doi:10.3772/j.issn.1006-6748.2018.04.002

Study on key management scheme for heterogeneous wireless sensor networks①

Qin Danyang (秦丹阳)②, Ma Jingya, Zhang Yan, Yang Songxiang, Ji Ping, Feng Pan
(Key Lab of Electronic and Communication Engineering, Heilongjiang University, Harbin 150080, P. R. China)

Abstract

Heterogeneous wireless sensor network (HWSN) is composed of different functional nodes and is widely applied. With the deployment in hostile environment, the secure problem of HWSN is of great importance; moreover, it becomes complex due to the mutual characteristics of sensor nodes in HWSN. In order to enhance the network security, an asymmetric key pre-distributed management scheme for HWSN is proposed combining with authentication process to further ensure the network security; meanwhile, an effective authentication method for newly added nodes is presented. Simulation result indicates that the proposed scheme can improve the network security while reducing the storage space requirement efficiently.

Key words: heterogeneous wireless sensor network (HWSN), key management, authentication, network security, storage space

0 Introduction

Nowadays, wireless sensor networks (WSNs) have attracted many scholars' attention because of their rapid development and wide application, which makes it a research hotspot at home and abroad[1]. WSN is an open network being deployed in hostile environment and prone to various attacks[2]. The importance of WSN's security is self-evident, hence, it is critical to achieve a secure key management scheme for WSN, which is studied by scholars in different countries[3]. In 2002, Eeschnauere and Gligor[4] first addressed a classical key management scheme termed E-G scheme[4] with a property of easy achievement rather than perfect security. An E-G based q-composite scheme proposed by Chan et al.[5] requires that two nodes should have at least q shared-keys to improve the security. The invulnerability of q-composite scheme is better compared to that of E-G scheme under conditions with fewer compromised nodes, but with the number of the compromised nodes increasing, the security of q-composite would become worse. A key predistribution scheme based on polynomial was proposed by Zhang et al.[6], which would improve the ability against compromise attacks of WSN. However, the performance of the scheme will become worse when the number of compromised nodes increases sharply. Heterogeneous wireless sensor network (HWSN) assumes a mutual heterosexual structure and function of nodes, which can prolong network life, improve network connectivity, testability and survivability. While in practical applications, the comprehensive characteristics are unsatisfactory because the aforementioned traditional key management schemes do not take the mutual characteristics of sensor nodes into account[7]. Therefore, how to take advantage of the mutual characteristics of HWSN to design an efficient key management scheme has arisen to our attention. Meanwhile, many existing key management schemes do not consider the security of newly added nodes[8]. To solve the above problems, an effective asymmetric key pre-distributed management scheme (APS) combining with Schnorr authentication[9] is proposed, and an authentication method for newly added node is presented. The proposed scheme will improve the whole network security and reduce the storage burden of sensor nodes.

1 Key management scheme for HWSN

1.1 Clustering model for HWSN

The formation mechanism of clusters for HWSN

① Support by the National High Technology Research and Development Program of China (No. 2012AA120802), National Natural Science Foundation of China (No. 61771186), Postdoctoral Research Project of Heilongjiang Province (No. LBH-Q15121), University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province (No. UNPYSCT-2017125) and Postgraduate Innovation Research Project of Heilongjiang University (No. YJSCX2018-051HLJU).

② To whom correspondence should be addressed. E-mail: qindanyang@hlju.edu.cn

Received on Dec. 18, 2017

will be described in this section. In this paper, large scale HWSN is adopted as the background, which is equipped with a base station (BS) as an advanced cluster fusion center for processing data. The nodes in the network are classified as cluster heads (CHs) and ordinary nodes, where CHs with tamper-resistant hardware (TRH) possess high energy. Suppose that CHs and ordinary nodes are deployed randomly and uniformly in interested area. During the initialization process, for cluster head selection, each CH will broadcast an H_{msg} to its neighbor nodes in a random interval to avoid collision between two neighbor CHs, where H_{msg} is a hello message including CH's location and ID information. For a wide transmission range with sufficient CHs, most ordinary nodes can receive H_{msg} messages from at least one CH, and the CH with the optimal signal intensity will be selected as their active cluster head. Meanwhile each ordinary node will also record the H_{msg} from other CHs. Once the cluster-head selection fails, these CHs will act as the backups. The network construction is shown in Fig. 1.

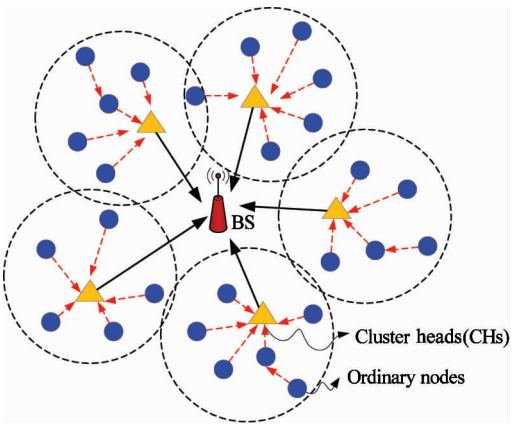

Fig. 1 Cluster model for HWSN

1.2 Generation of network certificate

After the formation of the cluster, there will be an ID signature process carried out by the CH for the nodes in its cluster. The CH will reserve the IDs and signatures of each ordinary node, while each ordinary node will acquire and store the certificates issued by the CH. Arbitrary ordinary node A, for instance, will select a random number x and calculate a y by $y = g^{-x} \bmod p$, then node A will send value y to its CH. Signature s will be carried out according to y and ID_A by $s = sig_A(ID_A, y)$. The certificate of node $A(C_A)$ consists of its ID, y and s, i. e. $C_A = (ID_A, y, s)$. The symbolic meanings are shown in Table. 1.

1.3 Proposed scheme

An asymmetrical key pre-distributed management scheme (APS) for HWSN based on Schnorr authentication will be presented in this section. With the consideration that CHs have more storage space than ordinary nodes and CHs are equipped with TRH, more keys are assigned to the CHs than those assigned to ordinary nodes, and the key of different lengths can be generated by the RSA algorithm[10]. Schnorr authentication is adopted in order to avoid the leakage of shared-key. The whole process of APS can be summarized as four stages: key pre-assignment stage, authentication stage, shared-key discovering stage and pairwise key setup stage.

1) Key pre-assignment stage

The key pre-assignment stage can be summarized as follows.

Step 1 A large key pool P will be generated by the key processing center (KPC), in which each key will correspond to a unique ID.

Step 2 l keys are chosen from P to be pre-assigned to ordinary nodes.

Step 3 M keys are chosen from P to be pre-assigned in CHs ($M >> l$) and each CH is pre-assigned with K_H that can only be acquired by the base station (BS).

2) Authentication stage

Ordinary nodes in the cluster should be authenticated just before the shared-key discovering stage to enhance the network security as shown in Fig. 2, and the symbolic meanings of this part are shown in Table 1.

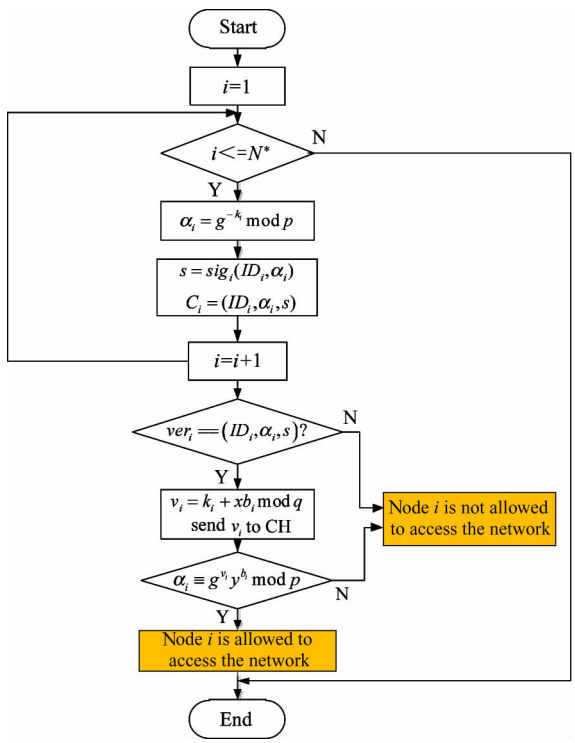

Fig. 2 Flow chart of authentication process

Taking arbitrary node i in the network as an example, the process of the authentication is as follows.

Step 1 Node i in the network will select a random k_i firstly to calculate $\alpha_i = g^{-k_i} \bmod p$.

Step 2 Node i will send its certificate C_i and α_i to the corresponding CH.

Step 3 CH will authenticate the certificate sent by node i, that is $ver_i = (ID_i, \alpha_i, s)$; once the validation fails, skip to Step 7; otherwise, skip to the Step 4.

Step 4 CH will select a random b_i and send it to node i.

Step 5 Node i will calculate v_i by $v_i = k_i + xb_i \pmod q$ after receiving b_i and send the value v_i to the corresponding CH.

Step 6 According to the received α_i and v_i, CH will verify $\alpha_i \equiv g^{v_i} y^{b_i} \bmod p$. If passing the validation, node i is a legitimate node and is allowed to enter the shared-key discovering stage; otherwise, skip to Step 7.

Step 7 CH terminates the communication with node i.

3) Shared-key discovering stage

In this stage, each ordinary node (say u) will send the unencrypted key list information to its CH. A key information is composed of node u's ID and location information; thus, the shared-key between two neighbor nodes will be discovered by CH after receiving the key list information. Whether two ordinary nodes (say u and v) are neighbors can be determined by the CH with the location information, i. e. node u and v will be defined as neighbor nodes by CH when the distance between these two nodes is within the transmission range.

4) Pair-wise key setup stage

Although with the shared-key discovering stage, partial ordinary nodes may not set up a shared-key with their neighbors. For this kind of nodes (node u and v are the neighbor nodes that don't share any keys in common), CH will acquire the shared-key between node u and v respectively, noted as K_u and K_v. Then, the pair-wise key $K_{u,v}$ between node u and v will be generated and be sent to node u, v respectively. The specific process is as follows.

Firstly, CH will check if node u or v has a shared-key with it. Recalling that a large number of keys are pre-assigned in CH, the probability of node u or v having at the least one shared-key with their CHs is high. When there is no common key shared between CH and node u or v, the following method is used to build the pair-wise key for node u and v.

Taking node u as an example, if there is no shared-key between CH and node u, CH will check if there is a 1-hop neighbor node z possessing a shared-key $K_{u,z}$ with node u. If CH find the shared-key between node u and z, it will ask node z to send $K_{u,z}$ to it, that is, $z \rightarrow \mathrm{CH}: \{K_{u,z}\}K_z$.

Assume that there is no shared-key between node u and $1-d$-hop neighbor nodes, where d is a system parameter. A request message containing node u's ID will be sent to BS by CH; then, BS sends a corresponding key encrypted by K_H to CH. After acquiring the key from BS, for each pair of neighbor nodes u and v, a pair-wise key $K_{u,v}$ will be generated and unicasted to u and v, noted as $\mathrm{CH} \rightarrow u: \{K_{u,v}\}K_u$, $\mathrm{CH} \rightarrow v: \{K_{u,v}\}K_v$, so that node u and v will acquire the shared-key $K_{u,v}$ and can communicate securely.

Table1 Notations and definitions

Notations	Definitions	Notations	Definitions
x	random number, $0 \leqslant x \leqslant q-1$	q, p	large prime number, where, $q \geqslant 2^{140}$, $p \geqslant 2^{512}$
k_i	random number, $0 \leqslant k_i \leqslant q-1$	N^*	number of nodes in the network except CHs
b_i	random number, $0 \leqslant b_i \leqslant 2^t$	s	signature of nodes
g	q-order element, $g \in Z_n^*$, $g^q \equiv 1 \pmod p$	t	secure parameter, $t \geqslant 40$

2 Security issues in HWSN

2.1 Broadcast key establishment

Via key broadcasting, the message can be delivered securely to their neighbor nodes by ordinary nodes[11]. It is easy to establish a broadcast key for each pair of neighbor nodes after the shared-key or pair-wise key is set up[12]. The broadcast key K_{uB} can be generated after being encrypted by corresponding shared-keys and the data packet $\{K_{uB}\}K_{u,v}$ will be generated and sent to node u by node v.

2.2 Key revocation

Once any ordinary node is damaged or compromised, the key message in the node should be revoked[13]. Suppose that the compromised nodes have been detected and reported to the corresponding CH, which will disseminate the 'revocation message' containing the IDs list of the revoked nodes. There is a shared-key between CH and ordinary nodes including

$1-d$ hop neighbors. The unique message authentication code (MAC) can be calculated by CH in accordance with each shared-key. Through corresponding MAC obtained from 'revocation message', the ordinary nodes can check whether the received message is integrated or not[14].

2.3 Newly added nodes

With the consideration of the security issues of newly added nodes[15], an efficient scheme is proposed to validate the newly added nodes in this section. For arbitrary newly added node e, l keys and a special key $K_{L,e}$ are pre-assigned, where $K_{L,e} = h(K_H \oplus e)$, $h(\cdot)$ represents one-way Hash function, K_H is a special key pre-stored in CH, $K_H \oplus e$ represents the XOR (exclusive or) of K_H and node e. Being deployed in a relevant area, node e will send a *Join message* to its CH, that is, $e \parallel location \parallel MAC(K_{L,e} \parallel location)$. As CH receives the *Join message*, corresponding key $K'_{L,e}$ will be generated according to node e and K_H. Comparing $K'_{L,e}$ with the $K_{L,e}$ in *Join message* sent by node e, the legitimacy of node e can be verified. If node e is a legitimate node, CH will find the neighbor node for e and generate a shared-key. The process of the newly added nodes access to the network is shown in Fig. 3.

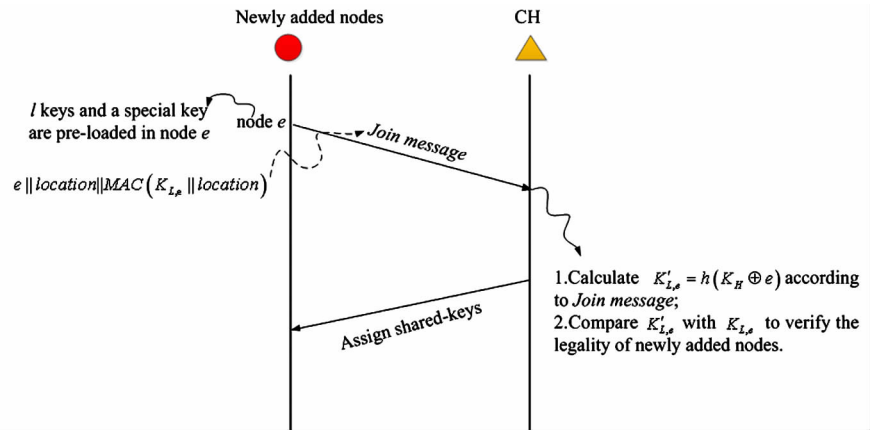

Fig. 3 Process of newly added nodes access to the network

3 Performance analysis and evaluation

3.1 Key pool size

Key pool size P is an important parameter for APS scheme. Assuming that the number of pre-assigned keys is fixed, when there are a certain number of ordinary nodes in the network being damaged, the effect on the communication ability of other nodes will decrease with the increasing P.

To obtain the maximum value of P, it should be satisfied that the probability of the ordinary nodes sharing at least q keys with the CHs is above threshold p[4]. $p(i)$ represents the probability of any ordinary node sharing i keys with its CH. For l and M keys pre-assigned for the ordinary nodes and the CHs respectively, there will be $C_P^l \cdot C_P^M$ combination methods for ordinary nodes and CHs to select l and M keys from P. If i common keys are existing between the ordinary nodes and the CHs, there will be C_P^i ways to select the common keys; and there will be C_{P-i}^{M+l-2i} ways to select the other $M+l-2i$ keys from the rest $P-i$ keys. Accordingly, there will be C_{M+l-2i}^{l-i} ways to assign the different $(M+l-2i)$ keys. Hence, $p(i)$ will be:

$$p(i) = \frac{C_P^i \cdot C_{P-i}^{M+l-2i} \cdot C_{M+l-2i}^{l-i}}{C_P^l \cdot C_P^M} \tag{1}$$

The probability p_c of any two nodes sharing at least q common keys can be represented as

$$p_c = 1 - (p(0) + p(1) + p(2) + \cdots + p(q-1)) \tag{2}$$

The maximum $P_{\max}$ will be obtained by the relationship of $p_c \geqslant p$ in Eq. (2).

3.2 Analysis on storage space

Compared with the key management schemes in homogeneous WSN, the storage demand can be remarkably reduced by the proposed APS scheme. The probability p_A of the ordinary node sharing at least 1 common key with its CH, namely shared key probability (SKP) for short, in APS will be:

$$\begin{aligned} p_A &= 1 - p(0) = 1 - \frac{C_P^{M+l} \cdot C_{M+l}^l}{C_P^l \cdot C_P^M} \\ &= 1 - \frac{(P-l)!(P-M)!}{P!(P-M-l)!} \end{aligned} \tag{3}$$

The shared key probability p_E for the E-G scheme is given as:

$$p_E = 1 - \frac{C_P^m \cdot C_{P-m}^m}{C_P^m \cdot C_P^m} = 1 - \frac{[(P-m)!]^2}{P!(P-2m)!} \quad (4)$$

Simulations on p_A and p_E are performed with different values of P, M and l, where P changes from 1 000 to 10 000 with an increment of 500. The results are shown in Fig. 4 and from top to bottom, the values of M, l, m are [125, 5, 25], [250, 10, 50], [375, 15, 75] and [500, 20, 100] respectively. M, l and m will satisfy $M \times l = m^2$. It can be observed that the larger the pre-assigned keys in the node is, the higher the shared key probability will be. With the same M, l, m values, the shared key probability will decrease with P increasing. Moreover, it can also be seen that the two curves approach to each other with the same M, l, m values.

For further comparison, it is assumed that 1 000 ordinary nodes and 10 CHs are in simulating HWSN scene, and each ordinary node and CH are pre-assigned with 15 and 375 keys respectively. To imitate the same condition with that of HWSN, 1 000 nodes pre-assigned with 75 keys are set in a homogeneous wireless sensor network, that is, $M = 375$, $l = 15$, $m = 75$. For HWSN, the total memory required to store the keys is $1\,000 \times 15 + 10 \times 375 = 18\,750$ (per unit key length); for homogeneous wireless sensor network, however, is $1\,000 \times 75 = 75\,000$ (per unit key length). The storage space of the E-G scheme is nearly 4 times as large as that of APS scheme. It reveals by the comparison that APS can save more storage space.

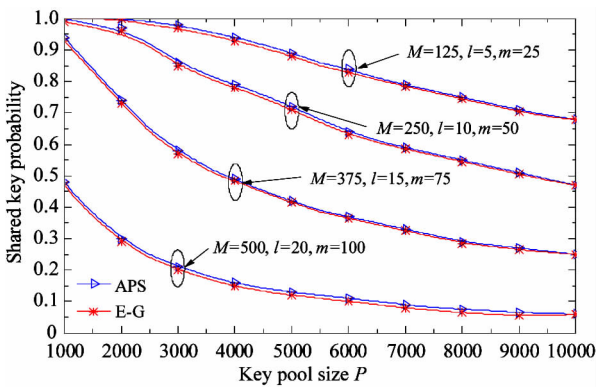

Fig. 4 Shared key probability with different P

The shared key probability curves with different pre-assigned keys are shown in Fig. 5, in which the vertical ordinate is the shared key probability, and the horizontal ordinate represents the number of pre-assigned keys m. In simulation, m varies from 25 to 200 with an increment of 25, and $l = m/5$, $M = 5m$ to satisfy $M \times l = m^2$; the key pool size P is 10 000, 5 000, 2 000 and 1 000 from the bottom to top. Simulating results in Fig. 5 indicate the same significance as Fig. 4, that is, the shared key probability will increase as pre-assigned keys become larger. Once the value of pre-assigned keys is fixed, the shared key probability will decrease with P increasing.

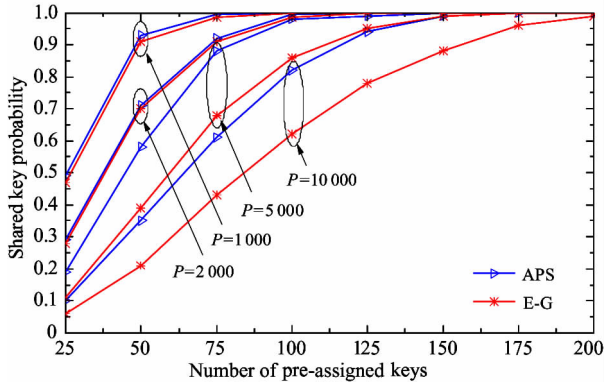

Fig. 5 Shared key probability with different m

From the analysis above, it can be observed that the proposed scheme will reduce the storage demand of sensor nodes remarkably compared to that of homogeneous wireless sensor network in achieving the same shared key probability.

3.3 The probability of being k-hop neighbors

The ordinary nodes will become the k-hop neighbors with the CHs according to shared-key establishing way. In this part, the probability for being 1-hop and 2-hop neighbor nodes (PBN1 and PBN2) will be analyzed. Recall that there are l and M keys pre-stored in some ordinary node u and CH respectively. To be the 1-hop neighbors means that node u and CH must have at least one key in common. According to Eq. (3), the probability of node u being 1-hop neighbor of CH can be deduced as

$$p_1 = \frac{(P-l)!(P-M)!}{P!(P-M-l)!} \quad (5)$$

To be the 2-hop neighbors means there is at least one shared-key between ordinary node v and any 1-hop neighbor node. If there are N ordinary nodes in the cluster and n_1 represents the number of 1-hop nodes in the cluster, there will be:

$$n_1 = \lfloor p_1 \times N \rfloor \quad (6)$$

Let event B indicate that there is at least one shared-key between node v and the 1-hop neighbor node, event C mean that there is no shared-key between node v and the 1-hop neighbor node, and event D represent that node v is not the 1-hop neighbor node. Thus, the shared-key probability between nodeand 1-hop neighbor node can be expressed as

$$p_{12} \equiv \mathrm{pr}(\mathrm{B}) = 1 - \mathrm{Pr}(\mathrm{C}) = 1 - [(C_P^l \cdot C_{P-l}^l)/(C_P^l)^2]^{n_1}$$

$$= 1 - [(C_P^l \cdot C_{P-l}^l)/(C_P^l)^2]^{\lfloor p_1 \times N \rfloor} \quad (7)$$

The probability of node v as a 2-hop neighbor node can be deduced as

$$p_2 = \frac{(p-l)!(P-M)!}{P!(P-M-l)!} \times \{1 - [(C_P^l \cdot C_{P-l}^l)/(C_P^l)^2]^{\lfloor p_1 \times N \rfloor}\} \quad (8)$$

In Fig. 6, the p_1 and p_2 curves are plotted with different values of P and M. The value of M in Fig. 6(a) and Fig. 6(b) are 200 and 500 respectively, $l = 20$, $N = 100$, and the value of P varies from 1 000 to 10 000 with an increment of 1 000. From Fig. 6, it can be concluded that the probability of being 1-hop or 2-hop neighbors will increase with the growing of M.

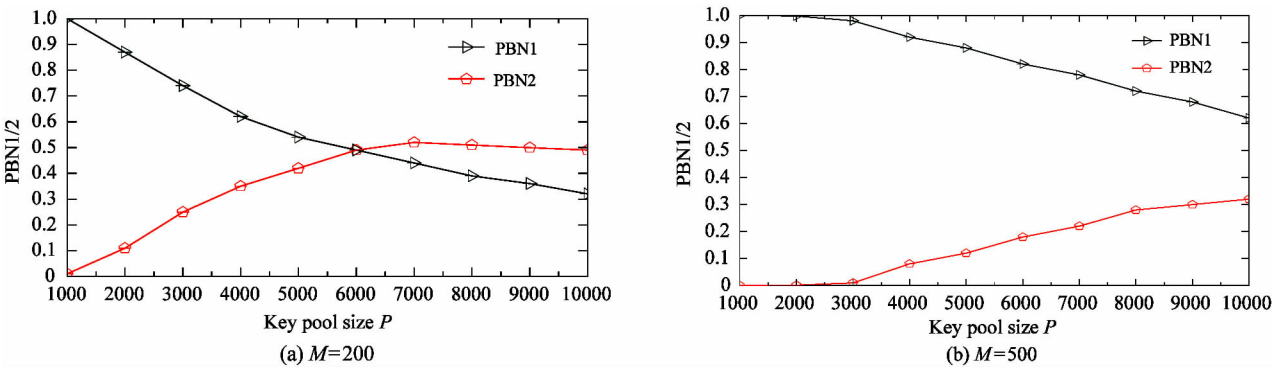

Fig. 6 Probability of being 1-hop or 2-hop neighbor nodes

3.4 Analysis on security performance

The ability against compromised attacks is an important security evaluation index of WSN. In this section, the ability against compromised attacks of the proposed APS scheme will be analyzed compared with the classical E-G scheme[4], q-composite scheme[5] and KP scheme[6].

Assume that CHs with TRH are relatively secure; hence, in this section, the security of ordinary nodes will be concerned. It is known that l keys are pre-assigned to each ordinary node. Thus, the probability of the known key K in the key ring is l/P. It is provided that there are r compromised nodes in the network, the probability of K being not in the compromised nodes' key ring will be $(1 - l/P)^r$. The probability of the secure link being exposed, represented as p_r, can be derived under the conditions of r compromised nodes in the network, as in Eq. (9).

$$p_r = 1 - \left(1 - \frac{l}{P}\right)^r \quad (9)$$

Eq. (9) shows that p_r will decrease with the decreasing of l when P and r are fixed. This is an essential reason for pre-storing a small number of keys in ordinary nodes.

If no less than q keys are required to build a secure link, then the probability of the newly established link being destroyed is even low when there are r compromised nodes. If there are i shared-keys between CH and ordinary nodes, the probability of the link being destroyed is $(1 - (1 - l/P)^r)^i$. Thus, it can be concluded that the probability of any secure link built between two ordinary nodes is compromised when r nodes have been captured (hereinafter is expressed as compromising probability) and can be deduced as

$$R(l) = \sum_{i=q}^{l} \left(1 - \left(\frac{l}{P}\right)^r\right)^i \frac{p(i)}{p_{link}} \quad (10)$$

$$p_{link} = p(q) + p(q+1) + \cdots + p(l) \quad (11)$$

where, l is the number of keys pre-assigned to ordinary nodes, $p(i)$ is shown in Eq. (1), and p_{link} is the probability of establishing a secure link for HWSN as shown in Eq. (11).

The probability of a secure link between two nodes being destroyed in q-composite scheme is

$$R(m) = \sum_{i=q}^{m} \left(\left(1 - \left(1 - \frac{m}{P}\right)^r\right)^i \times \frac{p'(i)}{p_{link}}\right) \quad (12)$$

where $p'(i)$ is the probability of having i keys in common between two nodes to satisfy:

$$p'(i) = (C_P^i \times C_{P-i}^{2(m-i)} \times C_{2(m-i)}^{m-i})/(C_P^m)^2 \quad (13)$$

From Eq. (10) and (12), it can be seen that $R(l)$ and $R(m)$ will increase with the increasing of l and m. Since m is much greater than l, there will be $R(m) >> R(l)$. It can be observed that the proposed scheme APS is more flexible to resist the compromised attack than the classical q-composite scheme.

In Fig. 7, the compromising probability with $q = 1$ is plotted. The key pool size P is 1 000; the number of compromised nodes r changes from 1 to 200 with an interval of 10; three different values are selected for E-G scheme, that is, $m = 20$, 30 and 50 respectively; and let $M = 100$, $l = 10$ for APS. It reveals that $M \times l \approx m^2$ when $m = 30$, so that the APS scheme has the same key sharing probability with E-G scheme. From Fig. 7,

it can also be observed that for any r, APS will have a lower compromising probability than KP and E-G scheme.

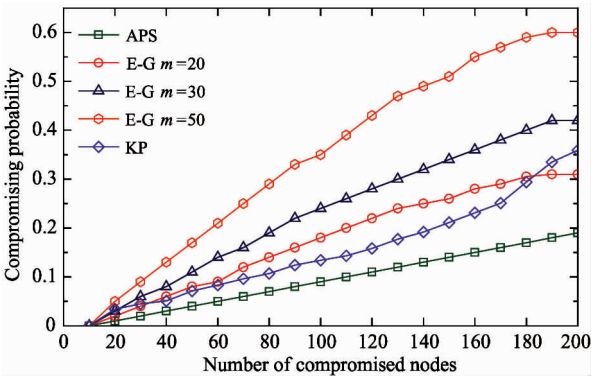

Fig. 7 Compromising probability with $q = 1$

The compromising probability with $q = 3$ is presented in Fig. 8. The other parameters are the same as Fig. 7. Compared with Fig. 8 and Fig. 7, a similar performance changing tendency can be obtained. Moreover, the largest compromising probability of APS curve in Fig. 7 is 0.2, while it is 0.01 in Fig. 8. Thus, it can be concluded that the larger q becomes, the lower the compromising probability will be.

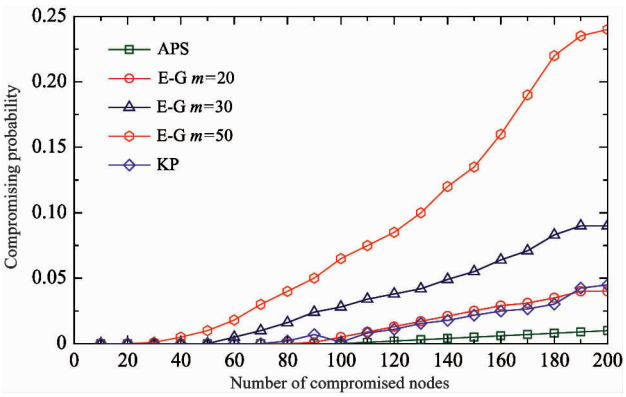

Fig. 8 Compromising probability with $q = 3$

As shown in Fig. 7 and Fig. 8, the ability against compromised attacks of the classical E-G scheme is more stable than the KP scheme when the number of compromised nodes varies greatly. At the same time, the KP scheme is more appropriate when the number of variation of compromised nodes is small. However, the above two schemes are all affected by the changing number of compromised nodes. The APS scheme proposed in this paper will fluctuate less with the changing number of compromised nodes. Above all, it indicates that the proposed APS can remarkably improve the resistance ability to compromised attack compared with E-G scheme and KP scheme.

4 Conclusion

In recent years, WSN has been widely applied with most attentions lying in prolonging the lifetime of the network and improving the reliability of data transmission. However, the mutual features of sensor nodes of HWSN make the network security become more complex than ever before. In order to enhance the network security and reduce the storage space requirements, an APS scheme is proposed for HWSN in this paper. Schnorr authentication is introduced to reduce the probability of illegal nodes accessing the network. In APS, keys are pre-assigned to the CHs and the ordinary nodes respectively. A new asymmetric key managing algorithm is presented, including key pre-assignment, identification authentication, shared-key discovery and pair-wise key setup. The performance of the proposed scheme is analyzed in terms of key pool size, the probability of being k-hop neighbor and the storage space requirement. Simulating results show that the whole network security can be improved with the decreasing of pre-assigned keys in ordinary nodes. Furthermore, the newly added nodes will pose a major challenge to the security of WSN. Security keys should be set up between newly added nodes and existing nodes, while the existing nodes may have been destroyed or may be malicious nodes. Thus, the importance of newly added nodes' security is self-evident. Hence, an effective authentication method for newly added nodes is introduced in this paper. Compared with the traditional key management schemes, the APS proposed in this paper can enhance the network security and reduce the storage burden of sensors significantly.

References

[1] Chen X, Makki K, Kang Y, et al. Sensor network security: a survey[J]. *Communications Surveys & Tutorials, IEEE*, 2009, 11(2): 52-73

[2] Lu K, Qian Y, Hu J. A framework for distributed key management schemes in heterogeneous wireless sensor networks[C]. In: Proceedings of the IEEE International Performance Computing and Communications Conference, Phoenix, USA, 2006. 513-519

[3] Das A K. A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks[J]. *International Journal of Information Security*, 2012, 11(3): 189-211

[4] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks[C]. In: Proceedings of the 9th ACM Conference on Computer and Communication Security, Washington, USA, 2002. 41-47

[5] Chan H, Perrig A, Song D. Random key pre-distribution schemes for sensor networks[C]. In: Proceedings of the

2003 IEEE Symposium on Security and Privacy, Washington, USA, 2003. 197-213

[6] Zhang J, Li H, Li J. Key establishment scheme for wireless sensor networks based on polynomial and random key pre-distribution scheme[J]. *Science Direct*, 2018, 71: 68-77

[7] Qin D Y, Jia S, Yang S X, et al. Research on stateful public key based secure data aggregation model for wireless sensor networks[J]. *High Technology Letters*, 2017, 23(1):38-7

[8] Metan J, Narasimha Murthy K N. Robust and secure key management in WSN using arbitrary key deployment[C]. In: Proceedings of the International Conference on Emerging Research in Electronics, Computer Science and Technology, Mandya, India, 2015. 246-250

[9] Yang C J, Zhou J M, Zhang W S. Pairwise key establishment for large-scale sensor networks: from identifier-based to location-based[C]. In: Proceedings of the 1st International Conference on Scalable Information Systems, Hong Kong, China, 2006. 55-64

[10] Thangavel M, Varalakshmi P, Murrali M, et al. An enhanced and secured RSA key generation scheme (ESRKGS)[J]. *Journal of Information Security & Applications*, 2015, 20(C): 3-10

[11] Ma C G, Shang Z G, Wang H Q. An improved key management scheme for heterogeneity wireless sensor networks [C]. In Proceedings of the 3rd International Conference on Mobile Ad-hoc and Sensor Networks, Beijing, China, 2007. 12-14

[12] Reegan A S, Baburaj E. Key management schemes in wireless sensor networks: A survey[C]. In: Proceedings of the 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, India, 2013. 813-820

[13] Kuchipudi R, Qyser A. A dynamic key distribution in wireless sensor networks with reduced communication overhead[C]. In: Proceedings of the International Conference on Electrical, Electronic and Optimization Techniques, Chennai, India, 2016. 3651-3654

[14] Roman R, Alcaraz C, Lopez J. Key management systems for sensor networks in the context of the internet of things [J]. *Computers & Electrical Engineering*. 2011, 37(2): 147-159

[15] Rams T, Pacyna P. A survey of group key distribution schemes with self-healing property[J]. *IEEE Communications Surveys & Tutorials*, 2013, 15(2): 820-842

Qin Danyang, born in 1983. She received her B. Sc. degree in communication engineering from Harbin Institute of Technology in 2006, and both M. Sc and Ph. D. degrees in information and communication system from Harbin Institute of Technology in 2008 and 2011 respectively. Currently, she is an associated professor at the Department of Communication Engineering of Heilongjiang University, Harbin, P. R. China. Her researches include wireless sensor network, wireless multihop routing and ubiquitous sensing.