Wireless Sensor Network, 2012, 4, 197-201
http://dx.doi.org/10.4236/wsn.2012.48029 Published Online August 2012 (http://www.SciRP.org/journal/wsn)

A Hybrid Key Management Scheme Based on Clustered Wireless Sensor Networks

Pengcheng Zhao, Yong Xu, Min Nan
Department of Mathematics and Computer Science, Anhui Normal University, Wuhu, China
Email: zpcah@163.com

Received May 17, 2012; revised June 25, 2012; accepted July 2, 2012

ABSTRACT

According to the weakness of session key construction based on node's own location, we propose a hybrid key management scheme which based on clustered wireless sensor networks. The use of hierarchical thinking, reducing the amount of key storage and computing, while supporting network topology, dynamic key management for which aims to prevent leakage. Through analyzing, it shows that the scheme have certain advantages in key connectivity, security, communication and energy consumption.

Keywords: Clustered Wireless Sensor Networks; Key Management; Network Security

1. Introduction

Wireless sensors networks (WSN) are widely used in military and national defense, medical care, environmental monitoring, traffic management and many other areas. People at any time, place and environment can access to a large number of detailed, reliable information. With the cost of sensor node's reduction and the availability of network is enhanced, WSN has a great prospect [1-3]. Because of its general configuration in regional of the absence or enemy territory, security problem will become a difficulty which WSN is most concerned, and key management is one of the most challenging issues in WSN security research, key management has therefore become the hot topics in WSN.

At present, according to the characteristics of the network structure, WSN can be divided into hierarchical key management model and distributed key management model. Node in distributed key management [4] complete communications and key update through key's pre-distribution to consult with each other, has the good distributed characteristic. However the node in hierarchical key management [5] will be divided into certain clusters, seeking for a node that has the ability to be the cluster head in each cluster. The key allocation and update of the ordinary node are all depending upon the cluster head to complete. Such plan has high request to the cluster head whose injury will serious influence entire network's security; according to the node whether needs to be update after deployment. WSN management can be divided into static key management [4] and dynamic keys management [6]; According to the method of node's distribution, it can be divided into determine key management scheme and random key management scheme. Determine key management is the earliest scheme who makes sensor nodes share the same key, one node captured the entire network will be compromised. Later, LAI and his companions propose an idea made each pair of nodes in the network share a pair of keys. Because the network requires $N(N-1)/2$ key storage, it does not apply to large-scare wireless sensor networks. Random key management includes E-G scheme [4], q-Composite random key scheme [7] and random key to the model. Before deployment sensor nodes select a certain number of key randomly from the pre-generated key pool, after nodes' deployment into designated area, communication between nodes in the key focus of their search for common key. These schemes have small amount of calculation and strong network expansion. But because it is the probabilistic model, in order to enhance the probability of security communication we need to save more keys. Once the node is compromised, the adversary will get a lot of key information.

Based on the above key management features of the scheme, this paper proposes a hybrid key management scheme base on clustered wireless sensor networks makes the improvement to the literature [8] thought on the basis of key pre-allocated.

The structure of this paper is as follows. Section 2 describes our detail hybrid key management scheme. The performance results will be evaluated in Section 3. Section 4 concludes the paper.

2. A Hybrid Key Management Scheme Based on Clusted Wireless Networks

Large-scale wireless sensor networks generally using the hierarchical structure, and making the network divided into clusters. Each cluster has a cluster head and multiple cluster members; the lower cluster is the member of high level, and making the top cluster head nodes communicating with the base station. This resulted in clustered wireless sensor networks, as shown in **Figure 1**. This scheme dividing the network into multiple clusters consisting of all connected regions [9]. Nodes within the same area most likely to become members of the same cluster, the closer the clusters head are away from the base station are most likely to elect to become the first top-level cluster.

2.1. Basic Idea

Cluster head in clustered wireless sensor network has a higher ability of information processing and storage capacity than normal nodes, which is responsible for node clustering. Collecting and processing information from the same cluster node and send it to the base station. It shows that the cluster head's key storage and connectivity requirements can be very high. We build a d-dimensional key tree between cluster head and base station as shown in **Figure 2**, using shared function **PK** (r) = **E**(K_M, R) (where R is a random member generated by the base station while K_M is the pre-loaded master key) to generate front-end session key. Cluster members generate their own key and adjacent key pair based on the information of their geographic location and pre-loaded master key. After key generation, the master key automatically removed form memory. On the one hand, the ordinary members of the cluster doesn't know the front communication session key, it can't access to the communication information of the front-end clusters while the front-end using shared function to generate tree structure session key, from doing this cluster head can have a relatively small amount of storage. On the other hand, ordinary nodes in the completion of loading master keys to generate the key pair will be automatically deleted, in order to avoid a cluster node captured the entire security compromised security risks.

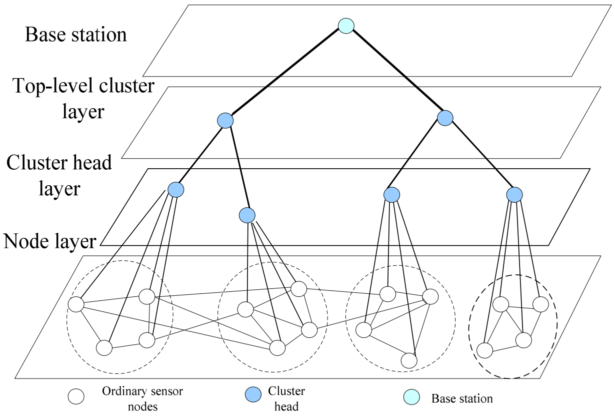

Figure 1. Two-dimensional index space of OpenCL execution model.

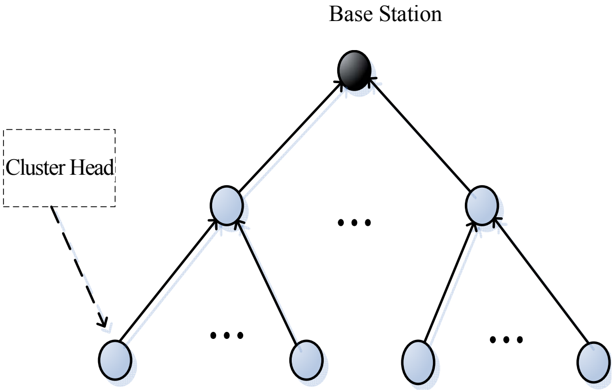

Figure 2. Key tree.

Bla*β* [10] with his companion proposed a key management mechanisms based on this assumption: Each node in the network can safely communicate with other nodes. In fact, for clustered sensor networks, nodes only need to communicate with neighboring nodes and cluster head securely, but not with any node.

2.2. Key Pre-Distribution Phase

Before the deployment, each node acts according to the region disposition, loading main key K_M in advance and randomly generating unique node *ID*. And each cluster head will also store a private key, session key **PK**(r) is initialization equal to K_M.

2.3. Key Establishment Phase

Clustered sensor network key establishment can be built by choosing a topology algorithm in WSN (such as TEEN, LEACH, etc.). Key establishment is divided into two types: One is to build a key tree between cluster head and base station, the other one is to establish communication key between members of the same cluster.

1) A key tree between cluster head and base station

Session key establishment between nodes is suitable for d-degree tree. To reduce the key storage and ensure access control of forward and backward while meeting key independence requirement, we let the members of the key tree have a private key K_i stored, base station and cluster head sharing one function **PK**(r) = **E**(K_M, R), base station let random number R encrypted with each node private key K_i (that is R_{k_i}) then sending to each cluster head. According to pre-load main key K_M generates a session key:

$$\mathbf{PK}(r)=\mathbf{E}(K_M,R) \tag{1}$$

2) Communication key between members of the same cluster

Based on the original proposal [8], the node indicated own positional information with S. According to pre-load main key K_M, The node generates a unique key and adjacent key pair based on location. Such as node u, based on its location and the local ID will have a unique key:

$$K_u=F_{K_M}(ID_u,S_u) \tag{2}$$

ID_u is the local identifier of node u, S_u shows location information, K_M is the main key, each node communicates with its hop neighbors in order to establish neighbors key pair. In order to communicate with neighbor nodes, such as nodes u and v, a message need to be broadcasted:

$$u\rightarrow *:, S_u, MAC_{K_M}(ID_u,S_u),$$

for authentication. When u and v found each other, using the main key K_M according to Equation (3) can direct access to session key. Two nodes are aware of K_M, and can communicate without any key exchange to agree on shared keys. Sharing key establishment of two adjacent nodes:

$$K_{u,v}=F_{K_M}(ID_u,S_u,ID_v,S_v) \tag{3}$$

when node obtains the key, the key establishment process is complete, simultaneously remove the primary key K_M permanently. Node store K_M only in the establish phase. Use an efficient one-way hash function to calculate key. In some scenarios, the anchor nodes deployed will be very intensive, time is short so that attackers cannot capture the nodes in the bootstrap. Therefore, the attacker will not able to get the primary key.

2.4. Key Maintenance Phase

The energy of the WSN node is limited or revolution occurred because of nodes capture, making the topology of WSN always changing. The key maintenance stage must process situations of nodes increasing, leaving, and revolting and so on.

1) A member increase in cluster

Two neighbor nodes, node u with newly joins node v, this time u already cleaned main key K_M. The node v in the initial vectoring phase, broadcasting message to announce its own locate mark and position. When node u receives this news, considering whether the new joined node is next to it, use Equation (4) to confirm.

$$|S_u-S_v|\le r \tag{4}$$

The r is the correspondence radius, if the condition doesn't satisfy with Equation (4), directly discarding receiving news otherwise u reply node v with its own information. Because node v knew K_M and local marking as well as two node's positional information, can directly obtain sharing session key with neighbor node u (Equation (3)). Finally, node v encrypt sharing key using the key of node u K_u then sent it back to node u to establish neighbor session key. The handshake message as follows:

$$v\rightarrow *:ID_u,S_v$$
$$u\rightarrow v:ID_v,S_u$$
$$v\rightarrow u:\left\{K_{u,v}\right\}_{K_u}$$

2) Leave and betrayal in cluster

For cluster members, after the key establishment, because sharing session is unique while K_M is deleted, the betraying of node will only have the affect with associated connections, other connections in WSN is secure. Base station will send the information of mutiny node encrypted with session key **PK**(r) to each cluster head. The cluster head who receives the information will forward it to the member of the same cluster, members of the cluster will check whether have sharing key with the mutiny node, if there are, delete the connection.

3) Exchange of the cluster head

Cluster head requires more energy than ordinary nodes, taking the extension of network's lifetime into consideration, the cluster head need to rotation. If cluster head is replaced, the corresponding keys will also update at the same time. After the authentication of new members, base station will update session key **PK**(r) to **PK**(r + 1) (*i.e.*, **PK**(r + 1) = **E**(**PK**(r), R)) and unicast it to new members, distributing all the keys and sharing function **E**(**PK**, R) from leaf node to root node, the base station send **PK**(r + 1) which is encrypted by **PK**(r) to other member of the key tree through multiple broadcast in order to achieve forward access control.

On the contrary, the leave of the cluster head will make base station use private key of the node which is left over to encrypt the random member R which is generated by base station sending to each cluster head through multiple broadcast, and according to the sharing function **PK**(r + 1) = **E**(**PK**(r), R), nodes obtain the new session key **PK**(r + 1) to complete the update. Though know the function **E**(**K**(r), R) but can't get R, leaving node can't get the session key, thus ensuring backward access control.

3. Comparison of Safety and Performance Analysis

3.1. Safety Analysis

1) Performance against node capture

This scheme based on the follow assumption: Base station is safe, cluster head has not been captured by the enemy in the initial deployment network. N is the number of network nodes, n_c is the captured number, m is the key number contains in each key ring, is the size of key pool. For the E-G mode [4], n_c nodes mutiny, enemy can attack

$$1-\left(1-\frac{m}{n}\right)^{n_c}$$

percents of the link. For q-composite mode [7], enemy can attack

$$\sum_{i=q}^{m}\left(1-\left(1-\frac{m}{|n|}\right)^{n_c}\right)^{i}\frac{p(i)}{p}$$

percents of the link. The proposed scheme, primary key is automatically deleted after key establishment phase; the capture of the same cluster can only get the captured node's unique key and its adjacent session key. This kind of nodes' anti-captured ability is strong which doesn't need to make the discussion here. But regarding the top level key tree built by the cluster heads, assuming an average degree of each node is d, the over all situation link number is l, in T time one node's mutiny can make enemy attack d/l percents of the link, through analyzing it is approximately to $2n_c/N$. The anti-attack performance comparison of the three schemes is shown in **Figure 3**:

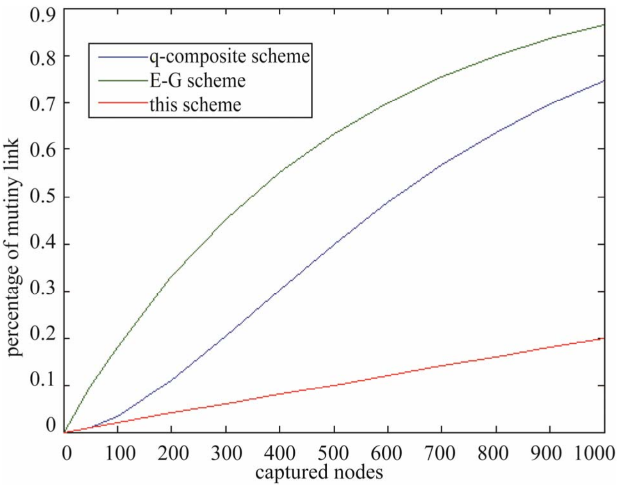

Figure 3. Simulation graph of anti-capture ability.

3.2. Network Performance Analysis

1) Key connectivity

A key management scheme base on hybrid clustered wireless sensor networks is the definite key allocation scheme therefore the network connection probability is 1. **Table 1** shows the comparison of key connectivity as follow: (see **Table 1**).

2) Communication and computation complexity

C_{GM} is the key storage of members; C_{Gc} is the key storage of base station; d is the degree of the tree; N' is the total number of nodes in the bottom of the key tree. It can be seen that although the calculation of this scheme is a little complexity, the communication path and key storage are relatively small and energy consumption of hash function and pseudo-random function is little. **Table 2** shows the comparison of communication and computational complexity as follow: (see **Table 2**).

4. Conclusion and Future Work

The proposal hybrid key management scheme is suitable for clustered wireless sensor networks, can build a unique session key between cluster heads, communication energy consumption is small, anti-attack ability is strong, easy to maintain. Using trust model to evaluate node's reliability to find the betray node will be the future research directions.

Table 1. Comparison of key connectivity.

Schemes and protocols	Key connectivity	Comparison with E-G scheme
E-G scheme	$1-\frac{((n-m)!)^2}{(n-2m)!n!}$	—
q-Composite scheme	$1-(P(0)+P(1)+\cdots+P(q-1))$	↓
This scheme	1	↑

m is the key number contains in key ring, is the size of key pool, $P(i)=\frac{C_i^m C_{2(n-i)}^{m-i} C_{n-i}^{2(n-i)}}{\left(C_n^m\right)^2}$, ↓ indicates decrease while ↑ indicates increase.

Table 2. Comparison of communication and computaional complexity.

Schemes and protocols	Computational complexity	Communication path hops	Numbers of key stored
E-G scheme	MAC_S+Enc	>1	Hundreds
q-Composite scheme	MAC_S+Enc	>1	Hundreds
Original scheme	MAC_S+Enc + hash functional calculation	1	Adjacent nodes number + 1
This scheme	MAC_S+Enc + hash functional calculation + pseudo-random functional calculation	1	$C_{GM}\le\log_d N'+1$ $C_{Gc}=1+\frac{d\left(1-d^{\log_d N'-1}\right)}{1-d}+N'$

5. Acknowledgements

This work was supported by a grant from National Science Foundation of Anhui Province (11040606M137). We would like to thank the anonymous reviewers for insightful feedbacks that improve the quality of this paper.

REFERENCES

[1] H.-X. Jing and X.-D. Hu, "A Location Based Key Management Scheme for Wireless Networks," *Communication Technology*, Vol. 11, No. 40, 2007, pp. 311-313.

[2] L. M. Yu, J. Z. Li, Y. Chen, *et al.*, "Wireless Sensor Networks," Tsinghua University Press, Beijing, 2005.

[3] X. W. Zhou and B. P. Qin, "Scalable Session Key Construction Protocol for Wireless Sensor Networks. Wireless Sensor Networks and Security," National Defense Industry Press, Beijing, 2007.

[4] L. Eschenauer and V. D. Gligor, "A Key Management Scheme for Distributed Sensor Networks," *The* 9*th ACM CCS*, Washington DC, 2002, pp. 41-47.

[5] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanism for Large-Scale Distributed Sensor Networks," *Procceedings of the* 10*th ACM Conference on Computer and Communications Security*, New York, 14 June 2004, pp. 62-72.

[6] M. Eltoweissy, M. Moharrum and R. Mukkamala, "Dynamic Key Management in Sensor Networks," *IEEE Communications Magazine*, Vol. 44, No. 4, 2006, pp. 122-130. doi:10.1109/MCOM.2006.1632659

[7] H. Chan, A. Perrig and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *Procceedings of the* 2003 *IEEE Symposium on Security and Privacy*, IEEE Computer Society, Washington, 2003, pp. 197-213.

[8] H.-X. Jing and X.-D. Hu, "A Location Based Key Management Scheme for Wireless Networks," *Communication Technology*, Vol. 11, No. 40, 2007, pp. 311-313.

[9] B. Shen, S. Y. Zhang and Y. P. Zhong, "Hierarchical Routing Protocol for Wireless Sensor Networks," *Journal of Software*, Vol. 17, No. 7, 2006, pp. 1588-1600. doi:10.1360/jos171588

[10] E.-O. Bla*ß* and M. Zitterbart, "An Efficient Key Establishment Scheme for Secure Aggregating Sensor Networks," *Proceedings of the* 2006 *ACM Symposium on Information, Computer and Communications Security*, Taipei, 2006, pp. 303-310.