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 11 (1): 102-109, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.102.109

An Enhanced Scheme against Node Capture Attack usimg Hash-Chain for Wireless Sensor Networks

[1]Tao Qin and [2]Hanli Chen
[1]Department of Modern Science and Technology, The Committee Party School of Hunan, Changsha 410006, China
[2]School of Civil Engineering, Central South University, Hunan, Changsha 410075, China

Abstract: Node capture is a severe threat to data security in Wireless Sensor Networks(WSNs). This paper aimed to design an enhanced and efficient scheme against node capture attack using hash-chain in wireless sensor networks. Key management is the fundamental security mechanism in wireless sensor networks, but existing schemes based on probability have poor resistance to node capture attack. In order to improve the resilience against node capture attack, a hash-chain based scheme to resist node capture attack was presented. The main idea of the proposed consisted of applying a hash function on the initial preloaded keys before deployment. During the key pre-distribution, the selected keys were hashed according to certain rules and the hashed results were as communication key. Theoretical analysis and simulation results show that, key exposal probability and average insecure degree decrease by 56 and 46% compared to existing algorithms, respectively. Through hash chain technique that conceals the same keys used to secure different links, the proposal outperforms other schemes in resilience against node capture attack and enhance the overall survivability of the network.

Key words: Wireless sensor network, hash-chain, node capture attack, key exposal probability, average insecure degree, key management, data security

INTRODUCTION

Recent advancement in wireless communications and electronics has enabled the development of sensor networks (Akyildiz *et al*., 2002). A large number of sensor nodes deployed in the sensing area collaborate to monitor, perception, acquisition and process the real-time monitoring information of environment (Perrig *et al*., 2004). Wireless sensor network, which can achieve detection, diagnosis, targeting and tracking capabilities, has very broad application prospects and mainly be used in industrial control, military surveillance, environmental science, health care, space exploration, intelligent buildings and other complex environments (Di Pietro *et al*., 2009; Chen *et al*., 2011; Idris *et al*., 2009).

The security problems must first be solved for large-scale application of wireless sensor networks. If one node is captured, the additional sensitive information will be obtained by attacker. The nodes are generally deployed in unattended or hostile areas where eavesdropping, spoofing and other security risks exist (Capkun and Hubaux, 2005; Bla and Zitterbart, 2006; Albath and Madria, 2007) which further increase the difficulty of security management. Node capture is a more serious attack, the attacker can take the captured nodes as a basis for further implementation of a variety of other attacks. Key management is the foundation of WSN security, to a certain extent which can resist the impact of node capture attack but the existing key management algorithms based on probability have poor performance against node capture attack. With the increase of captured nodes, the probability of disclosure of the key communications increases rapidly which leads to exposure of sensitive information (Laurent and Gligor, 2002; Chan *et al*., 2003).

While the effective key management algorithm can mitigate the adverse impact of node capture attack, but designing a key management algorithm for WSN is also facing many challenges. First, due to the speciality of electromagnetic environment, the collected and transmitted data may suffer from different types of malicious, such as eavesdropping, tampering and replay (Conti *et al*., 2008). Second, as resource limitations of node such as energy and storage space, the attacker can take the captured node as a base to obtain the secret material. Thus the traditional pairwise key establishment

Corresponding Author: Tao Qin, Department of Modern Science and Technology, The Committee Party School of Hunan, Changsha 410006, China

algorithm, such as traditional public key encryption system (public key cryptography, PKC) (De Soete, 1993) and the use of key distribution center (Key Distribution Center, KDC) (D'Arco, 2001) approach are not suitable to WSN. The current key management algorithm is the key pre-distribution, before the node is deployed, the server will be able to generate the secret key pre-configured in the node. After node deployment, the nodes calculate the communication key according to a certain rules or algorithms which is very suitable for WSN.

At present, many research programs have focused on probabilistic key pre-distribution scheme (Laurent and Gligor, 2002; Chan *et al*., 2003; Ren *et al*., 2011; Wei *et al*., 2007). The first key pre-distribution scheme which is based on probability and random graph theory, is proposed by Laurent and Gligo (2002). Before deployment, each node is preloaded into some keys which are selected randomly from a large key pool. After deployment, if two nodes in the communication range share a common key, they can use the shared key to encrypt the collected data. With less storage overhead, E-G scheme achieves higher key connectivity and meets the requirements of storage, distribution and other aspects in WSN. However, E-G scheme is weak in resilience against node capture attack and can not provide authentication among the communicating nodes. If the number of captured nodes increase, the attacker may get and obtain more sensitive information. On the basis of E-G scheme (Chan *et al*., 2003) developed the q-composite key establishment scheme. The difference between q-composite 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 (Su *et al*., 2007). If the number of shared keys are greater than q, the nodes use one-way hash function to compute a communicating key $k = hash (k_1 \| k_2 \| ... \| k_t)$ (Chan *et al*., 2003). Q-composite scheme improves the resilience of the network and the survivability is better than the E-G scheme. But with the increase in the number of captured nodes, the scheme has become poor. The two schemes have a common defect that is they are weak in resisting the node capture attack (Su *et al*., 2007).

In order to improve the resilience against node capture attack this study is the first to integrate probability based key management with hash-chain to develop an effective scheme to resist node capture attack. In our proposal, the main principle is to use one-way hash function to further reduce the impact of node capture attack by applying different time of hash to different nodes. If an attacker captures the key ring of one node it cannot discover keys having the same identifiers and used in a node such as , where is a system parameter. The paper studies key exposal probability and average insecure degree. Analysis and simulation results show that, compared to existing algorithms, the key exposal probability and average insecure degree decrease by 56 and 46%, respectively. The resilience against node capture attack is strengthened and the survivability of entire network is enhanced.

The mainly three contributions of this paper can be summed up as follows:

- Integrating key management with Hash-Chain to develop an effective scheme to resist node capture attack
- The proposed scheme whose parameter is adjustable can remarkably enhance network resilience against node capture attack

In this study, an enhanced scheme based on hash-chain was proposed to reduce the impact of node capture attack and guarantee the security of entire network.

E-G SCHEME AND HASH FUNCTION

E-G scheme: E-G scheme includes the following three steps:

Step 1: Key pre-distribution phase. Before node deployment, the key server first generates a key pool with size P and key identifiers, each node randomly selects and stores m different keys (called key ring) from the key pool which can ensure that any two nodes have common key with a certain probability.

Step 2: Shared key discovery phase. After node deployment, neighboring nodes (within communication range of one node) see if there is the shared key by exchanging the key identifier, if two nodes have the same key identifier, they select one as the pairwise key, otherwise go to step three.

Step 3: The key path establishment phase. If two nodes can not directly establish communication key, they can use intermediate nodes as a "bridge node" that shares pairwise keys with both of them to help establish an indirect key. Specifically, supposing that there are intermediate nodes n_1, n_2,..., n_l between the source node and n_s destination node n_d and each pair of neighboring nodes in the path has direct pairwise key. Source node n_s broadcasts the identifier of the key it stores, which is forwarded through the intermediate nodes securely until it discovers a "bridge node" that shares a pairwise key

with the two sensor nodes respectively. The source node and destination node can then establish pairwise key using the "bridge node".

Hash function: Hash function has a feature: for a given hash value, there is no practical way to calculate a raw input, in other words, the input is difficult to forge. For example, for a given output, k it is difficult to find k so that k = H (k). The commonly used hash function is MD5 and SHA-1 but MD5 and SHA-1 face many threats (Wang and Yu, 2005; Wang *et al*., 2005), thus they have poor safety performance. This study uses SHA-2 as hash function.

AN ENHANCED SCHEME BASED ON HASH-CHAIN

The details of enhanced scheme based on hash-chain: In WSN, the nodes can easily be captured and the stored sensitive information will continue to obtain by attacker due to the practical and physical environment of deployment area.

For the key management schemes based on probability, the same key may be stored in many nodes, if a node is captured, the key ring will be exposed which causes the security risks among other normal nodes, that is, the captured nodes will bring additional information to be exposed. In order to reduce the impact of node capture attack and the exposure of additional sensitive information, this study presents an enhanced scheme against node capture attack based on hash chain. The basic idea is to apply a hash function on the initial preloaded keys before deployment. If a node selects a key, it will use pre-stored hash function to hash the key according to certain rules and the hashed results will be as the communication key. Algorithm includes the following three steps:

Step 1: Key pre-distribution phase. the off-line key server generates key pool s, the size is |s| and each key has a ID, denoted by K_i ($\leq i \leq s$). Before deployment, each node randomly selects m (m<s) key from the key pool as key ring, The difference between the proposed scheme and E-G scheme is that the selected keys must be hashed (is node and is system parameter) times. Thus the key ring in node is:

$$Kr^j = \{h^{i \bmod N}(k_1), h^{i \bmod N}(k_2),..., h^{i \bmod N}(Km)\} \quad (1)$$

where, k_1, k_2,....,k_m is the selected keys. The one-way property of hash function can reduce the exposure of additional information caused by node capture attack. If the node i is captured and the stored information is obtained by attacker, but If node j which stored the same key with node i meets (j mod N) < (i mod N), even if the key information stored in the node i is captured, which will not affect the node j's key safety and reduce the number of the link captured and enhance the network security.

Step 2: The pairwise key establishment phase. After node deployment, the adjacent nodes establish the pairwise key through broadcasting the key identifier. If more than two keys are shared by the two nodes, then they can calculate the pairwise according to certain rules. For example, if the node i and node j share q(q>0) key and meet j mod N < (i mod N), then the node i can use (2) to compute the pairwise key with the node j, the node j can use (3) to calculate the pairwise key with i the node , where k_1, k_2 ,...., k_q is the shared key.

$$K_{ij} = \text{Hash}(k_1 \| k_2 \| ... \| k_q) \quad (2)$$

$$K_{ji} = \text{Hash}(h^{i \bmod N - j \bmod N}(K_1) \| h^{i \bmod N - j \bmod N}(K_2) \| ... \| h^{i \bmod N - j \bmod N}(K_q)) \quad (3)$$

Step 3: The key path establishment phase. If the adjacent nodes do not have a shared key, then the intermediate nodes must be as a "bridge node" to complete the key to the establishment. Supposing that there are intermediate nodes n_1, n_2,..., n_i between the source node n_s and destination node n_d and each pair of neighboring nodes in the path has direct pairwise key, the source node first broadcasts key identifiers it carriers which is forwarded among nodes and finally it finds a middle node which has pairwise with the source and destination node, respectively. Thus, the pairwise key of the source and destination node is established.

An example: In order to illustrate the proposed scheme, let us refer to the Fig. 1. To simplify the comprehension, assuming that the network has seven nodes and six secure links. In E-G and q-composite scheme, the corruption of the two nodes 3 and 7 induces the disclosure of the keys K1, K2, K3, K4 and K5 then the compromise of the two external links (1, 4) and (1, 5) (Fig. 1a). In the proposed scheme, keys are hashed before deployment (assuming in the example that the system parameter N = 5), the corruption of the two nodes 3 and 7 induces the disclosure of the derived keys $h^3(K2)$, $h^3(K3)$, $h^3(K4)$, $h^2(K1)$, $h^2(K2)$ and $h^2(K5)$ (Fig. 1b). However, In this case, the two external links (1, 4) and (1, 5) cannot be compromised because it is infeasible to calculate h (K1) and h (K2) knowing $h^2(K1)$ and $h^2(K2)$.

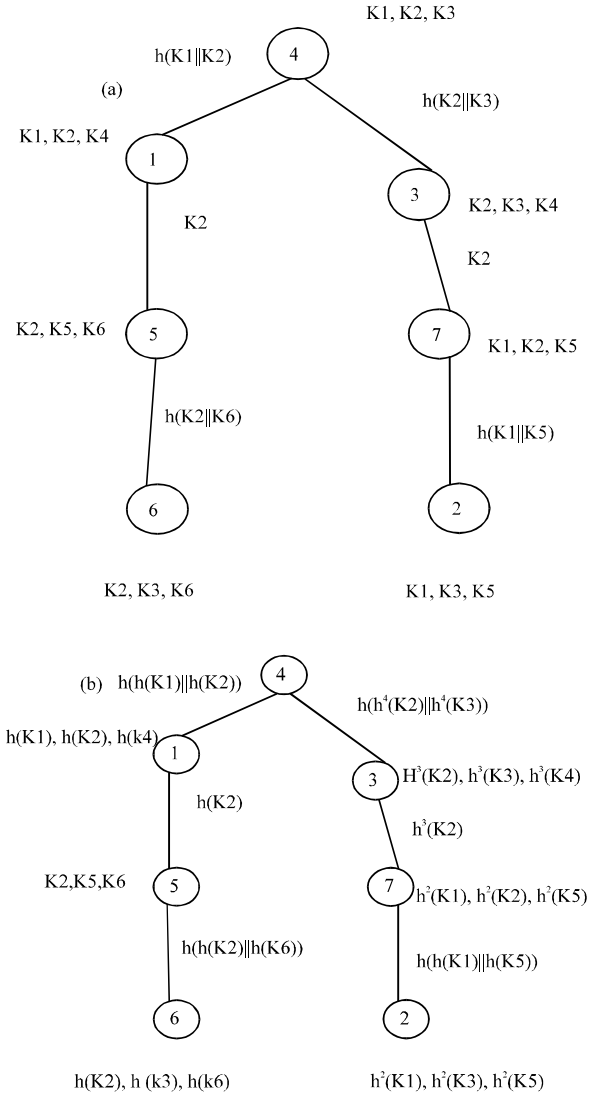

Fig. 1(a-b): Example of E-G scheme, q-composite and the proposed scheme. (a) Example of E-G scheme and q-composite and (b) example of the proposed scheme

SAFETY ANALYSIS AND EXPERIMENTAL SIMULATION

Key exposal probability: In E-G scheme, when a node is captured, the fraction of discovered keys is $p = m/|s|$, the fraction of uncompromised keys is then 1-p, When x nodes are compromised the fraction of uncompromised keys is $(1-p)^x$. The probability that a given key has been known is then $1-(1-p)^x$. For any given link composed of k shared keys the probability of being compromised is $(1-(1-p)^x)^k$. Let be the probability that two nodes share exactly k keys:

$$p(k) = \binom{|S|}{k}\binom{|S|-k}{2(m-k)}\binom{2(m-k)}{m-k} \Big/ \binom{|S|}{m}^2 \quad (4)$$

By calculating, the probability of a link between two uncompromised nodes being compromised when x nodes are compromised is:

$$p_{1x} = \sum_{k=1}^{m}(1-(1-\frac{m}{|S|})^x)^k \frac{p(k)}{\sum_{i=1}^{m} p(i)} \quad (5)$$

In the proposed scheme, the fraction of discovered keys when a node is captured is p_h which is shown in (6). Thus when x nodes are compromised the probability of a link between two uncompromised nodes being compromised is (7), the result is shown in Fig. 2, from the figure, due to the use of hash function, compared to E-G scheme, key exposal probability decrease by 56% which demonstrates the proposed scheme has excellent performance against node capture attack.

$$p_h = \frac{N+1}{2N}\frac{m}{|S|} \quad (6)$$

$$p_{hlx} = \sum_{k=1}^{m}(1-(1-\frac{N+1}{2N}\frac{m}{|S|})^x)^k \frac{p(k)}{\sum_{i=1}^{m} p(i)} \quad (7)$$

Average insecure degree: In E-G scheme, because a node randomly selects different keys from key pool, then one key may be selected by many nodes in a certain probability, if the key is captured, the nodes which store the captured key are unsafe. Average insecure degree measures, for each link key, the number of nodes that will reveal information about the link key if they are captured. Supposing there is one key i with iD k_i, the set of nodes which store the key k_i is t_i with the size $|T_i|$, the node u and v use the key k_i as their pairwise key, thus there is $(2|T_i|)$different u and v combinations in T_i, for each combination, there is (T_i-2) nodes which may leak the key. So, average insecure degree of the key k_i is (T_i-2). As for the entire network, average insecure degree is $(M-2)m/|s|$, where m is the total number of the whole network. In the proposed scheme, when one node is captured, the nodes which store the same key may be safe because the number of hash is different. If hash times are greater than the captured node, the nodes is safe, conversely, the node is unsafe. Supposing the key k_i is captured, the probability that k_i is hashed j $(0 \le j \le N-1)$ times is 1/N and the probability that the key k_i is captured is (N-j)/N, by applying the law of total probability, as for the whole network, when one node is captured the probability that the key k_i is captured is:

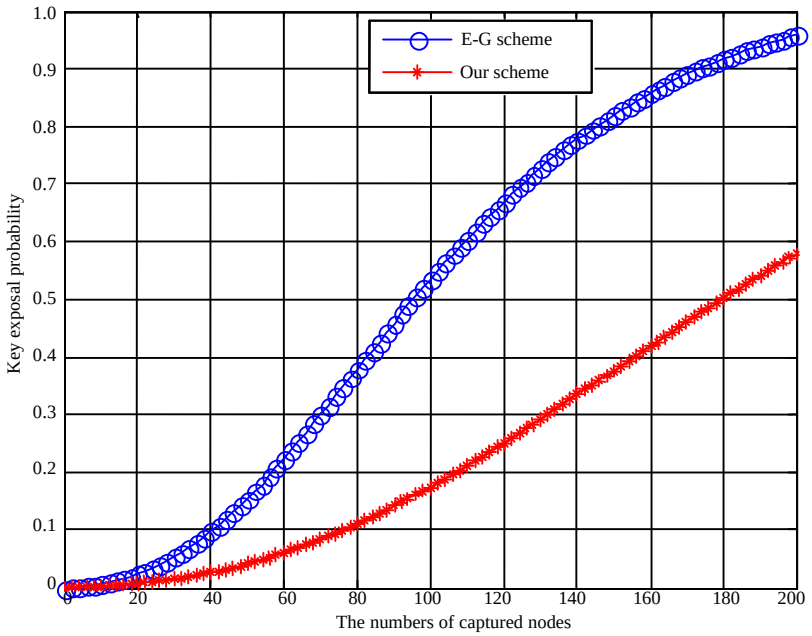

Fig. 2: Key exposal probability as a function of number of captured nodes

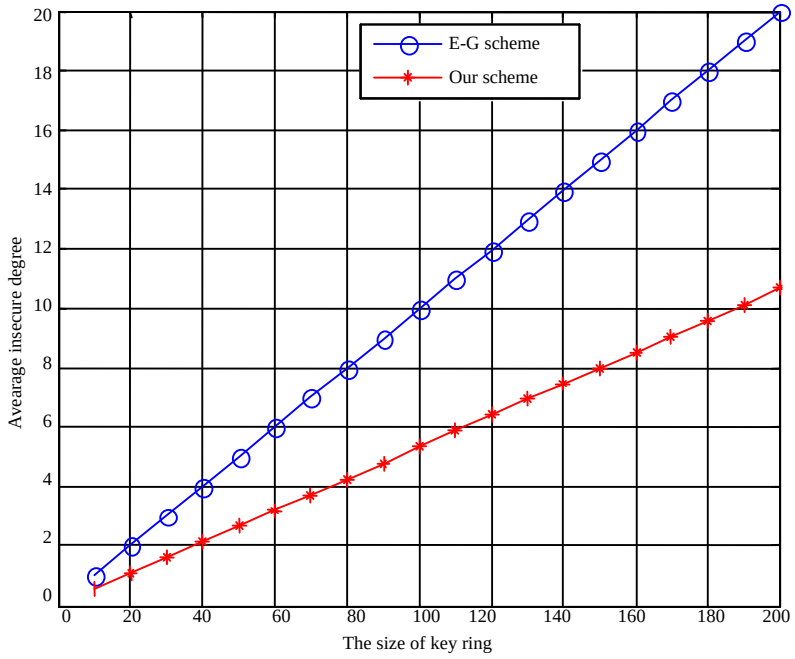

Fig. 3: Average insecure degree as a function of size of key ring

$$\sum_{j=0}^{N-1} \frac{N-j}{N}\frac{1}{N} = \frac{N+1}{2N}$$

According to the above analysis, if the set of nodes which store the key k_i is T_i, thus the average insecure degree of key k_i is $(N+1)|T_i-2|/(2N)$. As for the entire network, the average insecure degree is $(N+1)(m-2)m/(2N|s|)$. Figure 3 shows that compared to E-G scheme, the proposed scheme makes average insecure degree drop by 46.7% which reduces exposure of the extra information

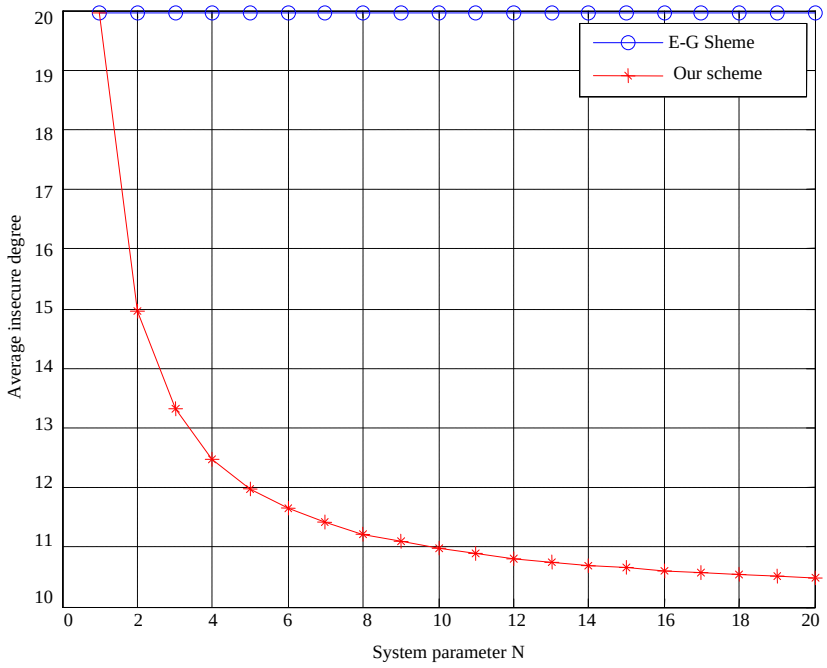

Fig. 4: Average insecure degree as a function of system parameter N

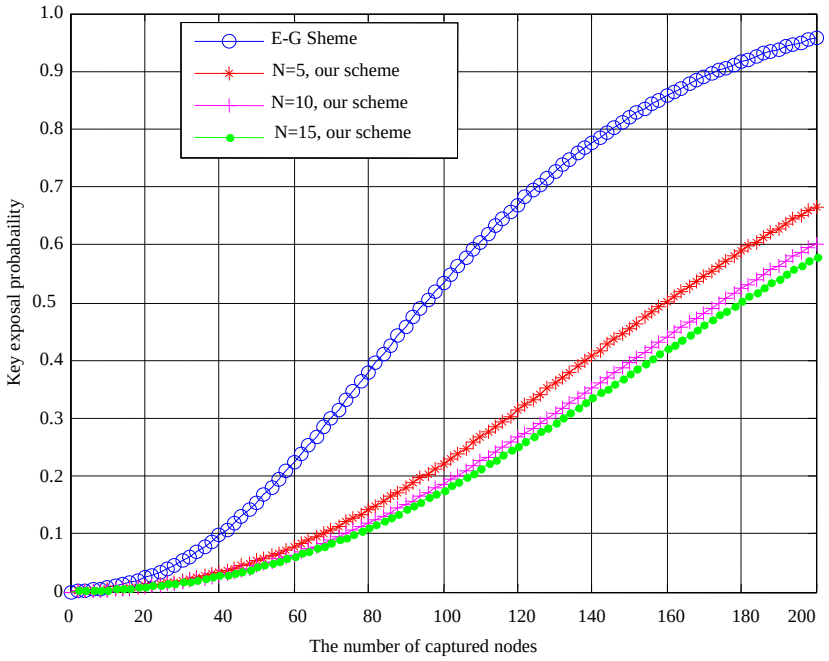

Fig. 5: Key exposal probability as a function of number of captured nodes with different system parameter N

caused by node captured attack and enhances safety performance of the network.

The selection of system parameters N: As description in section 3, the selection of system parameters N has a major impact on the performance of the proposed scheme. If the selected N is too large, the computational complexity will increase and power consumption is higher, which is not appropriate for WSN in the shortage of energy resources. If the selected N is too small, key

exposal probability and average insecure degree will increase. Average insecure degree changes with the system parameter N which is shown in Fig. 4. As shown in Fig. 4 because the E-G scheme does not use the hash chain and thus average insecure degree does not vary with changes in system parameters N. In the proposed scheme, a general trend is that the average insecure degree decreases as the system parameter becomes bigger. Furthermore, the average insecure degree of the proposed are about 45% less than the values of E-G scheme when N = 10.

Figure 5 presents the performance of the proposed and E-G scheme in terms of key exposal probability with different system parameter N. As shown in the plot, the key exposal probability grows as the number of captured node increases for both schemes. However, in the proposed scheme, due to the use of hash chain, the key exposal probability is always smaller than the E-G scheme. Meanwhile, the key exposal probability of the proposed are about 58% less than the values of E-G scheme when the number of captured node is 100.

It also should be noted that the increase of system parameter N also means communication and computing cost increase. Since the limit of N+1/2N as N approaches infinity is 1/2, N between 10 and 20 is proposed which makes the computation performances acceptable since nodes apply hash function a low number of times while not bringing too much computational overhead.

CONCLUSION

Security is the primary issue that affects large-scale application of wireless sensor networks. The study focuses on how to improve the resilience against node capture attack, from the perspective of key management, a new enhanced and hash chain based scheme against node capture attack was proposed. By using hash-chain, key exposal probability and average insecure degree are significantly reduced. Both the analytical and numerical results were presented, compared to existing schemes, the resilience against node capture attack is strengthened and the survivability of overall network is enhanced. The future work is to combine the deployment knowledge and hash chain to further enhance network survivability while focusing on analysis of the impact of time factor.

ACKNOWLEDGMENTS

This study was partly supported by Social Science Foundation of Hunan Province under Grant No. 2010YBA229 (2010.1-2012.12, The Committee Party School of Hunan.

REFERENCES

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

Albath, J. And S. Madria, 2007. Practical Algorithm for Data Security (PADS) in wireless sensor networks. Proceedings of the 6th ACM International Workshop on Data Engineering for Wireless and Mobile Access, June 10, 2007, ACM, New York, pp: 9-16.

Bla, E.O. and M. Zitterbart, 2006. An efficient key establishment scheme for secure aggregating sensor networks. Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, March 21-23, 2006, ACM, New York, pp: 303-310.

Capkun, S. and J.P. Hubaux, 2005. Secure positioning of wireless devices with application to sensor networks. Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, March 13-17, 2005, Piscataway, New Jersey, pp: 1917-1928.

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, 2003, Berkeley, CA, pp: 197-213.

Chen, T.S., J. Chen and Y.R. Tu, 2011. A study of bidirectional antenna for indoor localization using zigbee wireless sensor network. Inform. Technol. J., 10: 1836-1841.

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, 2008, ACM, New York, USA., pp: 214-219.

D'Arco, P., 2001. On the distribution of a key distribution center. Lecture Notes Comput. Sci., 2202: 357-369.

De Soete, M., 1993. Public key cryptography. Lecture Notes Comput. Sci., 741: 31-49.

Di Pietro, R., L.V. Mancini, C. Soriente, A. Spognardi and G. Tsudik, 2009. Data security in unattended wireless sensor network. IEEE Transact. Comput., 58: 1500-1511.

Idris, M.Y.I., E.M. Tamil, N.M. Noor, Z. Razak and K.W. Fong, 2009. Parking guidance system utilizing wireless sensor network and ultrasonic sensor. Inform. Technol. J., 8: 138-146.

Laurent, E. and V.D. Gligor, 2002. A key-management scheme for distributed sensor networks. Proceedings of the 9th ACM Conference on Computer and Communications Security, November 18-22, 2002, ACM Press, Washington, DC. USA., pp: 41-47.

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

Ren, H., X. Sun, Z. Ruan and B. Wang, 2011. An efficient scheme against node capture attacks using secure pairwise key for sensor networks. Inform. Technol. J., 10: 71-79.

Su, Z., C. Lin and F.J. Feng, 2007. Key management schemes and protocols for wireless sensor networks. J. Software, 18: 1218-1231.

Wang, X. and H. Yu, 2005. How to break MD5 and other hash functions. Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, May 22-26, 2005, Springer-Verlag, Berlin, Germany, pp: 19-35.

Wang, X., H. Yu and Y.L. Yin, 2005. Efficient collision search attacks on SHA-0. Lect. Notes Comput. Sci., 3621: 1-16.

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.