et al*., 2008; Taguea and Poovendran, 2007), node replication attacks (Conti *et al*., 2007), eavesdropping, traffic-analysis, etc. One of the most vexing problems is the node capture attack. An adversary can capture a node from the network as the first step for further different types of attacks. So, in this study we focus on how to improve the resilience against node capture attacks using secure pairwise key and guarantee the communication in sensor nodes is secure.

Due to the constrained nature of the resources available on sensor nodes, traditional wireless networking security solutions such as Public Key Cryptography (PKC) and Key Distribution Center (KDC) are not viable due to their processing requirements, power consumption, speed and communications overhead (Michael *et al*., 2009). Recent research suggests that symmetric secret key pre-distribution is probably the only practical approach for establishing secure channels among sensor nodes. Before deployment, the nodes can be preloaded with some keys or secret material which can be used to calculate the pairwise key. After deployment, the communicating nodes can calculate the pairwise key using certain rules. As two extreme cases, one may use a global key to setup session key between the sensor nodes, or assign each sensor node a unique random key with each of the other nodes. However, the former is vulnerable to node capture attack and the latter involves huge storage overhead on sensor nodes.

Eschenauer and Gligo (2002) first proposed Random Key Predistribution Scheme (RKP) which is based on probability density and random graph theory and is further improved by Chan *et al*. (2003), Chan and Perrig (2005), by Du *et al*. (2003, 2004) and by Liu and Ning (2003, 2005).

Although these existing schemes provide viable solutions to the key pre-distribution problem, they are vulnerable to node capture attacks. The capture of each node will increase fraction of keys known to the

Corresponding Author: Xingming Sun, School of Computer and Communication, Hunan University, No. 252, Lushan South Road, Changsha, 410082, China Tel: 86-731-88821 341 Fax: 86-731-888 22417

adversary. When a certain number of the nodes are captured, the adversary can obtain enough keys to compromise a large number of links and make the network ineffective. Meanwhile, the key connectivity is always related to the memory cost, the higher connectivity will introduces huge storage overhead on sensor nodes.

In order to improve the resilience against node capture attacks we are the first to present the KS scheme. In our proposal, the entire sensor network is devided into several non-overlapping triangle cell and KS scheme is applied to each pair of neighboring cells. After deployment, the communications between neighboring cells are accomplished through pairwise key, which is computed based on the Blom scheme. We study the resilience against node capture attacks, the local connectivity and memory cost. Analysis and simulation results show our scheme has a nice property: when large number of nodes are compromised, communications between any other nodes in the same cell are still secure. Present results show substantial improvement over (Eschenauer and Gligor, 2002; Chan and Perrig, 2005).

The main contribution of our scheme:

- We are the first to present the KS scheme based on Blom scheme
- We integrate node's deployment knowledge with predistribution pairwise key and KS
- KS can remarkablely enhance node resilience against node capture attack

Although, like other schemes, such as (Yu and Guan. 2008), also, the KS scheme uses node's deployment knowledge. However, the KS scheme and other scheme are different. In the KS scheme, nodes are devided into groups, each of which is deployed in a cell, the communications between the neighbor nodes in a cell are achieved through pairwise key pre-distributed using Blom scheme. It will ensure the communications within a cell are absolutely safe. So in will greatly enhance the resilience against node capture attack. In order to ensure the connectivity of the network, sensor nodes in neighboring cells should choose the secret materials from the same matrix. So, a node from its neighbor cells can communicate with the relevant nodes in the cell securely as long as it holds the secret key materials from the same matrix. Meanwhile, each cell has the same number of neighboring cells, thus the memory cost in a sensor node is not related to the connectivity.

BLOM SCHEME

Blom scheme can ensure that any pair of nodes in the network can create a unique shared key. Specific process is as follows:

A central authority first constructs a $(\lambda+1)\times N$ matrix G over a finite field GF(q), where, N is the total number of sensor node and q>N. G is known to all users. Then central authority constructs a $(\lambda+1)\times(\lambda+1)$ symmetric matrix D, where, D must be secret and can not be exposed to any node. An $N\times(\lambda+1)$ matric $A = (D\cdot G)^T$ is computed, where, A is called Blom matrix. Because matrix D is symmetric, so it is easy to see that the matrix A·G is also symmetric.

$$K = A \cdot G = (D \cdot G)^T \cdot G = G^T \cdot D^T \cdot G = G^T \cdot D \cdot G = (A \cdot G)^T \quad (1)$$

From Eq. 1, we can see $K_{ij} = K_{ji}$, where K_{ij} is the element in row i and column j of matrix K. So, user pair(i, j) can use the K_{ij} and K_{ji} as the pairwise key. Specific means is as follows:

- The central authority assigns the i-th row of matrix G to the node n_i (i = 1...N)
- The central authority assigns the i-th column of matrix G to the node n_i (i = 1...N)
- The node n_i and n_j exchange the i-th column and the j-th column, then they can compute K_{ij} and K_{ji} using their private rows of A, respectively

Because the matrix G is public and is known to all users, so the information of matrix G can be delivered using plaintext during the phase of exchanging. In the Blom scheme, if any λ+1 columns of G are linearly independent, the scheme will have the desirable t-secure property. That is to say, in a network with N users the collusion of less than t + 1 users can not reveal any key held by other normal users.

The definition of key superset: A set S1 is a key superset of another key set S2 if every element in S2 is in S1. S1 may have elements which are not in S2.

We define a key subset S2 as a matrix D a node holds key subset S2 if the node stores the secret information generated from (D,G) which belongs to S2. Note that two nodes can calculate pairwise key if they hold the secret materials from the same matrix. Fig. 1 shows the model of key superset and the details of KS scheme.

PAIRWISE KEY ESTABLISHMENT BASED ON TRIANGLE CELL DEPLOYMENT MODEL

Attack model: Data in the process of sending and transmitting should ensure its confidentiality, integrity and freshness. As the broadcast characteristic of wireless communication, data in the process of transmitting may suffer from eavesdropping, tampering and replay.

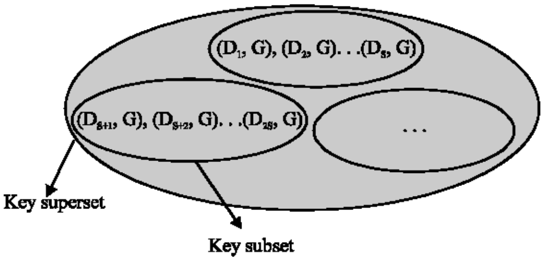

Fig. 1: Key superset model

Moreover, due to performance limitations of node itself, the attacker can easily capture any node and obtain the secret material in the node. When the number of captured nodes increases, the attacker may deduce and get more secret information, which will threaten the entire network security. Because the fact that nodes are compromised is impossible to avoid, we should reduce the impact from the compromised node or limit the impact within a small area as possible as we can, which will guarantee the security of entire network.

Network deployment model: In WSNs, as the node energy is limited, communication coverage is very small, thus usually only communicates with its neighboring nodes. According to the node deployment knowledge, the entire sensor network is devided into several non-overlapping triangle cells, Fig. 2 shows the congruent relationship between cell G_0 and its three neighboring cells G_1, G_2 and G_3. Accordingly, the sensor nodes are devided into the appropriate group, the groups of nodes can be deployed in the triangular cells, respectively. Thus the same group of nodes are more likely to be neighboring and establish pairwise key after deployment. According to the different deployment models, nodes may be subject to different distribution. In this paper we assume that the size of network is N, total of cells is G, each cell nodes are uniformly deployed.

Detail of key pre-distribution based on triangle cell deployment model: As shown in Fig. 1, each cell has public side with its three neighboring cells, thus each cell is among the three pairs of the cell. In the proposed scheme, KS scheme is applied to each pair of neighboring cells, if the neighboring cells store the secret key materials from the same matrix, they will calculate the pairwise key and establish a secure communication mechanism.

The proposed scheme includes four phases: key pre-distribution phase, pairwise key discovery phase, path-key establishment phase, node revocation and addition.

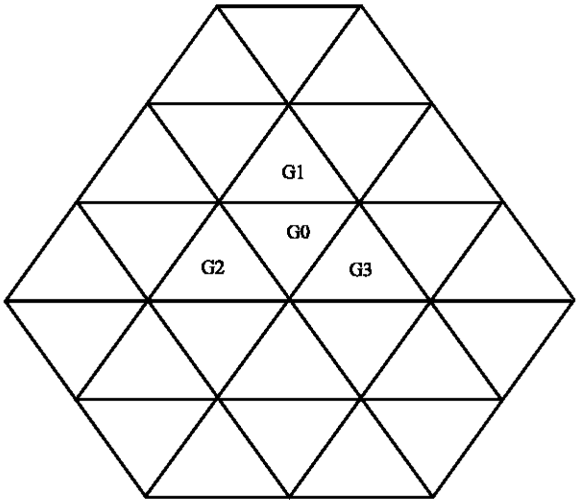

Fig. 2: Network deployment model

Key pre-distribution scheme: The purpose of this phase is to assign the secret key materials to each node. Neighboring nodes can establish pairwise keys after deployment using the secret key materials:

Construct Public Matrix: We assume that the size of network is N and there are N_c nodes in each cell . Each node has a unique positive identifier n_i for I = 1,2,...,N. The central authority constructs a $(\lambda+1)\times N$ matrix G like Eq. 2 over a finite field GF(q), where N is the size of network. Since, G is Vandermonde matrix and the node ID is used to be as the seed value of each column, thus each node only need to store a positive value which can be used to deduce the according column of matrix P to reduce the memory cost. Because the node ID is unique and it can be shown that any t+1 columns of G are linearly independent. Here, we choose $\lambda+2N_c-2$, the reason is to be stated later.

$$G=\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ n_1 & n_2 & n_3 & \dots & n_N \\ n_1^2 & n_2^2 & n_3^2 & \dots & n_N^2 \\ \dots & \dots & \dots & \dots & \dots \\ n_1^\lambda & n_2^\lambda & n_3^\lambda & \dots & n_N^\lambda \end{bmatrix} \tag{2}$$

Construct key superset: First secret symmetric matrix D_1, D_2...,D_S of size $(\lambda+1)\times(\lambda+1)$ are constructed randomly for each pair of neighboring cells in the entire network. We assum the total number of pairs of neighboring cells is N_S and the set of key subset (D_i, G) for i = 1,2...M is called key superset, where $M = S\times N_S$. Then matrix $A_i = (D_i, G)^T$ of size $N\times(\lambda+1)$ is computed for i = 1,2,...S, let $A_i(j)$ represent the j-th of matrix A_i. We can see that each secret matrix A_i is used by $2N_c$ nodes. In order to guarantee the secrecy of each secret matrix A_i, the (2N $_c$2)-secure Blom scheme should be used, that is to say λ should satisfy $\lambda = 2N_c\text{-}2$ and the size of A_i is $(2N_c\text{-}1)\times(2N_c\text{-}1)$.

Select key subset: Each node selects t(2≤t<s) secret key materials from the corresponding key sunset randomly . If node n_j selects matrix D_i, the i-th row of matrix A_i will be preloaded into node n_j’s memory space. For example, in Fig. 1, the pair of (G_0, G_1) is assigned a key subset and is corresponding to the matrix A_i, node n_j is in (G_0, G_1), thus the j-th row of A_i will be preloaded into the node n’s$_j$ memory space, so are the pair of (G_0, G_2) and (G_0, G_3).

Pairwise key discovery phase: After deployment, sensor nodes exchange their ID and the indices of key subset it carries . If two nodes share the secret key materials from the same matrix, they can calculate the shared key. Specifically, if nodes n_i and n_j store the i-th row and the j-th of matrix A_i, respectively, after exchanging their ID, node n_i can deduce the j-th column of matrix P using the node n_j’s ID, so is node n_j. The pairwise key can be calculated as follows:

$$K_{ij} = A_i(i)\cdot P(j) = A_i(j)\cdot P(i) = K_{ji} \tag{3}$$

Path-key establishment phase: After exchanging their ID and the indices of the subset it carries, if two nodes have no common secret key materials from the same matrix, they need to find an intermediate neighbor sensor node that shares pairwise keys with both of them to help establish an indirect key. Specifically, we suppose that there are intermediate nodes n_1,n_1,...n_i between the source node n_s and destination node n_d and each pair of adjacent nodes in the path has pairwise key. Source node n_s broadcasts the indices of the subset it carries, which is forwarded through the intermediate nodes securely until it discovers a bridge sensor node that shares a pairwise key with the two sensor nodes, respectively. The source node and destination node can then establish pairwise key along the message broadcast path in reverse.

Node revocation and addition: When the sensor nodes are compromised or captured, it is very likely to expose the pairwise key and the key subset, If more than λ sensor nodes that share the secret key materials from the same matrix are compromised, the according secret matrix is no longer considered secure . Thus we should remove these secret matrix as well as the IDs of all sensor nodes that share the secret key materials from the same matrix. When the number of the compromised nodes increase, the network connectivity will be affected, so the new nodes should be added. Prior to the deployment of new nodes, the according secret material is preloaded into the new node’s memory. After deployment,they can quickly establish direct or indirect shared key with their neighbouring nodes.

Since, the ID of each node is unique, the pairwise key is also unique to the pair of neighboring nodes. This property is very useful for secure communications, because it may not only provide encryption services, but also provide authentication service. Meanwhile, the sensor nodes are devided into several cells, nodes from specific cell are more likely to be neighbors of nodes from the same cell and those from nearby cells. In the entire network, the property that the pairwise key which is established along the message broadcast path is very few not only improves the resilience to node capture attacks, but also reduces the communication cost and saves memory space.

EVALUATION METRICS

Our scheme mainly discusses the following metrics:

Local connectivity: local connectivity is the probability that two nodes which are from the same cell or the neighbouring cells have at least one common secret key materials.

Memory cost: that is the memory requirement for storing key materials at one node.

Resilience against node captured: The additional key exposal probability that the keys stored in normal nodes are exposed should be as small as possible when some nodes are compromised is used to evaluate the resilience to the node capture attack.

Local connectivity: According to random graph theory, if a graph with N nodes is to achieve the given global connectivity P_c (Global connectivity is the ratio of the number of sensor nodes forming the largest isolated connected component in the final key graph G to the size of the whole network), the average degree of each node should satisfy Eq. 4:

$$d = \frac{N-1}{N}[\ln(N) - \ln(-\ln(P_c)] \tag{4}$$

For sensor network, the density is defined as:

$$D = \frac{N\times \pi R^2}{A} \tag{5}$$

where, N is the size of entire work, R is communication radiu of each node, A is the area of deployment region.

When the size of network is N, the communication radiu of each node is R, thus the average neighboring number of each node is D-1. Suppose the local connectivity between a node and its neighboring nodes is P_{local}, for a given global connectivity P_c, P_{local} should satisfy Eq. 6:

$$P_{local} = \frac{N-1}{(D-1)N}[\ln(N) - \ln(-\ln(P_c)] \tag{6}$$

In (Du *et al*., 2003), for a given global connectivity P_c in WSNs, the probability P_{share} that two nodes have at least one common secret key materials from the same matrix should satisfy Eq. 7:

$$P_{share} \geq P_{local} \tag{7}$$

In our scheme, the entire sensor network is devided into several non-overlapping triangle cells and KS scheme is applied to each pair of neighboring cells. Let $P_{inner\text{-}cell}$ presents the probility that any two nodes from the same cell share at least one common secret key materials from the same matrix, $P_{inter\text{-}cell}$ presents the probility that any two nodes from neighbouring cells share at least one common secret key materials from the same matrix, $P_{actural}$ presents the local connectivity in our scheme. $P_{inner\text{-}group}$ and $P_{inter\text{-}cgroup}$ can be denoted as follows:

$$P_{inner-cell} = 1 - \left(\frac{\binom{S}{t}\binom{S-t}{t}}{\binom{S}{t}^2}\right)^3 = 1 - \left(\frac{((S-t)!)^2}{(S-2t)!S!}\right)^3 \tag{8}$$

$$P_{inter-cell} = 1 - \frac{\binom{S}{t}\binom{S-t}{t}}{\binom{S}{t}^2} = 1 - \frac{((S-t)!)^2}{(S-2t)!S!} \tag{9}$$

$$P_{actural} = 1 - \left(\frac{\binom{S}{t}\binom{S-t}{t}}{\binom{S}{t}^2}\right)^4 = 1 - \left(\frac{((S-t)!)^2}{(S-2t)!S!}\right)^4 \tag{10}$$

For a given global connectivity P_c, we can select appropriate parameters(such as t) to enable $P_{inter\text{-}cell} \geq P_{local}$, $P_{inner\text{-}cell} \geq P_{local}$ and $P_{actrual} \geq P_{local}$. Because $P_{actrual} \geq P_{inner\text{-}cell}$, only $P_{inter\text{-}cell} \geq P_{local}$ can the global connectivity P_c be guaranteed

In E-G scheme (Eschenauer and Gligor, 2002), each node randomly selects m keys from the key pool S, so the local connectivity is:

$$P = 1 - \frac{\binom{S-m}{m}}{\binom{S}{m}} \tag{11}$$

In (Chan and Perrig, 2005), each node has shares key with other $2(\sqrt{N}-1)$, so the local connectivity is:

$$P = \frac{2(\sqrt{N}-1)}{N} \tag{12}$$

In (Du *et al*., 2003), each node randomly selects τ sub-space key from the multiple-space key ω in WSNs which is not partitioned, so the local connectivity is:

$$P = 1 - \frac{\binom{\omega-\tau}{\tau}}{\binom{\omega}{\tau}} \tag{13}$$

In our proposal, the KS scheme is applied to each pair of adjacent cells and we can select parameters such as S and T appropriately to achieve high local connectivity. In E-G scheme, due to the memory limitation, the number of selected keys should not be too large and thus the local connectivity which is related to the memory cost may be low. In (Chan and Perrig, 2005), if the size of whole network is large, the local connectivity will be more lower. In (Du *et al*., 2003), because the multiple-space key is applied to the entire network, it will be difficult to balance the security and efficiency. We will use experiments to analyse comparatively in part 5.

Memory cost: After deployment, each node is preloaded with 3t rows secret material which are from different matrix A and their neighboring's ID, so the memory cost of each node is 3t+D-1. However, the actual memory cost is less than 3t+D-1, because after the establishment of pairwise keys, the unused rows can be removed to save memory resources. In part 5, we will see that for the given global connectivity P_c = 0.999, D = 5.76π and t should satisfy t≥2. In E-G (Eschenauer and Gligo, 2002) and (Du *et al*., 2003), in order to maintain the probability that establishes direct shared key among any two nodes in a high level, the number of selected sub-key and sub-space key should not be small. For example, in E-G scheme, when the key pool S is 100000, only when the number of selected key reach to 250 can the probability that any two nodes establish direct share key equal to 0.5. Compared to our scheme, E-G scheme need more memory and the local connectivity is low. Meanwhile, if the number of selected sub-key or sub-space key is too large, although the high local connectivity is maintained, it means that an attacker can obtain more key material by compromising a smaller number of nodes, thus a good tradeoff between local connectivity and security performance is difficult to satisfy. In Chan and Perrig, 2005), the memory cost of each node is $2(\sqrt{N}-1)$, where N is the size of entire network, we can see that as the size of network increases, the space to store keys of each node also increases accordingly. A merit of our scheme is that the memory cost is unrelated with local connectivity, thus it is easy to achieve high level security. Besides, our scheme is scalable in that the number of cells can increase while the memory cost of each node is almost fixed.

Resilience against node capture: The additional key exposal probability that the keys stored in normal nodes are exposed should be as small as possible when some nodes are compromised is used to evaluate the resilience to the node capture attack. In our scheme, KS scheme is applied to each pair of neighboring cells, each pair of nodes select randomly a certain number of secret key materials from the key subset. As long as the number of captured nodes are less than $\lambda(\lambda = 2N_c\text{-}2)$, the secrecy of the secret material in key subset will be guaranteed. That is to say even if the number of captured nodes equal to λ, the remaining two nodes can still communicate securely, which means the additional key exposal probability is zero. Thus, our scheme has perfect resilience to the node capture attack.

In E-G scheme (Eschenauer and Gligo, 2002), the additional key exposal probability may be calculated as Eq. 14:

$$P = 1-(1-\frac{m}{S})^{x} \tag{14}$$

where, x is the number of captures nodes, m is the size of a selected key subset, S is the size of key pool.

In (Du *et al*., 2003), the additional key exposal probability may be calculated as Eq. 15:

$$P = \sum_{j=t+1}^{x}\binom{x}{j}\left(\frac{\tau}{\omega}\right)\left(1-\frac{\tau}{\omega}\right)^{x-j} \tag{15}$$

where each node has τ spaces from ω spaces and x is the number of captures nodes, t is the safe threshold value.

As shown in Eq. 14, if the parameters m and S are definite value, the additional key exposal probability P_C will increase with the growth of the captured nodes number. In (Du *et al*., 2003), if the number of captured nodes exceed the safe threshold value, P_C will increase rapidly. We will use experimental results to illustrate the above analysis in part 5.

EXPERIMENTAL SIMULATION

We use the setup in Table 1 for our simulation and numerical analysis.

Local connectivity: Based on Table 1 and Eq. 4, we can obtain:

$$P_{local} = \frac{N-1}{(D-1)N}[\ln(N)-\ln(-\ln(P_c))] = 0.3271 \tag{16}$$

According to the analysis of Section 4.1, for given global connectivity P_c, $P_{actrual}$ should satisfy Eq. 17:

$$P_{actural} \geq P_{local} \tag{17}$$

Figure 3 gives $P_{inter\text{-}group}$ (sharing at least one common secret key materials from the same matrix) as a function of key subset. As shown in Fig. 3, for the given global connectivity P_c, when the key subset S equals to 10, if only $t \geq 2$, inequality Eq. 17 can be satisfied.

In E-G scheme, if the size of key pool S is 100000, the memory for storing key materials in each node is 200, $\omega = 9$, $\tau = 2$; S = 10, t = 2, Based on the equation in Section 4.1, we can obtain the results which is shown in Fig. 4.

As shown in Fig. 4, compared to other schemes, our scheme has very high local connectivity, which means each node can establish direct keys with almost all its neighbors, thus can save a lot of energy on the establishment of indirect keys along the message broadcast path. Du's scheme is used to the entire network and the selected sub-space key should not be too large, so the local connectivity which is related to the memory cost is low. The local connectivity in E-G scheme and Chan's scheme is also related to the number of selected keys and the size of entire network respectively and it is difficult to balance the security and efficiency. The results commendably support our analysis in part 4 and objective of the paper.

Table 1: Simulation setup

Symbol	Value	Description
N	10000	Size of the network
P_c	0.999	Global connectivity
A	1000×1000 m^2	Network deployment area
R	24 m	Node communication range

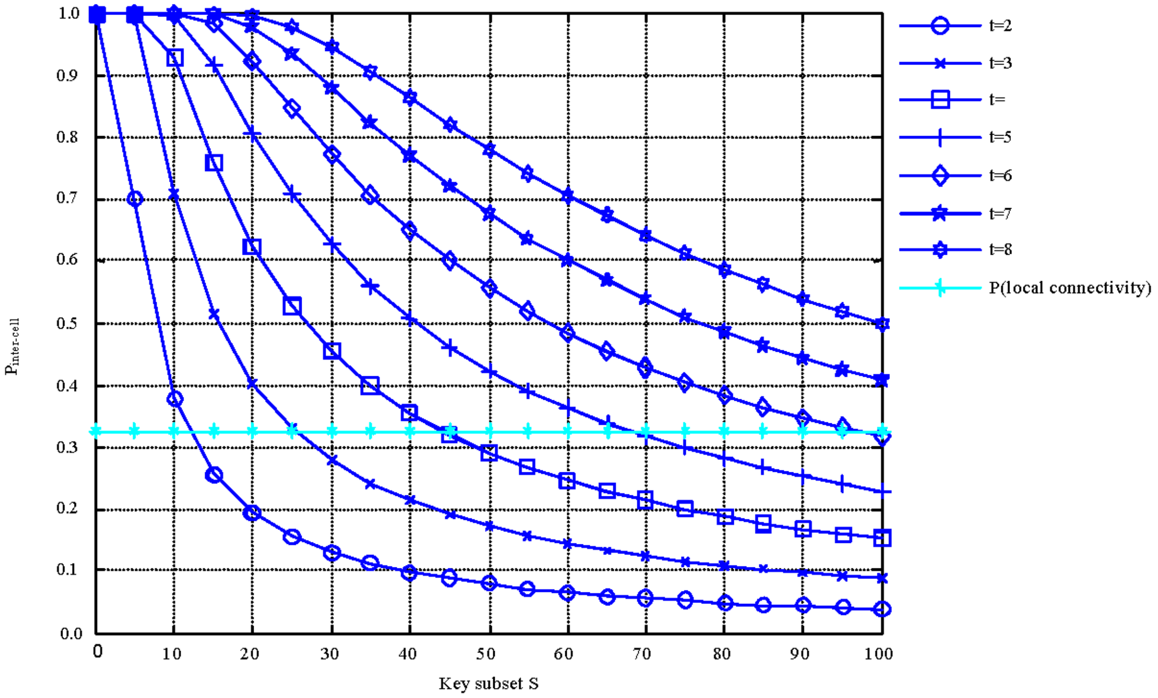

Fig. 3: (Sharing at least one common secret key materials from the same matrix) as a function of key subset

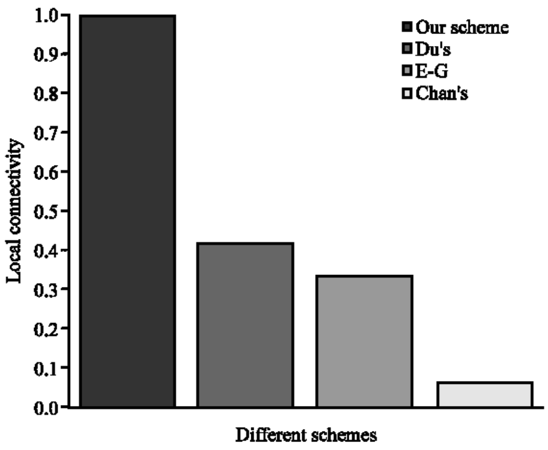

Fig. 4: Local connectivity of different schemes

Resilience against node capture attacks: The additional key exposal probability is used to evaluate the resilience to the node capture attack. In our scheme, we obtain the $(2N_c-2)$-secure property in each pair of neighboring cells by setting $\lambda = 2N_c-2$, which means that even though up to $(2N_c-2)$ nodes are captured the remaining two nodes in the neighboring cells can still communicate securely. Hence, in our proposal when an adversary captures some nodes, he/she only knows the secret key materials in the captured nodes but can not derive the keys stored in other normal nodes, which means the additional key exposal probability is zero. Thus, our scheme has perfect resilience to the node capture attack. the additional key exposal probability is zero, the results are stated in Fig. 5.

As shown in Fig. 5, compared to other schemes, our scheme has excellent resilience against node captured attacks. Because in our scheme, the entire network is devided into several non-overlapping triangle cells, KS scheme is applied to each pair of neighboring cells and the consequence of node capture attack is restricted within a small range, which can guarantee that the communication between sensor nodes is secure. Du's scheme has the property that when the number of captured nodes reach to a threshold value, the additional key exposal probability will increase rapidly. What is different with Du's scheme is that the additional key exposal probability in E-G scheme will increase with the number of captured nodes. The performance results again well support our analysis in part 4 and our design goal.

Several schemes have been proposed for use in WSNs, such as the use of elliptic-curvecryptography (ECC), the use of group and keyed-hash Chain (Hussian *et al*., 2009). Eschenauer and Gligo (2002) first proposed Random Key Predistribution Scheme which is based on probability density and random graph theory. Before deployment, each node is preloaded into a random subset of key from a large key pool. Any

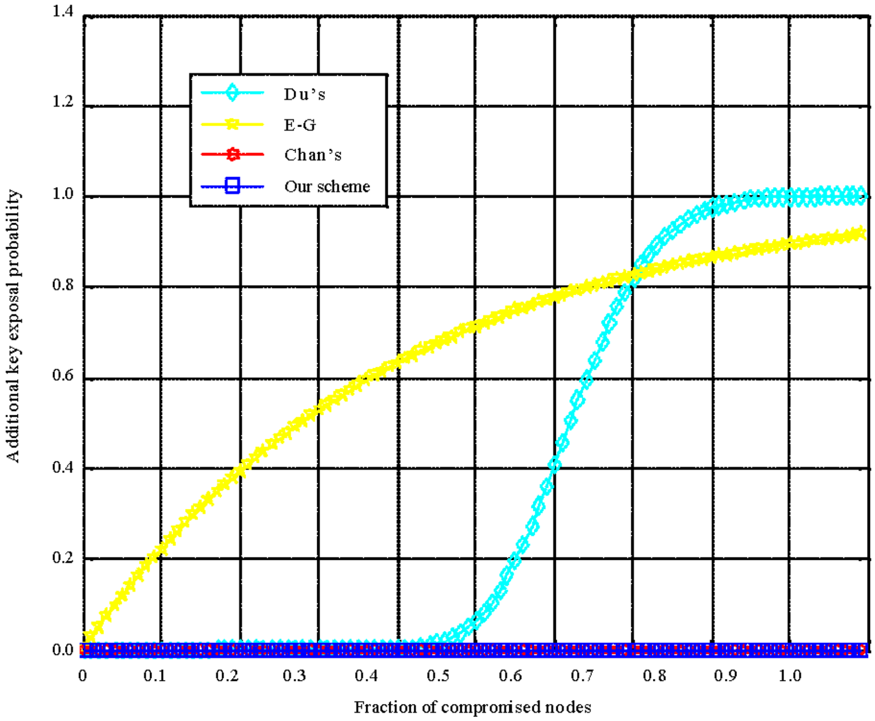

Fig. 5: The additional key exposal probability as a function of fraction of captured nodes

two nodes in the communication range can talk to each other only if they share a common key. Chan *et al.* (2003) further improved the E-G scheme and developed the q-composite key establishment scheme and random pairwise key scheme, The difference between this scheme and the previous one is that the q-composite scheme requires two nodes to find q (with q>1) keys in common before establishing shared key, which improves the resilience of the network. Liu and Ning (2003) developed a framework in which pairwise keys are predistributed by using bivariate polynomials, Their scheme takes advantage of expected node locations to improve the efficiency of establishing shared key. Moreover, (Liu and Ning, 2005) used node deployment knowledge to improve the local secure connectivity. Their approach assumes a group-based deployment model, in which the entire network is devided into several non-overlapping square cells and nodes are devided into groups, each of which is deployed in a cell. Meanwhile, the depolyment knowledge and hierarchical clustering algorithm are used to achieve a good performance in term of lifetime and balance power consumption (Wei *et al.*, 2007; Xin *et al.*, 2008). Du *et al.* (2003) proposed a multiple-space key pre-distribution scheme which is based on Blom scheme. This scheme exhibits a nice threshold property: when the number of compromised nodes is less than the threshold, the probability that communications between any additional nodes are compromised is close to zero. Moreover, Du *et al.* (2003) proposed a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments, which improves the performance (including connectivity, memory usage and network resilience against node capture) of sensor networks. Chan and Perrig (2005) proposed a Peer Intermediaries for Key Establishment (PIKE), a class of key-establishment protocols that involves using one or more sensor nodes as a trusted intermediary to facilitate key establishment. Although the existing schemes can improve some these metrics, they have a common weakness that they are vulnerable to node capture attacks.

CONCLUSIONS

In this study, we propose an efficient scheme against node capture attacks using secure pairwise key in wireless sensor networks. We utilize key superset scheme and the triangle cell deployment model to restrict the consequence of attacks within a small range, which greatly enhances the resilience against node capture attacks. We presented both the analytical and numerical results, compared to existing schemes, high local connectivity which is unrelated to memory cost is achieved and the resilience against node capture attacks outperforms others.

ACKNOWLEDGMENTS

This study was partially or fully supported by National Basic Research Program of China (973 Program) under Grant No. 2006CB303000 (2006.9-2011.8, Hunan University), 2009CB326202 (2009.4-2011.8, Hunan University) and 2010CB334706 (2010.4-2013.3, Hunan University). Key Program of National Natural Science Foundation of China under Grant No. 60736016 (2008.1-2011.12, Hunan University). National Natural Science Foundation of China under Grant No.60873198 (2009.1-2011.12, Hunan University), 60973128 (2010.1-2012.12, Hunan University) and 60973113 (2010.1-2012.12, Hunan University).

REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramamiam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Networks, 38: 393-422.

Chan, H. and A. Perrig, 2005. Pike: Peer intermediaries for key establishment in sensor networks. Proceedings of IEEE Conference on Computer Communications, Mar. 13-17, Pittsburgh, PA, 524-535.

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. Proceedings of the IEEE Symposium on Security and Privacy, May 11-14, Berkeley, CA, 197-213.

Conti, M., R.D. Pietro, L.V. Mancini and A. Mei, 2007. Efficient and distributed protocol for the detection of node replication attacks in wireless sensor networks. Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing, Sept. 09-14, Montreal, Quebec, Canada, pp: 80-89.

Conti, M., R.D. Pietro, L.V. Mancini and A. Mei, 2008. Emergent properties: Detection of the node-capture attack in mobile wireless sensor networks. Proceedings of the 1st ACM Conference on Wireless Network Security, March 31-April 2, New York, USA., pp: 214-219.

Du, W., J. Deng, Y.S. Han and P.K. Varshney, 2003. A pairwise key predistribution scheme for wireless sensor networks. Proceedings of the ACM Conference on Computer and Communications Security, Oct. 27-30, New York, NY, USA, 42-51.

Du, W., J. Deng, Y.S. Han, S. Chen and P.K. Varshney, 2004. A key management scheme for wireless sensor networks using deployment knowledge. Proceedings of IEEE Conference on Computer Communications, Mar. 7-11, NY, USA, 586-597.

Eschenauer, L. and V. D. Gligor, 2002. A key-management scheme for distributed sensor networks. Proceedings of the ACM Conference on Computer and Communications Security, Nov. 18-22, Washington, DC, USA, 41-47.

Hussian, S., M.S. Rahman and L.T. Yang, 2009. Key predistribution scheme using keyed-hash chain and multipath key reinforcement for wireless sensor networks. Proceedings of the PerCom 2009 IEEE International Conference on Pervasive Computing and Communications, Mar. 09-13, Galveston, TX, USA, 1-6.

Liu, D. and P. Ning, 2003. Establishing pairwise keys in distributed sensor networks. Proceedings of the ACM Conference on Computer and Communications Security, Oct. 27-30, Washington D.C., USA, 52-61.

Liu, D. and P. Ning, 2005. Establishing pairwise keys in distributed sensor networks. ACM Trans. Inform. Sys. Security, 8: 41-77.

Michael, H., N. Thomas and L. Elfed, 2009. Security for wireless sensor networks: A review. Proceedings of the IEEE Sensors Applications Symposium (SAS), Feb. 17-19, Limerick, 80-85.

Perrig, A., J. Standovic and D. Wagner, 2004. Security in wireless sensor networks. Commun. ACM, 47: 53-57.

Taguea, P. and R. Poovendran, 2007. Modeling adaptive node capture attacks in multi-hop wireless networks. Ad Hoc Networks, 5: 801-814.

Wei, D., H.A. Chan and B. Silombela, 2007. Rectangular grids design to balance power consumption for homogeneous sensor networks with high node density. Inform. Technol. J., 6: 827-834.

Xin, G., W. H. Yang and B. DeGang, 2008. EEHCA: An energy-efficient hierarchical clustering algorithm for wireless sensor networks. Inform. Technol. J., 7: 245-252.

Yu, Z. and Y. Guan, 2008. A key management scheme using deployment knowledge for wireless sensor networks. IEEE Trans. Parallel Distributed Syst., 19: 1411-1425.