Study on Dynamic Key Management of Clustered Sensor Networks

Huanzhao Wang,† Dongwei Luo††, Feifei Chen and Zengzhi Li

Department of Computer Science & Technology,
Xi'an Jiaotong University, 710049, Xi'an,China

Summary
Sensor networks are characterized by strict resource limitations and large scalability. Many sensor network applications require secure communication, but establishing a shared key for communicating parties is very challenging. The low computational capability and small storage budget within sensor nodes render many popular public-key based key distribution and management mechanisms impractical, especially for clustered sensor networks. For address the issue of key management in clustered sensor networks, we propose a dynamic key management scheme based on key-pool in this paper. We first summarize the existing approaches of key management; in contrast with them, we introduce our scheme which consists of two phases: key distribution and key exchange. By our approach, the cluster heads and leaf nodes construct different size of key rings from the base station respectively, and the new elected cluster head will exchange keys with the old cluster head, which is called role exchange. Finally, a series of performance analysis to our scheme show that, in the clustered sensor networks, the sensor nodes save more memory resource and the entire networks shows great resilience against node capture; and an evaluation of traffic and energy consumption overhead in key exchange phase is also presented.

Key words:
Sensor networks; dynamic key management; key-pool; clustered sensor networks; key exchange.

Introduction

Nowadays, Sensor Networks has attracted more and more attentions because of its extending utilizing within ordinary life and military field. Typically, Sensor Networks is used in various kinds of fields such as environment inspection, target tracing, scientific detection and so forth. For the purpose of insuring the communication security between congeneric sensor nodes worked in antagonistic district, security mechanism like authentication and encryption in traditional networks model can be referenced as a basic safeguard. Hence information transmitting among sensor nodes can be protected by encrypting them with pre-distribution pairwise keys. But applying those tradition schemes e.g. public key encryption techniques indiscriminatingly into sensor networks is not only inadequate but also unreasonable. Since the resources possessed by sensor nodes are strictly restricted, the limited power source and storage memories of sensor nodes could not afford the heavy consumption during encrypting key generation and exchange process.

In order to adapt the prime key distribution mechanism in sensor networks, [1] brought forward a probability-based key pre-distribution mechanism to solve the problem of pairwise keys construction. And [2] made an improvement on it to achieve two key distributing mechanisms: q-composite random key pre-distribution scheme and random-pairwise keys scheme. Furthermore, [3] developed a random subset assignment scheme and a grid-based key pre-distribution scheme. [4] presented a closest pairwise keys pre-distribution scheme and a location-based pairwise keys scheme using bivariate polynomials. [5] proposed a novel random key pre-distribution scheme that exploits deployment knowledge. And based on Blom's key pre-distribution scheme [6], [7] developed a multiple-space key pre-distribution scheme.

An evident phenomenon of all the above schemes is that they all based on the sensor networks with reticulate topological structures. The arrangement of networks is not layered, which means every two nodes can communicate with each other. Obviously in the reticulate topological sensor networks, each node is completely equivalent. But issue on dynamic key management in clustered sensor networks is unsolved yet. It is obviously that in the clustered sensor networks, a sensor nodes just communicates with the nodes which in the same cluster, so it just need keep "just enough" keys other than keep keys with every nodes in the networks. And in the clustered sensor networks the cluster head nodes consume more energy than other nodes, there should be some scheme to change the cluster head, so the problem of how to distribute or exchange keys among sensor nodes when the cluster head changes need to be resolved. In this paper, we describe our key-pool based management protocols to solve this problem and analyze the performance of them on the groundwork of several experiments.

Manuscript received June 5, 2006.
Manuscript revised June 25, 2006.

2. Background and basic scheme

2.1 Properties of Sensor Networks

Sensor Networks has many properties [2] diversified from conventional networks. Here we summarize them as follows:

- *Restricted memory resource and narrow correspondence bandwidth*: sensor nodes are always inadequate in memorizer capacitance and confined in low correspondence bandwidth. It is infeasible to save all the sharing keys with their relative neighbors in one node.
- *The potential risks of being captured physically*: usually sensor nodes are low-cost and randomly broadcasted into an open territory or even an antagonistically region. There low-secure application manner embeds the potential risks of being attacked by hostile devices; and the worst situation is that all the communication keys might be captured by their enemy.
- *Hardly possible to obtain the configure information previously*: the randomization of sensor networks arrangement leads the consequences that it is a high spending and nearly impossible work to obtain the configuration information in advance.
- *Impractical to adopt Public Key Infrastructure*: the restrictions on power source and calculating capability strictly limit the conventional security solutions, including RSA Signature[8] and Diffie-Hellman key exchanging protocol[9], to migrate into the sensor networks platform.

2.2 Basic scheme

In this paper, we name the *probability-based key pre-distribution method* developed in [1] as basic scheme, which follows the principles below:

Assume *m* to be the sum account of keys saved in certain nodes. The key initialization procedure is executed before the arrangement of sensor nodes: each sensor node randomly select *m* keys from the predefined global key-pool and save them into their own memory, the aggregation of *m* keys is called the key-ring to certain node.

After that, it comes into the key setup phase. First the whole system enforces a key detection protocol to find out every sensor node' neighbors who contains no less than one shared keys with it. This key detection protocol is simply implemented by assigning static mark to each key before the arrangement phase, and every node broadcasts its static key marks set during the protocol performing. Then the affirmations are achieved by each sensor node through handshaking protocol. It will unveil the key sharing relationship between that node and its neighbor. The sharing key is used as encryption key while establishing a communication link.

The nodes and the communication links between them form a connected graph after the key setup phase. If there is not sharing key between certain node and its neighbors, they should negotiate a path key and use it to construct a secure link. Then in a connected topology, since there always has a path between each pair of nodes, the source node can transfer a path key to its destination through this link.

Consider a random graph $G(n, p_l)$, a graph of n nodes, the probability that a link exists between any two nodes is p_l. [10] showed that for monotone properties of a graph $G(n, p_l)$, there exists a value of p_l over which the property exhibits a 'phase transition', i.e. it abruptly transitions from 'likely false' to 'likely true'. Hence, it is possible to calculate some expected degree d for the vertices in the graph such that the graph is connected with some high probability c. [1] calculates the necessary expected node degree d in terms of the size of networks n as:

$$d = (\frac{n}{n-1})(\ln(n) - \ln(-\ln(c))) \quad (1)$$

For a given density of sensor networks deployment, let n' be the expected number of neighbors within communication range of a node. Since the expected node degree must be at least d as calculated, the required probability p of successfully performing key setup phase with its neighbors is:

$$p = \frac{d}{n'} \quad (2)$$

3. Dynamic key management of clustered Sensor Networks

Basic scheme [1] has partly solved the problem of keys distribution in Sensor Networks. It shows great resilience against node capture and reasonably supports large networks scale. However, this scheme and the posterior improved schemes have not resolved the problem of keys management in Sensor Networks entirely. Especially, most proposed schemes are based on Sensor Networks with reticulate topological structures, whereas none of them focuses on the problem of keys management in the clustered sensor networks architecture. So in this paper we propose our key-pool based dynamical key management protocol in hopes of solving this problem.

3.1 Architecture of clustered Sensor Networks

A typical Sensor Networks is composed of several hundreds to thousands of sensor nodes. Each sensor node is mainly limited in computation and information storage capacity, mean time, with highly power constraint and communicates thought a short-range wireless networks interface. Most sensor networks have a base station that acts as a gateway. It is the coordinator and arbiter of the sensor networks, and the center of data processing.

Except for the base station, the sensor nodes are separated into two categories logically according to their residence positions in sensor networks as well as their roles in the data handling process. One is called leaf node, which does the material sense jobs and transfer those monitor data to the "lead node"; the other is cluster-head node, which aggregates the data from leaf nodes, and send the packed data messages to the base station. Nodes can cooperate with others to accomplish tasks by wireless communication after the topology has formed right after the deployment.

What should be noticed especially is the nodes in different clusters do not communicate with each other, while only the nodes in same cluster can. This prescription will significantly depress the traffic of networks than the reticulate topological does. Here we assume every node in the same cluster can communicate with each other. Fig.1 shows the classic architecture of clustered sensor networks. In this architecture, communications among sensor nodes are loose synchronized in order to meliorate the networks management efficiency. Time axis is divided into slots, and every node is assigned to a time slot under the surveillance of base station. So the communication behaviors only occur during their restricted slots, and they will turn into sleep mode during other slots to save their power.

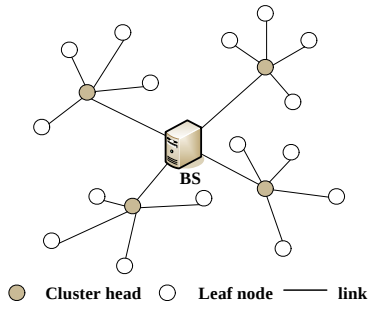


Fig. 1 Architecture of clustered sensor networks

3.2 Dynamic key management of clustered Sensor Networks

Dynamic key management based on key pool requires two manipulations—dynamic key distributing and key exchanging, which can be conveniently classified as two phase illuminated behind.

3.2.1 Dynamic key distribution

In dynamic key distribution phase, each node selects its key ring according to the networks architecture. As the base station represents to be the topological root, it constructs a key set S as its key ring from the globe key space. Then other nodes mentioned above construct their own key rings after the base station broadcasts its key ring. This key distribution process can be formalized as follows:

- Set S denotes the key ring of base station, A_{i_1} is the key ring of certain cluster head node. A'_{i_1} is the new generation key-pool of certain cluster head node given by base station; $C_{i_1 i_2}$ is the key ring of certain leaf node.
- For $\forall A_{i_1}, 1 \le i_1 \le d$, $A_{i_1} \subset S$, d is the account of cluster head nodes in the certain sensor networks;
- For $\forall C_{i_1 i_2} (1 \le i_1 \le d, 1 \le i_2 \le n)$, exists $A'_{i_1} \subset S$ and $C_{i_1 i_2} \subset A'_{i_1}$, makes $\exists K \in A_{i_1}$, then $K \in A'_{i_1}$ and $K \in C_{i_1 i_2}$.

Since sensor nodes need communicate with each other to form the topologic after deployment, but at that moment, the communication keys have not distributed yet. So it should introduce advisable authentication scheme to avoid invalid nodes with illegal authorizations entering into the sensor networks.

During the phase of key setup, each node should detect whether it keeps common keys with its neighbors respectively. This can be accomplished by broadcasting all the key identifiers a node possessing. However, this broadcasting and detecting approach is straightforward to implement, but it has obvious disadvantage. A casual eavesdropper may intentionally identify the key sets of all the nodes in a network, and thus picks an optimal set of nodes for reckoning a large subset of the key pool S , which will threaten the whole networks accumulatively. A more secure method of key detection is to utilize client puzzles such as a Merkle puzzle proposed in [11]. Fig.2 shows the process of key setup.

As shown in Fig.2, if a leaf node which pretends to be a receiver detects that it possesses a common key with the broadcasting node in its cluster, it will return an ACK message carrying the common key identify to this broadcasting node. This node listens to the traffic after

broadcasted its key ring and receives all the ACKs. Through this, the broadcasting node learns the same keys between it and every response nodes then use them to establish secure links.

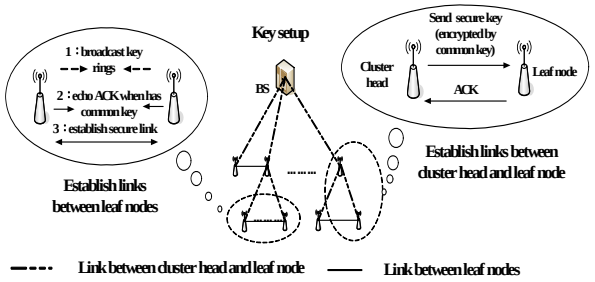


Fig. 2 Key setup phase of dynamic key distribution in clustered sensor networks

The instance of constructing secure link between the cluster head and a leaf node is quite different from above. The cluster node first randomly generates a key K as its link key. Because every node in its cluster at least shares one common key K_i with the cluster head, hence it generates a sealed packet with the key K, which encrypted by the key K_i , and then sends this packet to the corresponding leaf node. When the leaf node receives the packet, it gets the link key K by decrypting the packet with K_i , and finally sends ACK to the cluster head. So the cluster head and the leaf node are possible to use this key K to communicate with each other through the secure link.

Since each key of certain node is randomly picked up from the key ring of base station, a possible consequence is that the key rings of two nodes in the same cluster are all composed of distinguished keys; hence it requires building path key.

To insure a higher connectivity probability in the entire sensor networks, the size of key rings specified in key setup phase should be appropriate. Suppose there are two given nodes n_1,n_2 in the same cluster, by chance without common keys in their key ring. However, there is a great opportunity to form a secure link n_1,s_1..s_n,n_2 between them, where each pair of nodes physically neighborhood on this link carries a common key. The process of secure link generation is illustrated in Fig.3; the source node n_1 generates a secure key X and sends X to the destination node n_2 through the prior secure link. At last, n_2 returns ACK to the source node. Finally the secure path is set up with the key X.

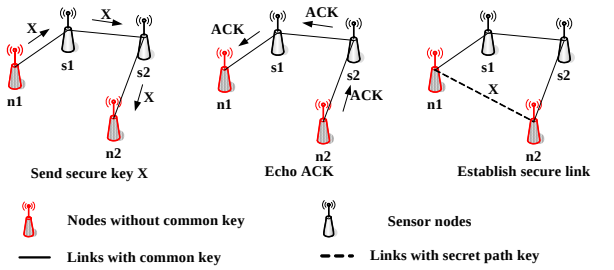


Fig. 3 Establish secure link with secret path key

Through the phases described above, the entire sensor networks forms a connectivity graph, in which the nodes of same cluster can communicate with each other through secure links. The cluster head nodes send the data packets received from leaf nodes to their up layer parents till the packets arrive to base station.

3.2.2 Key exchange

In clustered sensor networks, the cluster head nodes consume more energy than the leaf nodes do because of the heavy traffic and data process. In order to lengthen the life time of sensor networks, there must be a scheme to balance the energy consume among the sensor nodes. Thus we propose a key exchange scheme to address the issue of balancing energy consume. This scheme is designed to balance the energy consume among nodes by ‘role exchange’, mean time to insure their secure communication. It also reduces the extra traffic for reaching the consuming balance.

In a typical sensor networks, the communication among sensor nodes are loose time synchronized. The leaf nodes work in their own slots, and in other slots they go into the idle or sleep mode, by this means, they save more energy for telling traffic. However, the cluster head nodes are assumed to work in busy mode all the time.

For lower the energy consumption of cluster head, sensor networks will be reorganized after a round of data transmission has completed, i.e. all the leaf nodes have ‘loose synchronized’ with their cluster head once. This reorganization process will be accomplished by adding a time slot to the end of data transmission period. Each cluster in the sensor networks selects a more powerful cluster head in this special slot. Then a role exchange process will happen between the new cluster head and the old one. In this process, the two nodes exchange their key rings and other cluster management information. The whole process is transparent to others nodes of same cluster, namely all the other nodes will not realize this transform, they just communicate with each other as usual.

The process of keys exchange is shown in Fig.4.

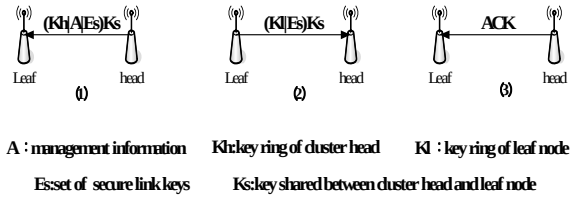


Fig. 4 Key exchange phase

First, the old cluster head send a message which contains cluster management information, key ring of old cluster head and set of all secure link keys relative to it to the new cluster head. The message should be encrypted by the common key between the old and new cluster head. Then the new cluster head receives the message, it decrypts the message by the common key and return a message which contains its own corresponding information to the old cluster head. Finally, the old cluster head echoes an ACK to accomplish the "role exchange" process.

Obviously, this keys exchange process makes the entire sensor networks run efficient; because it releases the burden of all nodes manipulating the dynamic key distribution again after the topologic has changed. Now the extra overhead only includes the traffic of 'role exchange'.

4. Performance analysis

As analysis in section 2, sensor nodes should take less memory on the premise of secure communication because of their strict memory constraint. So that the key rings of every node should be sufficient small in the case of certain connectivity probability. Second, even if some nodes have been captured by an adversary, the scheme should be strong enough to protect other nodes and links between them to be safe. We name this property the resilience against nodes capture. Finally, the key exchanging cost should be low to make the whole networks runs efficiently. So under the guidelines above, here in this section, we will evaluate the performance of our dynamic key management of clustered sensor networks.

4.1 The relation between key ring size and networks connectivity probability

According to Eq.1 and Eq.2 in section 2, the provided number of sensors in the entire networks is n, expected probability of whole networks connectivity is c and expected number of neighbors is n'. Then via Eq.1, we first calculate the expected degree of any given node d. Then we use d for calculating p via Eq.2, the desired probability that any two nodes can execute process of key setup. So in order to provide the probability p in clustered sensor networks, the key ring sizes of cluster head nodes should satisfy the equation:

$$P = P_{cluster-head} = 1 - \frac{C_{2m_1}^{|S|} \cdot C_{m_1}^{2m_1}}{(C_{m_1}^{|S|})^2} \quad (3)$$

Here the key ring size of base station is $|S|$ and the key ring size of cluster head nodes is m_1. Any given cluster head node has $(C_{m_1}^{|S|})$ different ways of picking its m_1 keys from the key pool of size $|S|$. And two cluster head nodes have $(C_{2m_1}^{|S|} \cdot C_{m_1}^{2m_1})$ ways of having no common key in their key rings of size m_1.

Similarly, for the leaf nodes in a cluster, assume the key ring size of them is m_2, they fulfill the equation:

$$P = P_{leaf} = 1 - \frac{C_{2m_2}^{|m_1} \cdot C_{m_2}^{2m2}}{(C_{m_2}^{m_1})^2} \quad (4)$$

Based on the analysis above, we can see that key ring size of every sensor node in the basic scheme are the same, and it right equal to the size m_1 of cluster head nodes within the clustered sensor networks. But in the clustered sensor networks, the key ring size of leaf nodes is smaller than the cluster heads', i.e. $m_2 \le m_1$. So in dynamic keys management scheme of clustered sensor networks, the leaf nodes can save more memory resource for keys storage, significantly low cost than in the basic scheme of flat networks structure.

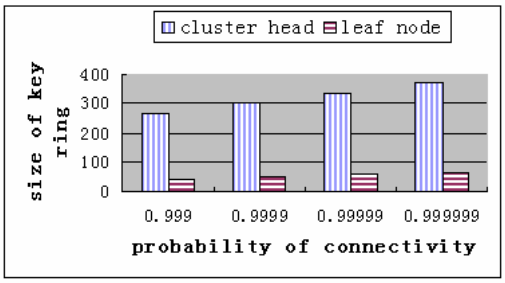


Fig. 5 Relationship between size of key ring and probability of connectivity

Fig.5 shows the relationship between size of key ring and the probability of connectivity. We can learn that the size

of key ring of cluster head in our dynamical key management of clustered sensor networks is equal to the size of key ring of all nodes in the basic scheme, but the key ring size of leaf node is much smaller than the key ring size of cluster head. So it can save more memory resource in dynamical key management of clustered sensor networks. And the Fig.5 shows that if the sensor networks need higher probability of connectivity, the nodes must keep more keys in their own key ring.

4.2 Resilience against node capture

In this section, we estimate our approach on improving sensor network's resilience against node capture attack. Eavesdropping on the fraction of links in the networks, an attacker is possible to cause intention damage to the entire networks by recovering keys from captured nodes.

Let the number of nodes in the entire sensor networks is n and the number of captured nodes is n_C. Assume that the size of every cluster in the clustered sensor networks is of the same, namely they all are composed of d sensor nodes. So we have:

$$n = d + d^2 \tag{5}$$

Because the key ring size of cluster head is different form leaf nodes, so when a node has been captured, the average number of keys to be recovered is:

$$C = \frac{d \cdot m_1 + d^2 \cdot m_2}{n} \tag{6}$$

Then the probability of any key to be recovered in key pool S is:

$$P_c = \frac{C}{|S|} \tag{7}$$

Hence the probability of any secure link to be attacked is:

$$P_a = 1 - ((1 - P_C)^{n_C}) \tag{8}$$

In dynamic keys management of clustered sensor networks, the key ring size of leaf nodes is smaller than the basic scheme, so if a certain number of nodes have been captured, there will be fewer keys to be recovered in our scheme. We also learn form Eq.8 that the probability of secure links been attacked in dynamic keys management is lower than basic scheme. It is obvious that dynamic key management based on key pool in clustered sensor networks provides a better resilient against nodes capture than basic scheme.

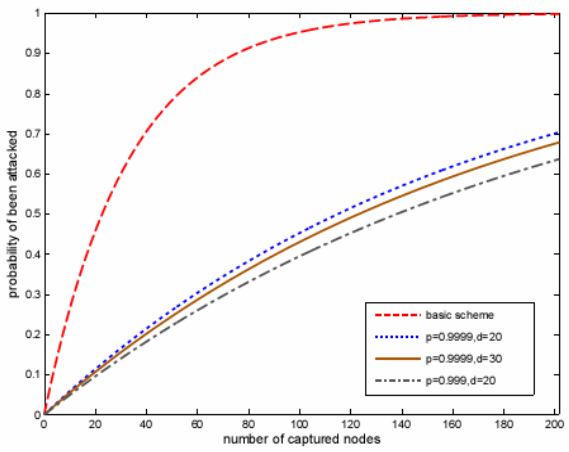


Fig. 6 Resilience against node capture
(p: probability of connectivity; d: size of cluster)

As Fig.6 shows, the resilience against node capture in dynamical key management of clustered sensor networks is better than the basic scheme. With the same number of nodes being captured, the secure link in our approach has smaller probability of been attacked than in basic scheme. We can also learn that the larger size of the cluster, the better resilience of the networks under the same probability of connectivity. Moreover, smaller required probability of connectivity leads to better resilience under stated size of cluster.

4.3 Communication overhead of key exchange

Every sensor nodes share the energy consuming in the reticulate topological sensor networks. But unique properties in the clustered sensor networks call for the mechanism of balancing energy consuming. In proposed dynamic keys management, keys exchange solves the problem above after a whole round of data transmission has finished, which can be accomplished by insert a special slot. The overhead of key exchange is weighed in the following way.

Noted that in the sensor networks, even though every leaf node keep a common key with the corresponding cluster head, the message transmitted between them always be in the multi-hop mode. Assume that the sensor network is composed of n clusters, and i–*cluster* is composed of d_i nodes. For multi-hop route in sensor networks, let P_j be the rate of data packet being transmitted through j hops, and d be the number of slots for the whole data transmission. The number of time slot for the whole data transmission in each cluster may be different; the d should be large enough to make every cluster finish a whole data transmission. From section 3.2.2, there are

three extra packets in keys exchange, so the equation of calculating overhead of keys exchange is (A denotes the additional spending ratio under normal working condition, compared to available communications traffic):

$$A=\frac{3n}{\sum_{i=1}^{n}\sum_{j=1}^{d_i} jp_j d_i + n} \quad (9)$$

Obviously in the classic sensor networks, there is more energy consumption in the message transmission than in the data processing. So the Eq.9 reflects overhead of energy consumption of the key exchange on some level.

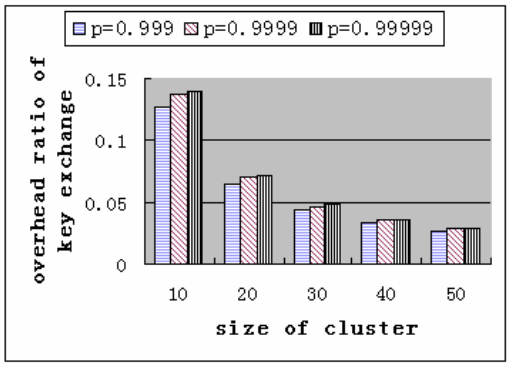


Fig.7 Communication overhead of key exchange

From Fig.7, the smaller size of cluster it is, the larger ratio of communication overhead will be during the phase of key exchange, that's because large cluster scale will lead to more effective communication traffic involved in the whole traffic. And it also shows that it may have larger ratio of overhead when the networks has a higher probability of connectivity, with a fixed size of cluster. The direct reason of this phenomenon is higher connectivity probability leads to bigger key ring residing in a node, consequently results in the decrease of whole traffic.

5. Conclusion and Future Works

In this paper, we introduce a dynamical key management scheme of clustered sensor networks and illuminate the key distribution and exchange process in this scheme. In our approach, the cluster heads and leaf nodes select different size of key rings from the base station respectively and the new elected cluster head will exchange keys with the old cluster head, which is called role exchange. The performance analysis in section 4 shows that the leaf nodes save more memory resource than the nodes in basic scheme do. We can also learn that in our approach the sensor networks shows great resilience against node capture attack. In the last of performance analysis, we evaluate the traffic and energy consumption overhead of the key exchange.

The challenge in our future work is to establish a secure routing architecture strengthened by our approach in clustered topological sensor networks. In addition, we will study the global connectivity and the local resilience in the sensor networks. Other key distribution and key exchange scheme will also be considered.

References

[1] Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communication Security, pp. 41-47, November 2002.

[2] H. Chan, A. Perrig, and D. Song.. Random key predistribution schemes for sensor networks. In IEEE Symposium on Research in Security and Privacy, 2003.

[3] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In 10th ACM Conference on Computer and Communications Security, October 2003.

[4] D. Liu and P. Ning, Location-Based Pairwise Key Establishments for Static Sensor Networks, Proc. 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 72-82, 2003.

[5] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. Technical Report, Syracuse University, July 2003.

[6] R. Blom. An optimal class of symmetric key generation systems. Advances in Cryptology: Proceedings of EUROCRYPT 84, Lecture Notes in Computer Science, Springer-Verlag, 209:335-338, 1985.

[7] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A pairwise key predistrubution scheme for wireless sensor networks. In Proceedings of the 10th ACM Conference on Computer and Communications Security. October 2003.

[8] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120-126, 1978.

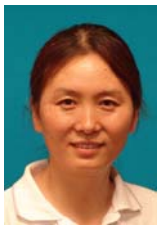
[9] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. Inform. Theory, IT-22:644-654, November 1976.

[10] Erdös and Rényi. On random graphs I. Publ Math. Debrecen, 6:290-297, 1959.

[11] R. Merkle. Secure communication over insecure channels. Communications of the ACM. 21(4):294-299, 1978.

[12] F. An, X. Cheng, J. M. Rivera, J. Li, and Z. Cheng. PKM: A Pairwise Key Management Scheme for Wireless Sensor Networks. ICCNMC, 2005.

[13] C. Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE International Workshop on Sensor Networks Protocols and Applications, May 2003.



Wang Huanzhao female, received the B.S. and M.S. degrees in Computer Architecture from Xi'an Jiaotong University in 1984 and 1989. She is an associate professor of Xi'an Jiaotong University. Her research interests include network security, wireless sensor networks.

Luo Dongwei, male, born in 1982. He received his B.S degree in Computer Science from Xi'an Jiaotong University, in 2004. Since then, he has been a M.S degree candidate of the same major. His current research interests include wireless sensor networks and network security.