An improved key pre-distribution scheme based on the security level classification of keys for wireless sensor networks

Jianmin Zhang*, Hua Li and Jian Li

College of Computer,
Henan Institute of Engineering,
Zhengzhou 451191, China
Email: zjm1996@163.com
Email: laklihua@2980.com
Email: zzhngc@126.com
*Corresponding author

Abstract: The use of wireless sensor networks (WSNs) in any real-world application requires a certain level of security. To provide security of operations such as message exchange, key management schemes have to be well adapted to the particularities of WSNs. Unfortunately, the resource limitation of sensor nodes poses a great challenge for designing an efficient and effective key establishment scheme for WSNs. This paper proposes a novel key management scheme. In the proposed scheme, the pre-distributed keys in nodes are classified different security levels and the higher security level of the pre-distributed key in compromised nodes will disclose the fewer pre-distributed keys in the uncompromised nodes than that of the lower security level of the pre-distributed key. The proposed scheme is analysed based on connectivity, resistance against attacks, memory consumption and communication overhead. Simulation results confirm that the proposed scheme has a good resilience against node compromising attacks compared to the existing schemes.

Keywords: wireless sensor networks; WSNs; key predistribution; security level classification; hash function.

Reference to this paper should be made as follows: Zhang, J., Li, H. and Li, J. (2020) 'An improved key pre-distribution scheme based on the security level classification of keys for wireless sensor networks', *Int. J. Information and Computer Security*, Vol. 12, No. 1, pp.40–52.

Biographical notes: Jianmin Zhang received his PhD in Computer Science from Huazhong Science University in 2007, and currently is an Associate Professor of College of Computer at Henan Institute of Engineering. His research areas include wireless sensor network, things of internet and network security.

Hua Li is an Instructor of College of Computer at Henan Institute of Engineering. His research areas include wireless sensor network, network security and algorithm design.

Jian Li is a Professor of College of Computer at Henan Institute of Engineering. His research areas include wireless sensor network and network security.

1 Introduction

Wireless sensor networks (WSNs) are compromised of large number of self-configuring of tiny sensor nodes communicating among themselves using radio signals (Liang et al., 2014; Rawat et al., 2014). Since their advent, WSNs have gained a great deal of attention and have been deployed for a wide variety of applications, including military sensing and tracking, patient status monitoring, traffic flow monitoring (Puccinelli and Haenggi, 2005; Padmavathi and Reddy, 2014). Since sensor nodes may be located in hostile locations, particularly with military applications, security is an essential issue in these networks. Then WSNs are usually subject to many types of security threats and attacks, such as the capture of a sensor node, intentionally providing false information, impersonation, data modification, eavesdropping, etc. Therefore, security considerations, such as authentication and confidentiality must be undergone to ensure integrity of sensor node and proper functionality of the network. Key management protocols are the core of these security issues. The goal of key management in WSNs is to establish secure links between neighbour sensor nodes.

However, due to the constrains on WSNs traditional pairwise key establishment techniques such as public key cryptography and key distribution centre (KDC) cannot be applied directly to WSNs. Due to their importance, many key management solutions have been proposed for WSNs. The existing schemes can be classified into two categories according to whether the solution is based on symmetric cryptography or asymmetric cryptography. Asymmetric cryptography offers better resistance against sensor node compromising attacks and allows a high scalability, but requires an additional heavy part on the software and hardware of sensor nodes. Furthermore, it is still energy consuming. Even with the present day technology, use of public cryptographic (asymmetric functions) is not appropriate due to the computational limitations of sensor nodes (Ge et al., 2016). A particular symmetric approach in WSNs is to use key pre-distribution with the sensor nodes, resulting in low cost key establishment. In this regard, various schemes have been proposed for key management in WSNs.

In this paper, we exploit the use of the probabilistic key predistribution scheme in conjunction with the hash function to establish a secure link between sensor nodes and improve network resilience to nodes captures. In the proposed scheme, the keys in sensor nodes are classified to different security levels and with property of the one-way hash function, the pre-distributed keys with higher levels in the compromised nodes will reveal fewer pre-distributed keys in the uncompromised nodes than that of pre-distributed keys with lower levels in the compromised nodes.

The rest of this paper is organised as follows. Section 2 presents related work. Section 3 presents the proposed scheme in details. Section 4 describes the performances of our scheme, and Section 5 concludes the paper.

2 Related works

In this section, we focus on the solution based on symmetric cryptography. We briefly review and analyse some existing key management schemes.

Eschenaure and Gligor (2002) proposed a random key predistribution scheme (refer to as EG scheme) for WSNs. It also constitutes the foundation of the subsequent of key distribution schemes in WSNs. In this scheme, before deployment, a large key pool which contains many distinct keys with key identifier is randomly generated. And each sensor node is loaded with a predefined number of keys that constitute its key rings. After deployment the network, a pair of neighbouring nodes may have shared common keys to establish a secure connection. In the literature, this procedure of discovering of the common key between two sensor nodes is called shared key discovery. If there is no common key between two nodes, they have to establish a key through an intermediate sensor node which has common keys with both sensors, which is called path key establishment. Unfortunately, this scheme cannot provide sufficient security as the number of compromised increases. To improve the network resilience against the node capture attack, Chan et al. (2003) generalised this scheme to the q-composite scheme , in which two nodes can establish a secure communication link only if they share at least q ($q > 1$) common keys. They showed that the network resilience against the node capture attach can be improved when number of compromised nodes is small. Because of the low-cost hardware, sensor nodes are not tamper resistant devices. If a sensor node is captured, all its stored cryptographic information can be easily extracted by the adversary. In the EG and the q-composite scheme, all sensor nodes use the same key pool. This implies that the security of the network is gradually erode as keys formed key pool are compromised by an adversary that captures more and more sensor node. As the number of compromised sensor nodes increases, the fraction of the affected keys increases quickly. As a result, a small number of compromised nodes may affect large fraction of the secure link. This problem is defined as network resilience in WSNs, which is used to evaluate how much fraction of the communication between non-captured nodes will be compromised when a certain number of sensor nodes are captured by the adversary.

Liu et al. (2005) proposed a new key predistribution scheme, which is combined the basic scheme proposed by Eschenaure and Gligor (2002) with Blundo's polynomial-based key distribution scheme (Blundo et al., 1992). In this scheme, every sensor node is preloaded with coefficient of symmetric bivariate polynomial computed at one of its variables using its identification. The symmetry property of the polynomial allows two nodes to get their pairwise key respectively. This scheme exhibits a nice threshold property, which means that 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. A similar method was also developed by Du et al. (2005), in which matrices are used instead of polynomials. Later, these two schemes have been further explored in Dai and Xu (2010), Delgosha and Fekri (2009) and Rasheed and Mahapatra (2011). These methods are all immune to node compromised attacks when the numbers of the compromised nodes are below a given value. The main drawbacks of these methods are that the attackers can get the whole communication keys once the number the compromised nodes are greater than the threshold value and besides they introduce higher storage and computation overheads.

Alternative approaches exploit the knowledge of the sensor nodes development. Du et al. (2006) proposed several schemes that use location information. The goals of such schemes are to save memory costs while maintaining a high level of security. Zhou et al.

(2009) considered the priority of deployment packets in order to avoid unnecessary key assignments. In this scheme, they assumed that the sensor nodes are deployed in groups of some sensor nodes over a rectangular area. In the key pre-distribution phase, the original key pool is divides into many smaller pools, each of which is associated to different group. This group-based deployment model was further developed in Bag and Roy (2013) and Lee and Kwon (2014). Although these schemes can gain substantial improvement over exiting schemes that do not exploit deployment, they are only suitable to scenarios where deployment knowledge can be explored and this kind of information is not available in a generic deployment scenario.

Another important works in the literature that aims increase the network resiliency without reducing secure connectivity was proposed for multiphase sensor networks. In the robust key (RoK) pre-distribution (Castelluccia and Spognardi, 2007), the key chains of each generation are constructed from two different key pools and the pre-distributed keys have limited lifetimes and are refreshed periodically. As a result, a network that is temporarily attacked automatically self-heals. In the random generation material (RGM) key predistribution scheme (Ergun et al., 2011), each generation of deployment has its own random keying material and pairwise keys are established between node pairs of particular generations. These keys are specific to these generations. Das (2012) proposed a new dynamic random key establishment mechanism in large-scale distributed sensor networks. One good property of the dynamic key distribution scheme is that the already deployed nodes in a deployment phase refresh their own keys in key rings before another deployment phase occurs. Zhou et al. (2014) proposed a key management scheme for multiphase deployment WSN. In the scheme, the deployment field is divided into hexagonal cells, each cell has deployment point, and nodes which have the same point form a group. The strength of the key pre-distribution schemes for multiphase sensor networks is that it provides high resilience against node capture as compared to that for the other existing random key distribution schemes. However, the main disadvantages of these schemes compared with the EG and q-composite schemes reside on the higher computation effort for generating the keys, and on the fact that the total number of generations must be determined in advance. Another inconvenient with these schemes is that the network should remain loosely synchronised.

In conclusion, we can see that the existing schemes do not meet all the requirements of WSNs. When connectivity is met, security is dropped, when security is achieved, resource consumption is high, etc. In this paper, we propose a novel scheme that provides a trade-off between resource consumption and security. The proposed scheme uses one-way hash function to classify to the pre-distributed keys in nodes into different security levels. In spite of its simplicity, the proposed scheme perform better in terms of network resilience to node capture than EG and q-composite schemes.

3 The proposed scheme

In this section, we discuss the main motivations behind development of our scheme and describe how the proposed key predistribution scheme works in detail.

3.1 Motivation

In the EG scheme, the keys pre-distributed in sensor nodes are selected randomly without replacement from the key pool, the same key may be repeated for several pair of neighbour nodes throughout the network. From the analysis of the EG scheme (Eschenaure and Gligor, 2002), it follows that the security degrades dramatically if the key pool size is chosen smaller. On the other hand, to keep higher network connectivity the key pool size should not be chosen larger. These problems also exit for the q-composite scheme (Chan et al., 2003).

To overcome the aforementioned problems, we introduce a new random key pre-distribution scheme for alternative approaches to the key pre-distribution and direct key establishment phase of the EG scheme. Our scheme is motivated by the following considerations. As it is infeasible to increase the key pool size to strength the security of network, the alternative approach is to decrease the effects due to compromised secret material in the compromised nodes. To do this, the pre-distributed keys in the nodes are classified into different security levels by using the one-way hash function. With the one-way property of the hash function, the adversary cannot always use the compromised nodes to get the keys in the uncompromised node.

3.2 Details of the scheme

The general framework of the proposed scheme consists of three phases: initialisation phase, shared-key discover, and path-key establishment phase. Although path-key establishment phase is the same as EG scheme and q-composite scheme, key pre-distribution phase and shared-key discover phase are different in the previous schemes. The details of initialisation phase and shared-key discover phase in our scheme are described below.

3.2.1 Initialisation phase

This phase is done offline by a key generation centre (KGC) before deploying the sensor nodes in a target field. The main task of this phase is to assign the pairwise key generation information to sensor nodes. It consists of the following steps:

Step 1 The KGC generates a large pool of key seeds over the finite field F_q and each key seed has a unique identification ID.

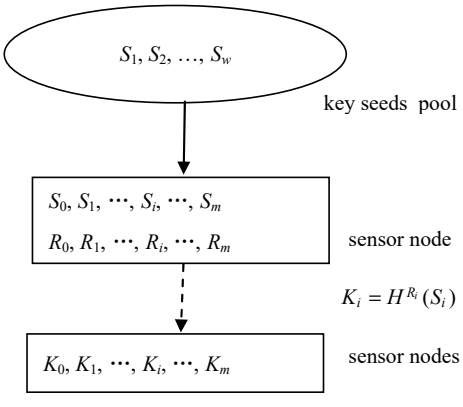
Step 2 For each sensor node, the KGC randomly picks m keys from the key pool as seeds and generates m random number R_i, $0 \le R_i < R$. Here, we call R the system security level. And for each seed S_i, there is a corresponding random number R_i in the nodes. Then the pre-distributed keys are computed as follows

$$K_i = H^{R_i}(S_i) \tag{1}$$

here, H is a one-way hash function . R_i is called the security level of key K_i in the sensor node. The identification ID of key K_i is the same as the ID of the seed S_i.

An example of initialisation of the proposed scheme is illustrated in Figure 1.

Figure 1 A sample key pool generation



3.2.2 Shared key discovery phase

Once the nodes are deployed in the target field, they need to establish link keys with each of their neighbours. To discovery whether two neighbour nodes can establish a common key, the sensor nodes disclose a list of ID of the keys and their corresponding security level.

Suppose the sensor node u and sensor node v are neighbours. And these two sensor nodes have some common key ID's. These two nodes selected the key whose ID is the lowest in these common keys to compute their pairwise. Suppose the pre-distributed key in sensor u is K_{ut} and there corresponding security level is $R_{ut,}$ and the pre-distributed key in sensor v is K_{vt} and there corresponding security level is $R_{vt,}$ and the seed of K_{ut} and K_{vt} are both S_t.

Then the sensor node u can computes pairwise keys between sensor node u and v as follows:

$$K_{uv} = H^{\alpha}(K_{ut}) = H^{\lambda}(S_t) \tag{2}$$

here

$$\alpha = \begin{cases} 0 & \text{if } R_{ut} \geq R_{vt} \\ R_{vt} - R_{ut} & \text{if } R_{ut} \geq R_{vt} \end{cases} \qquad \lambda = \max(R_{ut}, R_{vt}),$$

$R_{ut}(R_{vt})$ is the security level of key $K_{ut}(K_{vt})$ in node $u(v)$.

Similarly, the sensor nude v can compute the pairwise key as follows.

$$K_{vu} = H^{\beta}(K_j) = H^{\sigma}(S_t) \tag{3}$$

here,

$$\beta = \begin{cases} 0 & \text{if } R_{vt} \geq R_{ut} \\ R_{ut} - R_{vt} & \text{if } R_{vt} < R_{ut} \end{cases} \qquad \sigma = \max(R_{ut}, R_{vt})$$

Obviously, $\lambda = \sigma$ then $K_{uv} = K_{vu}$.

Here, we define the λ (or σ) is the security level of the pairwise key K_{uv} (or K_{vu}).

4 Performance analysis

In this section, we evaluate the proposed scheme. The evaluation metrics includes the storage, communication and computation overhead of each node in the network, the network connectivity, the security of the scheme.

4.1 Overhead

- *Memory overhead:* according to our scheme, during the initialisation phase each sensor needs to store m keys over F_q. In addition, each node needs to store the ID of the keys and the security level of the keys. Assume the ID's of keys are chosen from a finite field $F_{q'}$ and the security levels of keys are chosen from a finite field $F_{q''}$. Thus, the overall storage overhead of each sensor is $m(\log q + \log q' + \log q'')$ bits. Compare to the EG scheme (Eschenaure and Gligor, 2002) and q-composite scheme (Chan et al., 2003), there more $m\log q''$ bits storage needed.
- *Communication overhead:* in the shared key discover phase each sensor needs to disclose of a list of the IDs and security levels of m keys to its neighbour nodes. Then the communication overhead of each node is $m(\log q' + \log q'')$ bits. Like the memory overhead, there are more than $m\log q''$ communication overhead needed than that of the EG scheme and q-composite scheme.
- *Computation overhead:* as in the initialisation phase the sensor nodes do not include computation, here we only analyse the computation overhead in the shared pairwise key discover phase. From formula (2) and (3), we get each sensor node only need do $1 + |\alpha - \beta|$ times one-way hash computation. In the EG scheme, there is no additional one-way hash computation needed to compute the pairwise keys. And in the q-composite scheme, there is hash computation needed to compute the q common keys, so there are more $|\alpha - \beta|$ times hash computations needed in our scheme than that of in the q-composite scheme. Now we give the quantitative analyses relationship between the system security level and the computation needed to compute pairwise.

Suppose the system security level is R, and the security of levels of pre-distributed keys in two nodes are a and b respectively. Without loss of generality, let $a \le b$. Then the computation need is:

$$f(R) = \sum_{i=0}^{R-1} \frac{1}{R} \sum_{j=i}^{R-1} \frac{j-i}{R} = \frac{R^2 - 1}{6R} \tag{4}$$

4.2 Local connectivity

Local connectivity is the probability of two neighbour sensor nodes establishing communication key directly. It is an important metric to evaluate a key predistribution

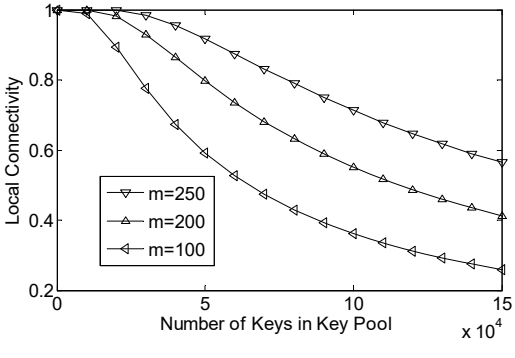
scheme. To achieve a desired global connectivity, the probability of direct key establishment must be higher than a certain threshold value.

From the shared pairwise key discover method, we know that if two sensor nodes have common key ID these two nodes can establish a pairwise key directly. As there are w key seeds in the key pool and each sensor node has m pre-distributed key, the local connectivity is:

$$P_{local} = 1 - \frac{\binom{w}{m}\binom{w-m}{m}}{\binom{w}{m}\binom{w}{m}} = 1 - \frac{\binom{w-m}{m}}{\binom{w}{m}} \tag{5}$$

Figure 2 show the probability to establish direct key given different number of the keys preload in each sensor. In general, the larger m is, the higher the probability establishing a direct key between two physically neighbouring nodes. The reason is that the more key in each sensor node, the higher the probability of two sensor nodes have the same key seeds. But larger m is, the more memory is needed in sensor node.

Figure 2 The probability of establishing direct keys between neighbours for different key pool size and memory needed in nodes



4.3 Security analysis

In this subsection, we first study the resiliency of the proposed scheme against sensor capture through probability analysis. Then we compare our scheme with some existing schemes by calculating the fraction of compromised communication among non-compromised nodes.

Node capture attack is one of the most serious threats in WSNs. An adversary may physically capture sensor nodes and compromise the stored secret information since sensor nodes are not tamer resistant due to their low cost. We assume that if a sensor node is captured all the information in the sensor node will be disclosed by the adversary. The resilience of the scheme is measured as the fractions of total network communication that are compromised when x sensor nodes are captured (Eschenaure and Gligor, 2002).

4.3.1 Resilience against nodes capture

In this section, we calculate the fraction of compromised data-communication among non-compromised sensor nodes. To compute this fraction, we calculate the probabilities of compromising the pairwise keys between any two non-compromised sensor nodes after x sensor nodes have been compromised.

Suppose K be the pairwise key used by two non-compromised sensor node u and v. The K is derived by using the seed S_t and the security level of the corresponding pre-distributing keys in node u and v are R_{ut} and R_{vt} respectively. Then $K = H^{|R_{ut}-R_{vt}|}(S_t)$.

Let $A(i)$ be the joint event that there is at least one pre-distributed key whose seed is S_t in each of the i compromised nodes and the pairwise K can be derived from one of these keys in each of the i compromised nodes . Let D_x be the event that x sensor nodes have been compromised. The probability of communication key K between two unknown node u and v when x nodes have been compromised is:

$$P_b = P\left(A(1)\middle|D_x \cup A(2)\middle|D_x \cup \cdots A(i)\middle|D_x \cup \cdots \cup A(x)\middle|D_x\right) \tag{6}$$

As the events $A(1)$, $A(2)$,…, $A(i)$, …, $A(x)$ are mutually exclusive, we have

$$\begin{aligned} P_b &= P\left(A(1)\,|\,D_x\right) + P\left(A(2)\,|\,D_x\right) + \cdots P\left(A(i)\,|\,D_x\right) + \cdots + P\left(A(x)\,|\,D_x\right) \\ &= \sum_{i=1}^{x} P\left(A(i)\,|\,D_x\right) \end{aligned} \tag{7}$$

Let $B(i, S_t)$ represents the event that there is at least one pre-distributed key whose seed is S_t in each of the i compromised nodes. Let $C(R_{ut}, R_{vt})$ to represent the event that all the minimum security levels of keys whose seed is S_t in the i compromised nodes are no greater than both R_{ut} and R_{vt}. Then,

$$P_b = \sum_{i=1}^{x} P\left(A(i)\,|\,D_x\right) = \sum_{i=1}^{x} P\left(B\left(i, S_t\right) \cap C\left(R_{ut}, R_{vt}\right)\,|\,D_x\right) \tag{8}$$

Since the event $C(R_{ut}, R_{vt})$ is dependent of the event $B(i, S_t)$ and D_x, we have

$$P_b = \sum_{i=1}^{x} P\left(C\left(R_{ut}, R_{vt}\right)\right) \cdot P\left(B\left(i, S_t\right)\,|\,D_x\right) \tag{9}$$

As there are w key seeds in the key seed pool and each node picks m seeds from the key pool, we have

$$P\left(B(i, S)\,|\,D_x\right) = \binom{x}{i}\left(\frac{m}{w}\right)^{i}\left(1-\frac{m}{w}\right)^{x-i} \tag{10}$$

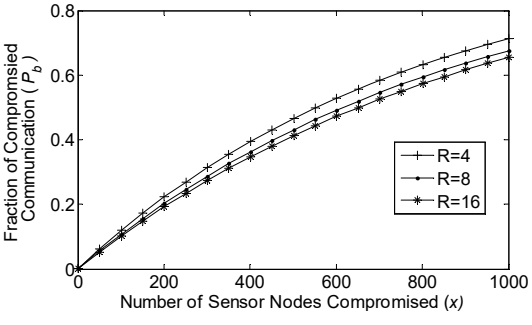
Assume R_{ct} is the minimum security level of the all of the pre-distributed keys whose seeds are S_t in one of the i compromised nodes. With two random number R_{ct} and R_{ut} (R_{vt}) and $0 \le R_{ct}, R_{ut}, R_{vt} < R$, the probability $R_{ct} > R_{ut}$ (R_{vt}) is $\sum_{i=0}^{R-1}\frac{1}{R}\sum_{j=i+1}^{R-1}\frac{1}{R} = \frac{R-1}{2R}$, then

$$P\left(C\left(R_{ut}, R_{vt}\right)\right) = 1 - \left(\frac{R-1}{2R}\right)^{2i} \tag{11}$$

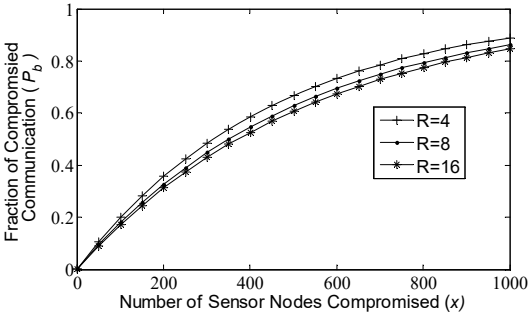
From formulas (9), (10) and (11) the probability of a data-communication link between two non-compromised sensors being compromised is:

$$P_b = \sum_{i=1}^{x} \binom{x}{i} \left(\frac{m}{w}\right)^{i} \left(1 - \frac{m}{w}\right)^{x-i} \left(1 - \left(\frac{R-1}{2R}\right)^{2i}\right) \tag{12}$$

Figure 3 Fraction of compromised link between non-compromised nodes with different connectivity, after an adversary has compromised x random nodes given, (a) plocal = 0.34 (b) plocal = 0.50



(a)



(b)

Figure 3 shows the relationship between the fraction of compromised links for non-compromised nodes and the number of compromised nodes. We can see that the larger of the system security level, the better resilience against node compromising attacks. But from formula (4), we know that the more computation needed in the sensor node with the larger of the system security level. From Figure 3, we can get that the resilience against node compromising attacks does not increases rapidly as the system

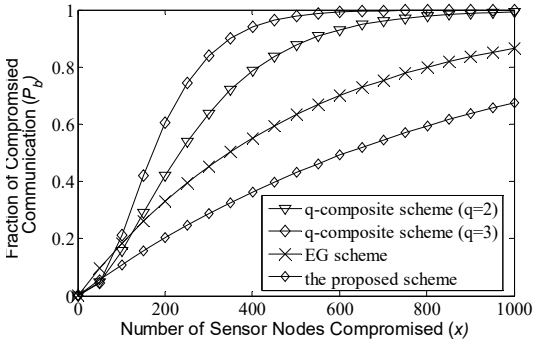
security level increases. Consider the computation and security, security level is not the larger the better. In the following analyses, the system security level we use is to set 4.

4.3.2 Comparison with previous schemes

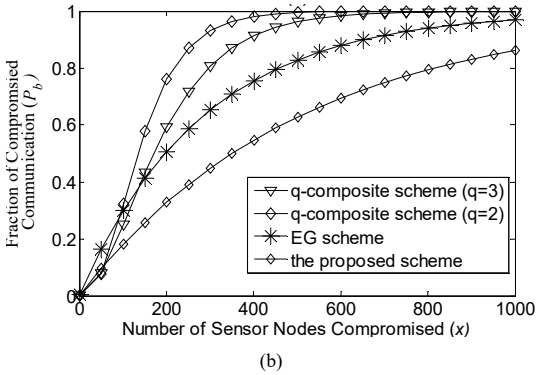
To evaluate our work, in this subsection we compare the security of our scheme with that of the related previous works. Here, we compare our scheme with EG scheme (Eschenaure and Gligor, 2002), *q*-composite scheme (for $q = 2, 3$) (Chan et al., 2003).

In the following analysis, we use the same amount of the storage per node for a fair comparison. In the all schemes, we assume that each sensor node is capable of holding 200 cryptographic keys in its memory. The local network connectivity probability is taken as 0.33 and 0.5 with suitable values of the parameters for the different schemes.

Figure 4 Fraction of compromised link between non-compromised nodes, after an adversary has compromised x random nodes, (a) local network connectivity is 0.33 (b) local networks connectivity is 0.5



(a)



(b)

Figure 4 compares the fraction of links compromised between non-compromised sensors given the same local connectivity P_L, and storage overhead. We can see that our scheme significantly better than the other two schemes. For example, in Figure 3(a), when there are 600 sensor nodes compromised, there will be 70.0% of links compromised between non-compromised sensors in EG scheme, 97.8% in q-composite (q = 2), 87.7% in q-composite (q = 3) , while there will only be 49.2% in our scheme.

5 Conclusions

In this paper, a new key predistribution approach based on the security level of pre-distributed keys in sensor nodes was proposed and numerically evaluated. In the proposed scheme, sensors nodes are first assigns some key seeds and random number as the security level of the pre-distributed keys. Our scheme is resilient against node compromise attack. The effectiveness of the proposed algorithms has been demonstrated through analysis and comparisons with the existing schemes.

References

Bag, S. and Roy, R. (2013) 'A new key predistribution scheme for general and grid-group deployment of wireless sensor networks', *EURASIP Journal on Wireless Communications and Networking*, Vol. 2013, No. 1, pp.1–19.

Blundo, C., de Santis, A., Herzberg A, et al. (1992) 'Perfectly-secure key distribution for dynamic conferences', *Proceedings of Annual International Cryptology Conference*, Springer Berlin Heidelberg, California, USA, pp.471–486.

Castelluccia, C. and Spognardi, A. (2007) 'Rok: a robust key pre-distribution protocol for multi-phase wireless sensor networks', *Proceedings of the 3rd International Conference on Security and Privacy in Communications Networks and the Workshops*, IEEE, Nice, FR, pp.351–360.

Chan, H., Perrig, A. and Song, D. (2003) 'Random key predistribution schemes for sensor networks', *Proceedings of 2003 IEEE Symposium on Security and Privacy*, IEEE, Oakland, California, USA, pp.197–213.

Dai, H. and Xu, H. (2010) 'Key predistribution approach in wireless sensor networks using LU matrix', *IEEE Sensors Journal*, Vol. 10, No. 8, pp.1399–1409.

Das, A.K. (2012) 'A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks', *International Journal of Information Security*, Vol. 11, No. 3, pp.189–211.

Delgosha, F. and Fekri, F. (2009) 'A multivariate key-establishment scheme for wireless sensor networks', *IEEE Transactions on Wireless Communications*, Vol. 8, No. 4, pp.1814–1824.

Du, W., Deng, J., Han, Y.S., Varshney, P., Katz, J. and Khalili, A. (2005) 'A pairwise key predistribution schemes for sensor networks', *ACM Transactions on Information and System Security*, Vol. 8, No. 2, pp.228–258.

Du, W., Deng, J., Han, Y.S. and Varshney, P. (2006) 'A key predistribution scheme for sensor networks using deployment knowledge', *IEEE Transactions Dependable Secure Compute*, Vol. 3, No. 1, pp.62–77.

Ergun, M., Levi, A. and Savas, E. (2011) 'Increasing resiliency in multi-phase wireless sensor networks: generation wise key predistribution approach', *The Computer Journal*, Vol. 54, No. 4, pp.602–616.

Eschenaure, L. and Gligor, V.D. (2002) 'A key-management scheme for distributed sensor networks', *Proceedings of the 9the ACM Conference on Computer and Communications*, ACM, Washington, DC, USA, pp.41–47.

Ge, M., Choo, K.K., Wu, H. and Yu, Y. (2016) 'Survey on key revocation mechanisms in wireless sensor networks', *Journal of Network and Computer Applications*, Vol. 63, No. 3, pp.24–38.

Lee, J.H. and Kwon, T. (2014) 'GENDEP: location-aware key management for general deployment of wireless sensor networks', *International Journal of Distributed Sensor Networks*, Vol. 10, No. 5, pp.1–17.

Liang, Q., Cheng, X. and Huang, S.C. (2014) 'Opportunistic sensing in wireless sensor networks: theory and application', *IEEE Transactions on Computers*, Vol. 63, No. 8, pp.2002–2010.

Liu, D., Ning, P. and Li, R. (2005) 'Establishing pairwise keys in distributed sensor networks', *ACM Transactions on Information and System Security*, Vol. 8, No. 1, pp.41–77.

Padmavathi, K. and Reddy, K.S. (2014) 'Wireless sensor networks application of wellness determination for elderly people', *International Journal of Research in Computer Engineering & Electronics*, Vol. 3, No. 4, pp.45–53.

Puccinelli, D. and Haenggi, M. (2005) 'Wireless sensor networks: applications and challenges of ubiquitous sensing', *IEEE Circuits and Systems Magazine*, Vol. 5, No. 3, pp.19–31.

Rasheed, A. and Mahapatra, R.N. (2011) 'Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, No. 1, pp.176–184.

Rawat, P., Singh, K.D. and Chaouchi, H. (2014) 'Wireless sensor networks: a survey on recent developments and potential synergies', *The Journal of Supercomputing*, Vol. 68, No. 1, pp.1–48.

Zhou, B., Li, S., Li, Q., Sun, X. and Wang, X. (2009) 'An efficient and scalable pairwise key pre-distribution scheme for sensor networks using deployment knowledge', *Computer Communications*, Vol. 32, No. 1, pp.124–133.

Zhou, B., Wang, J., Li, S. and Wang, W. (2014) 'A new key predistribution scheme for multiphase sensor networks using a new deployment model', *Journal of Sensors*, pp.1–10, Article ID 573913.