International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.225-234
http://dx.doi.org/10.14257/ijsia.2016.10.5.21

An Improved Random Key Predistribution Scheme for Wireless Sensor Networks Using Deployment Knowledge

Lina Zhu[1,2], Zuochang Zhang[2], Jianhua Li[1] and Renjie Zhou[3]

[1] *School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai, China*
[2]*School of Information and Statistics, Guangxi University of Finance and Economics, Nanning, China*
[3]*Key Laboratory of Complex Systems Modeling and Simulation, School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, China*
zhuln@sjtu.edu.cn, geozzc@163.com, lijh888@sjtu.edu.cn, rjzhou@hdu.edu.cn

Abstract

Key management is the basis of many security mechanisms and services in wireless sensor networks (WSN). Random key predistribution scheme is widely considered as the most practical for WSN. However, this scheme faces the challenge that it cannot achieve the ideal security connectivity and strong resilience against node capture simultaneously. To address this limitation, an improved random key predistribution scheme using deployment knowledge is proposed in this paper. Firstly, sensor nodes are divided into different groups according to their location expected. And the key pool is grouped into key pool subsets accordingly. To realize the communication between adjacent groups, the corresponding key pool subsets have a certain degree of overlapping. For all keys, there is no limitation on key reuse. Neighboring nodes sharing q *common keys will establish secure link with high probability. Moreover, our scheme inherits the advantage of* q*-composite random key predistribution scheme that it can maintain security even if some nodes are captured. Theoretical analysis and simulation experiments show that the improved scheme performs well on network connectivity and resilience.*

Keywords*: wireless sensor networks, key management, key predistribution, random key predistribution, deployment knowledge*

1. Introduction

With the development of embedded technology, wireless communication technology and sensor technology, WSN has been widely used in many fields. Because of open deployment environment, dynamic topology structure, limited resources and energy, sensor nodes are faced with more threat. Security problem has become the important factor for WSN large-scale application. Key management is the cornerstone of many security services such as authentication and encryption. A critical task of key management is to establish a communication key between two sensor nodes in the network.

WSN usually consists of a large number of sensor nodes with resources strictly constrained. Due to high demand on node storage, computing, communication and energy consumption, asymmetric key management scheme is currently considered not suitable for WSN. Among various symmetric key management schemes, the most simple solution is that all nodes use the same key. Each node only needs to store one key. The storage complexity is minimum, but the resilience against nodes capture is the worst. If one node is compromised, the whole network is threatened. Another typical solution is that each node stores N-1 keys for secure communication with other N-1 nodes, where N is the total

ISSN: 1738-9976 IJSIA

number of nodes. In this scheme, some nodes captured will not affect secure communication between other nodes; but the storage complexity is O(*N*) not suitable for large-scale WSN. In WSN, adjacent nodes communicate directly; nodes far away from each other communicate by intermediate nodes. It is not necessary to create a session key for each pair of nodes, then random key distribution scheme[1][2] is proposed. Keys are selected randomly from key pool to compose key ring for each node. Nodes hold the same keys with certain probability and generate a session key using the same ones. Although random key management scheme cannot ensure that any two adjacent nodes establish secure link, but it reduces the node storage complexity, computational complexity and communication complexity. It is considered as the most suitable key management scheme for WSN.

However, random key management scheme cannot guarantee high security connectivity and strong resilience against node capture at the same time. Take *q*-composite random key predistribution scheme for example, on the premise of generating key pool and node's key ring with fixed size: to improve the security connectivity, *q* should be reduced; to strengthen the resilience against node capture, *q* should be increased. The contradiction between security connectivity and resilience has brought great challenge for research on random key management.

2. Related Work

Eschenauer and Gligor [1] first proposed a random key predistribution scheme called EG scheme for short. In this scheme, some keys were selected randomly from a key pool to set up key ring for each node, and any two nodes shared at least one key can establish a secure link. Based on EG scheme, Chan *et al*. [2] proposed a q-composite random key predistribution scheme called CPS scheme for short. They extend the number of common keys for secure communication from 1 to q. These random solutions suppose sensor nodes are deployed randomly, and they do not take into account the wireless communication range when establishing secure links.

In many practical applications, the deployment location of sensor node can be designed in advance and realized by casting at fixed points. It is more necessary for heterogeneous WSN, which not only can double the network transmission rate and prolong the network life cycle [3], but also achieve the optimal configuration of different types of nodes [4][5]. To improve the network connectivity, targeted key distribution for nodes is carried out by using deployment knowledge.

Du *et al*. [6] proposed a random key predistribution scheme using deployment knowledge. They divide physical area into square grids. Accordingly, the key pool is divided into key pool subset. There is a one-to-one correspondence between grid cells and key pool subsets. Key pool subsets corresponding to neighboring gird cells are called neighboring key pool subsets, which have a overlapping degree. However, no key is shared by more than two neighboring key pool subsets. Jaworski *et al*. [7] divided physical area and key pool into hexagon grids. For nodes to be deployed in given region, keys are selected randomly from the corresponding key pool subset and six adjacent subsets, *i.e*., key can be used up to seven times. Mittal and Novales [8] partitioned the deployment area into a grid of rectangular regions and combined neighboring regions into different types of clusters, each of which has an associated key space. The key spaces of all clusters are mutually exclusive, so sensor nodes belonging to nonneighboring regions do not share keys.

Most of these key predistribution schemes using deployment knowledge are based on EG scheme, *i.e*., any nodes in communication range shared one key can establish a secure link. Moreover, due to the use of plane figure for describing the key group, these schemes have different degrees of limitation on keys reuse, which actually goes against the random key distribution.

3. Improvement on CPS Scheme using Deployment Knowledge

Since CPS scheme is much stronger against node capture on a small scale than EG scheme, and the deployment knowledge of sensor nodes is helpful to improve the network's connectivity, we put them together to get better resilience and connectivity at the same time. In particular, there is no limit on key reuse, which is designed to ensure uniform key distribution, *i.e.*, each key has an equal probability of being assigned to a node.

In order to express clearly, symbols for subsequent use are listed in Table 1.

Table 1. Notation

Symbol	Definition
ID_{ki}	the short identifier of key k_i
ID_{Ni}	the short identifier of node N_i
k_i	the ith key in key pool
m	the number of keys in a node's key ring
N_i	the ith sensor node in WSN
P_{in}	the probability of any two nodes in a group to set up a secure link
P_{cro}	the probability of any two nodes from neighboring groups to set up a secure link
P_{glo}	the global connectivity
P_{com}	the probability of any secure link independent of captured nodes is compromised
$q_{,}$	the lower limit on the number of shared keys to establish a secure link
$q_{,,}$	the actual number of keys shared by both ends of a secure link
q	the number of keys shared by neighboring key pool subsets
S	the original cryptographic key pool
$\|S\|$	the number of keys in S
$\|S_{sub}\|$	the number of keys in key pool subset S_{sub}

3.1. Description of the Improved Scheme

The goal of this improved scheme is to allow sensor nodes to find q common keys with each of their neighbors after deployment. Our scheme follows the three-phase model including key predistribution, shared-key discovery, and path-key establishment. Because of using deployment knowledge, the first phase is considerably different from CPS scheme. Moreover, without restriction on key reuse, the first phase is also different from those key predistribution schemes using deployment knowledge already existed.

3.1.1. Initialization and Key Predistribution Phase: This phase is conducted before sensors are deployed. Sensor nodes to be deployed are randomly divided into $u \times v$ groups $G_{i,j}$ with the same size where $1 \le i \le u$ and $1 \le j \le v$. Each group of nodes are broadcasted from the deploying point arranged in a grid. The location of nodes in a group follow uniform distribution, so a node belonging to a given group can be anywhere in the corresponding region with the same probability. Similarly, the key pool S is divided into $u \times v$ key pool subsets $S_{i,j}$ with the same size where $1 \le i \le u$ and $1 \le j \le v$. $S_{i,j}$ is used by nodes in group $G_{i,j}$. Key pool subsets are called neighbors, if the corresponding node groups are deployed in neighboring grid cells.

1) Describing key pool subset: To realize the unlimited key reuse, we adopt hypergraph to depict key pool subsets. In mathematics, a hypergraph is a generalization of a graph, where an edge can connect any number of vertices. Formally, a hypergraph H is a pair $H=(X, E)$ where X is a set of elements called vertices, and E is a set of non-empty subsets of X called hyperedges. When it comes to the key pool of WSN, as shown in Figure.1, vertex denotes key and hyperedge denotes key pool subset, where $X=\{k_1, k_2, \ldots, k_{|S|}\}$, $E=\{S_{1,1}, S_{1,2}, \ldots, S_{1,v}, \ldots, S_{u,1}, S_{u,2}, \ldots, S_{u,v}\}$. Since each key pool subset has the same size, the hypergraph below is actually a k-uniform hypergraph.

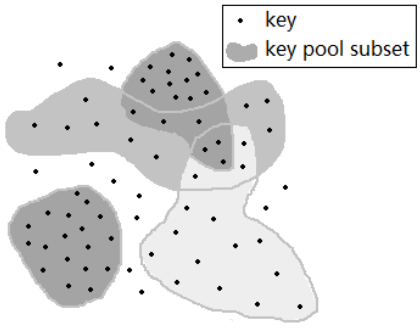


Figure 1. Describing Key Pool Subset by a Hypergraph

2) Setting up key pool subset: For simplicity, all key pool subsets are supposed to be in the same size, *i.e.*, $|S_{sub}| = \frac{|S|}{u \times v}$. Take the establishment of adjacent key pool subsets $S_{i,j}$ and $S_{i,j+1}$ for example: firstly, $|S_{sub}|$ distinct keys are randomly selected from the key pool S to make up $S_{i,j}$; and q keys denoted as S_q are randomly selected from $S_{i,j}$ to be part of $S_{i,j+1}$; then $|S_{sub}|-q$ distinct keys are randomly selected from $S-S_q$ and added into $S_{i,j+1}$. With this, neighboring key pool subsets $S_{i,j}$ and $S_{i,j+1}$ are set up, ensuring the number of shared keys no less than q and unlimited key reuse.

3) Key predistribution: After the key pool subsets are set up, for each sensor node in the deployment group $G_{i,j}$, m keys are randomly selected from the corresponding key pool subset $S_{i,j}$ to make the node's key ring. Then, these keys and their short identifiers are loaded into the memory of node.

3.1.2. Share-Key Discovery Phase: In the share-key discovery phase, each node discovers all keys shared with each of its neighbors. This can be accomplished with a simple local broadcast of all key identifiers that a node possesses. The message receiver compares the identifiers of its key ring with the key identifiers broadcasted. If the number of common keys (denoted as q') is more than q, the receiver would store the shared-key (including all common keys) with the sender's identifier and feedback the shared-key with its node identifier to the sender. Figure 2 shows the process of shared-key discovery.

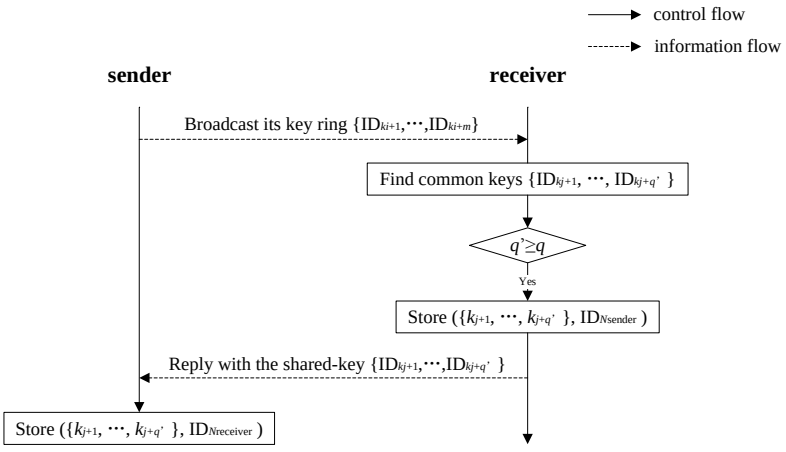


Figure 2. The Process of Shared-Key Discovery

The shared-key discovery phase establishes all secure links, both ends of which share at least q keys. A new session key K is generated by hash function using the shared-key, *e.g.*, K=hash($k_1||k_2||\ldots||k_{q'}$). Each node has a local topology information.

3.1.3. Path-key Establishment Phase: The path-key establish phase assigns a path-key to any two nodes far away but are connected by two or more secure links. Assume the communication path is $N_i \rightarrow v_1 \rightarrow v_2 \rightarrow \ldots \rightarrow N_j$: firstly, N_i selects q keys at random from its key ring as the path-key; then, it sends these keys to v_1 using the secure link between N_i and v_1; v_1 forwards them to v_2 using the secure link between v_1 and v_2 and so on until N_j receives the path-key from N_i. It's important to note that path-key is transmitted in the form of key itself instead of key identifier. There are two reasons: for one thing, N_j cannot recognize all these q keys merely according to their short identifiers; for another, the communication path from N_i to N_j is composed of secure links ensuring the path-key security.

To find secure multi-hop communication paths for any two nodes, the easiest way is flooding. As shown in [6], most of these multi-hop paths are within three hops. Therefore, the lifetime of flooding messages can be limited to reduce flooding overhead.

3.2. Evaluation of the Improved Scheme

By analyzing the relationship among parameters such as the key pool size, the overlapping degree of neighboring key pool subsets, the node's key ring size, q, and the probability of any two nodes connected, we evaluate network connectivity and resilience against node capture of the improved scheme.

3.2.1. Local Connectivity: Local connectivity refers to the probability of any two nodes within the wireless communication range establish a secure link. Suppose the wireless communication radius is bigger than the diagonal of two adjacent grid cells. Generally speaking, the wireless communication radius of sensor node is from dozens of meters to a few hundred meters. According to subsequent parameters settings, this assumption is reasonable. Since sensor nodes are divided into groups, local connectivity is analyzed under two conditions: nodes in the same group and nodes from neighboring groups.

1) Connectivity in a group: Let $p_{\text{in}}(i)$ be the probability that any two nodes in a group have i keys in common. There are $|S_{\text{sub}}|$ keys in each key pool subset, and m keys in each node's key ring. Any given nodes has $C^m_{|S_{\text{sub}}|}$ different ways of picking its m keys from the key pool subset. So there are $(C^m_{|S_{\text{sub}}|})^2$ ways for two nodes in the same group to form their key rings. Suppose these two nodes have i keys in common. There are $C^i_{|S_{\text{sub}}|}$ ways to pick the i common keys. After the i common keys have been picked, there remain $2(m-i)$ distinct keys in the two key rings that have to be picked from the remaining key pool subset. The number of ways to do this is $C^{2(m-i)}_{|S_{\text{sub}}|-i}$. The $2(m-i)$ distinct keys must be distributed to the two nodes equally. The number of such equal distributions is $C^{m-i}_{2(m-i)}$. The total number of ways to choose two key rings with i keys in common is the product of the terms above, *i.e.*, $C^i_{|S_{\text{sub}}|} \cdot C^{2(m-i)}_{|S_{\text{sub}}|-i} \cdot C^{m-i}_{2(m-i)}$. Hence, we have the probability that any two nodes in a group have i keys in common

$$p_{\text{in}}(i) = \frac{C^i_{|S_{\text{sub}}|} \cdot C^{2(m-i)}_{|S_{\text{sub}}|-i} \cdot C^{m-i}_{2(m-i)}}{(C^m_{|S_{\text{sub}}|})^2}. \quad (1)$$

The probability of any two nodes in a group to form a secure link is

$$P_{\text{in}} = 1 - \sum_{i=0}^{q-1} p_{\text{in}}(i) = \sum_{i=q}^{m} p_{\text{in}}(i) \cdot \tag{2}$$

Figure 3 shows the relationship between the local connectivity within a group and q. P_{in} decreases as q increases. When q values the half length of node's key ring, P_{in} gets close to 0.

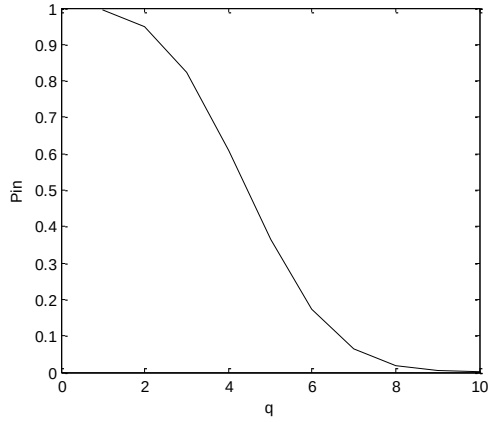


Figure 3. Local Connectivity within a Group (P_{in})

2) Connectivity between neighboring groups: Let $p_{\text{cro}}(i)$ be the probability that any two nodes from neighboring groups have i keys in common. Suppose adjacent key pool subsets share $q"$ keys denoted as $S_{q"}$ where $q" \geq q$. There are $C_{q"}^{i}$ ways to pick the i common keys. After the i common keys have been picked, for one node, the remaining $m-i$ distinct keys in its key ring can be picked from its remaining key pool subset; then for the other, the remaining $m-i$ distinct keys in its key ring can only be picked from its key pool subset except for $S_{q"}$. The order can be reversed. So the total number of ways to pick the remaining distinct keys in node's key ring is $2\times(C_{|S_{\text{sub}}|-i}^{m-i} \cdot C_{|S_{\text{sub}}|-q"}^{m-i})$. The probability that any two nodes from neighboring groups share i keys is

$$p_{\text{cro}}(i) = \frac{2C_{q"}^{i} \cdot C_{|S_{\text{sub}}|-i}^{m-i} \cdot C_{|S_{\text{sub}}|-q"}^{m-i}}{(C_{|S_{\text{sub}}|}^{m})^2} \cdot \tag{3}$$

The probability of any two nodes from neighboring groups to form a secure link is

$$P_{\text{cro}} = \sum_{i=q}^{\min\{q",m\}} p_{\text{cro}}(i) \cdot \tag{4}$$

Specific parameters for simulation are as follows: the total number of sensor nodes is 1,000; the deployment area is $100m \times 100m$; the deployment area is divided into a grid composed of $100 = u \times v = 10 \times 10$ cells with size $10m \times 10m$; the number of keys in original key pool is 10,000; the number of keys in node's key ring is 20.

From the parameter values above, there are 10 nodes in each group and 100 keys in each key pool subset, $1 \leq q \leq 20$, and $q \leq q" \leq 100$.

Figure 4 shows that the bigger q the smaller P_{cro}. In the case of fixed q, P_{cro} first increases then decreases as q'' increases. Figure 5 gives the value of q'' corresponding to the maximum P_{cro}. Statistical results show that the ideal q'' is $5q$.

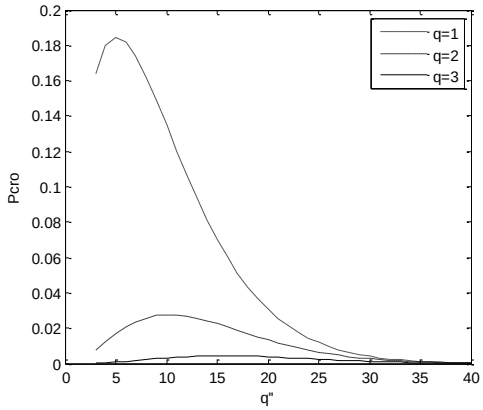


Figure 4. Local Connectivity across Neighboring Groups (P_{cro})

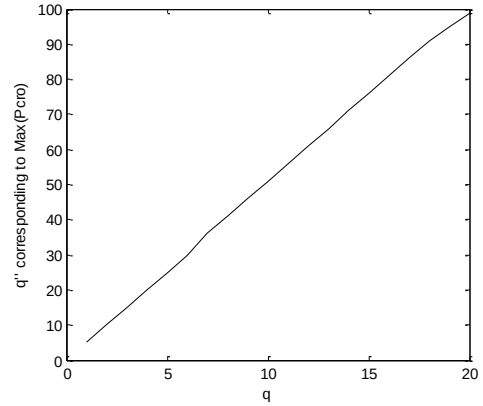


Figure 5. q'' Corresponding to the Maximum Pcro

3.2.2. Global Connectivity: When node distribution and key sharing are uniform, global connectivity can be estimated using the local connectivity and other network parameters according to Erdős-Rényi model [9][10]. A secure link here is established in two different conditions: within a group or across neighboring groups. In this improved scheme, key predistribution is a random event, since any key has an equal probability of being assigned to any node. According to the law of large numbers, the global connectivity can be measured by the average of local connectivity in two different conditions. Two nodes at the ends of a secure link are deployed independently and each of them is put in any given deployment group with an equal probability $\frac{1}{(u \times v)^2}$. Suppose these two nodes establishing a secure link share q' keys, the global connectivity is

$$P_{glo} = \frac{1}{(u \times v)^2} \times \frac{P_{in} + P_{cro}}{2} = \frac{1}{2(u \times v)^2} (\sum_{q'=q}^{m} p_{in}(q') + \sum_{q'=q}^{\min\{q'',m\}} p_{cro}(q')) \cdot \quad (5)$$

Table 2 illustrates the global connectivity value of CPS scheme and our scheme when q is different. In our scheme, the global connectivity is composed of the local connectivity within a group and cross neighboring groups. It is necessary to consider the number of common keys in neighboring key pool subsets for calculating the local connectivity cross neighboring groups. The lower limit of this parameter is q and the connectivity is a increasing function, so we give the lower limit of the global connectivity value in our scheme. The result shows that the improved scheme using deployment knowledge is much better than CPS scheme except for q=1 or 2. Strictly speaking, when q=1, it is actually EG scheme. Even if q=1 or 2, the improved scheme would also be superior to CPS scheme by increasing q''. The global connectivity of CPS scheme decreases dramatically as q increases, nevertheless, it reduces much more moderately in our scheme.

Table 2. Global Connectivity of CPS Scheme and the Improved Scheme

q	CPS scheme	Our scheme	q	CPS scheme	Our scheme
1	0.0393	≥5.3670e-005	11	1.1239e-026	≥3.9982e-009
2	7.0664e-004	≥4.7655e-005	12	7.6062e-030	≥3.6474e-010
3	7.6325e-006	≥4.1217e-005	13	3.7542e-033	≥2.4095e-011
4	5.5227e-008	≥3.0419e-005	14	1.3172e-036	≥1.1220e-012
5	2.8337e-010	≥1.8234e-005	15	3.1691e-040	≥3.5493e-014
6	1.0652e-012	≥8.6366e-006	16	4.9632e-044	≥7.2363e-016
7	2.9905e-015	≥3.1834e-006	17	4.6819e-048	≥8.7936e-018
8	6.3344e-018	≥9.0452e-007	18	2.3460e-052	≥5.6159e-020
9	1.0163e-020	≥1.9654e-007	19	4.9493e-057	≥1.4935e-022
10	1.2330e-023	≥3.2376e-008	20	2.4796e-062	≥9.3286e-026

3.2.3. Resilience against Node Capture: The goal of this part is to find out how a successful attack on some sensor nodes affects the rest. The probability that secure link between any two uncompromised nodes can be decrypted by the compromised keys is used to measure the network's resilience against node capture. Since the improved scheme is based on CPS scheme and it ensures uniform key distribution, the analysis of resilience is similar to CPS scheme except for the probability of setting up a secure link.

Let the number of captured nodes be x. The probability that a given key has not been compromised is $(1-\frac{m}{|S|})^x$. For any secure link, if the session key was the hash of q' shared keys, then the probability of that link being compromised is $(1-(1-\frac{m}{|S|})^x)^{q'}$. Two kinds of secure link should be considered respectively, and the average value is taken to measure the resilience. Hence, the probability that secure link between any two uncompromised nodes is compromised when x nodes have been captured is

$$P_{\text{com}} = \frac{1}{2}\left(\sum_{q'=q}^{m}(1-(1-\frac{m}{|S|})^x)^{q'}\frac{p_{\text{in}}(q')}{P_{\text{in}}} + \sum_{q'=q}^{\min\{q'',m\}}(1-(1-\frac{m}{|S|})^x)^{q'}\frac{p_{\text{cro}}(q')}{P_{\text{cro}}}\right). \quad (6)$$

Fix x and q, P_{com} decreases as q'' increases. Since $q'' \geq q$, the upper bound of P_{com} is calculated by $q''=q$. As shown in Figure.6, with the same number of nodes captured, P_{com} is smaller with bigger q. In other words, attacker have to capture more nodes to compromise secure links when q is bigger. The resilience of this improved scheme is better than EG scheme (q=1), even if half nodes are captured.

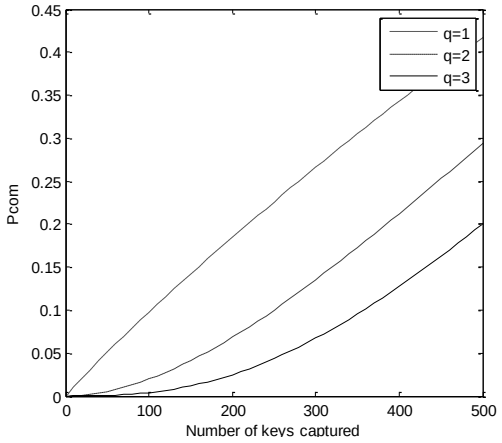


Figure 6. Probability of other Secure Links Compromised (P_{com})

4. Conclusion

An improved random key predistribution scheme using deployment knowledge is introduced in this paper. Compared with EG scheme and CPS scheme, the improved scheme considers wireless communication range and takes advantage of the prior knowledge about deployment. Compared with existing random key predistribution scheme using deployment knowledge, the improved scheme has no limit to key reuse, ensuring real random key predistribution; and it is based on CPS scheme rather than EG scheme. Simulation experimental results show that the improved scheme gets better security connectivity than CPS scheme, and better resilience against node capture than EG scheme.

Acknowledgements

The research presented in this paper was supported in part by the Special Research Fund for the Doctoral Program of Higher Education (No.20130073130006), the National Natural Science Foundation of China (No.61262002, No.61300211), Guangxi Natural Science Foundation (No.2013GXNSFBA019274), Zhejiang Natural Science Foundation (No. LQ13F020017), and Guangxi Higher Education Institution Scientific Research Project (No.2013YB214).

References

[1] L. Eschenauer and V. Gligor, "A key management scheme for distributed sensor networks", V. Atluri, Editor. Computer-communication networks. Proceedings of the 9th ACM Conference on Computer and Communications Security, **(2002)** November 18-22; Washington DC, USA, pp.41-47.
[2] H. Chan, A. Perrig, and D. Song. "Random key pre-distribution schemes for sensor networks", B. Werner, Editor. Hardware and cryptography. Proceedings of IEEE Symposium on Security and Privacy, **(2003)** May 11-14; California, USA, pp.197-213.
[3] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh. "Exploiting heterogeneity in sensor networks", K. Makki and E. Knightly, Editors. Sensor networks. Proceedings of the 24th IEEE International Conference on Computer and Communications Societies, **(2005)** March 13-17; Florida, USA, pp.878-890.
[4] V. P. Mhatre, C. Rosenberg, D. Kofman, R. R. Mazumdar, and N. B. Shroff. "A minimum cost heterogeneous sensor network with a lifetime constraint", IEEE Transactions on Mobile Computing, Vol.4, No.1, **(2005):** pp.4-14.
[5] C. H. Wu and Y. C. Chung. "Heterogeneous wireless sensor network deployment and topology control based on irregular sensor model", Lecture Notes in Computer Science, Vol.4459, **(2007)** pp.78-88.
[6] W. Du, DENG J. Deng, Y. S. Han, and P. K. Varshney. "A key predistribution scheme for sensor networks using deployment knowledge", IEEE Transactions on Dependable and Secure Computing Vol.3, No.1, **(2006)**: pp.62-77.
[7] J. Jaworski, M. Ren, and K. Rybarzyk. "Random key predistribution for wireless sensor networks using deployment knowledge", Computing **(2009)**, Vol.85, No.1-2, pp.57-76.
[8] N. Mittal and R. Novales, "Cluster-based key predistribution using deployment knowledge", IEEE Transactions on Dependable and Secure Computing Vol.7, No.3, **(2010)** pp.329-335.
[9] P. Erdős and A. Rényi, "On Random Graphs I", Publicationes Mathematicae **(1959)**, No.6, pp.290–297.
[10] B. Bollobás, Editor, Random Graphs (2nd ed.), Cambridge University Press, Cambridge **(2001)**.

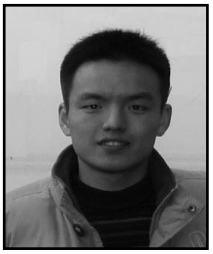
Authors

Lina Zhu received the B.S. degree in computer science and technology from Central China Normal University, Wuhan, China, in 2003, the M.S. degree in pattern recognition and intelligent system from Wuhan University, Wuhan, China, in 2006, and the Ph.D. degree in computer application technology from Harbin Engineering University, Harbin, China, in 2010. She is now an Associate Professor of Guangxi University of Finance and Economics, Nanning, China. She is also a postdoctoral research fellow from October 2014

in Shanghai Jiaotong University. Her research interests include intrusion detection, situation awareness, and WSN key management.

Zuochang Zhang received the B.S. and M.S. degrees in cartography and geography information system from Wuhan University, Wuhan, China, in 1999 and 2005. His research interests include GIS and its applications, Internet of Things, and network security. He has published several papers in these areas. He has participated in a number of domestic and foreign research projects, and developed several network security-related projects.

Jianhua Li is currently a Professor/Ph.D. Supervisor and the Dean of the College of Information Security, Shanghai Jiao Tong University, Shanghai, China, where he received the B.S., M.S., and Ph.D. degrees, in 1986, 1991, and 1998, respectively. He was the chief expert in the information security committee experts of National High Technology Research and Development Program of China (863 Program) of China. He is a Committee Member of the information security area of the state tenth five-year plan of China, a Committee Expert of the China State Secrecy Bureau and Shanghai Secrecy Bureau, and a Committee Expert of the Information Technique Standardization Committee of Shanghai, China. He was the Leader of over 30 state/province projects of China, and has authored over 200 papers. He has authored six books and holds about 20 patents. He made three standards and has five software copyrights. He was a recipient of the National Technology Progress Award of China in 2005, the National Technology Progress Award of Shanghai in 2003 and 2004, and two National Technology Progress Awards of Shanghai in 2004. His research interests include information security, signal process, and computer network communication.



Renjie Zhou is an assistant professor in Key Laboratory of Complex Systems Modeling and Simulation, School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, China. He received Ph.D. degree from Harbin Engineering University, Harbin, China, in 2012. From 2009 to 2011, he was a visiting scholar in the Department of Electrical and Computer Engineering at the University of Massachusetts at Amherst. His research interests include measurement and analysis of online social networks, and network security.