Strategy and Simulation of Trust Cluster Based Key Management Protocol for Ad hoc Networks

Li Xu
Key Lab of Network security and Cryptology
Fujian Normal University
Fuzhou, China

Xiaoding Wang, Jinbo Shen
Key Lab of Network security and Cryptology
Fujian Normal University
Fuzhou, China

Abstract---Secure and efficient communication among a set of mobile node is one of the most important research subjects in ad hoc wireless networks. Due to the resource scarcity in ad hoc networks, traditional key management protocol cannot be effectively applied to such decentralized networks. After study different strategies, in this paper the trust evaluation based clustering technique is employed to propose a hybrid decentralized key management protocol using the NS^3 (New Secret Sharing Scheme) algorithm for ad hoc networks, covering the aspects of key deployment, key refreshment and key establishment. Both theoretical analysis and simulations indicate that the proposed protocol has less complexity and stronger security than some current strategies.

Key words—ad hoc network, security, key management, clustering, secret sharing.

I. INTRODUCTION

Wireless ad hoc networks [1] have drawn significant attentions recently due to its wide applications in different areas. However, ad hoc networks are subject to various kinds of attacks. Such as wireless communication links can be eavesdropped without noticeable cost and communication protocols on all layers are vulnerable to specific attacks.

On the other hand, asymmetric cryptographic algorithms are not suitable for providing security on wireless ad hoc networks due to the limited computation, power, and resource storage resources space on wireless nodes. Therefore, symmetric key cryptographic algorithms are employed to support security in wireless ad hoc networks [2] [3]. However, the design of any service in ad hoc networks do not rely on any centralized entities, because such entities would be attacked easily, and their reach ability would not be guaranteed at all times for all participants of the network. Therefore, it is not possible to implement a centralized, trusted entity for managing public keys of the participants in local area networks or the Internet. The network needs distributed solution must be found. There are many key establishment protocols in the literature based on symmetric key cryptography for wireless ad hoc networks [3，4].

Zhou and Hass [5] proposes a secure key management scheme by employing (t, n) threshold cryptography. Thesystem can tolerate t-1 compromised servers securely and efficiently in case that the servers are scattered in the whole area. A share refreshing scheme is proposed to counter mobile adversaries. However, efficient and secure distributions of secret share are not addressed. [6] Proposes a security concept based on a distributed certification facility and the approach of which divides the network into clusters with one special head node each. These cluster head nodes execute administrative functions and hold shares of a network key used for certification. Instead of a registration authority, arbitrary nodes with respective warranty certificates may warrant for a new node's identity. However, this method will result in too many communications cost. Our protocol mainly derives from it, but better than it.

In our protocol, the clustering scheme derives from [7] and our former paper [9][10], both of which proposes a cluster-based trust evaluation scheme, in which neighboring nodes form a cluster and select one node as a cluster head. The head issues a trust value certificate that can be referred to by its non-neighbor node. In this way, an evaluation of an unfamiliar node's trust can be done very efficiently and precisely.

The rest of this paper is organized as follows. In section II, we present our key management protocol. Section III we discuss reaction of our solution to topology changing. Then, we present an analysis of proposed protocol in section IV and summarize the results in section V.

II. A CLUSTER BASED PROTOCOL FOR SECURING AD HOC NETWORKS

Based on the analysis in section 2 we know seldom of the existing key management schemes is suitable for ad hoc networks. Although these are some ones, they are still too inefficient, not functional on an arbitrary or unknown network topology, or not tolerant to a changing network topology or link failures.

A. General Method

In our protocol, the first step is a cluster creating method that divides the entire set of nodes into subgroups based on the geometric locations of nodes; a cluster is first formed

978-1-4244-3521-0/09/$25.00 ©2009 IEEE

based on the trust values of the neighbor nodes. Then, a cluster head (CH) that has the highest trust value in the cluster issues a trust value certificate for cluster member nodes. Once the clusters are constructed, the set of dominator of leaders, and the key is generated as a contribution from all the leaders.

Every node in the network is given a system public key and system private key. Besides the system key, each node also needs a cluster key. This cluster key is unique to every cluster and a single cluster key is shared by all the nodes of an individual cluster. This cluster key is generated by the cluster head and distributed to the entire cluster member. In addition, this key is encrypted with the system public key and broadcast by the head. Each cluster head also has a unique pair of public/private key called head key. Besides, each node needs to maintain a table consisting of [cluster ids, nodes id, node trust value, cluster head's pub key, create time validation, signature (cluster ids, nodes id, node trust value, create time)]. When a new node joins the network, first it has to find a cluster, if it receives CH beacons, the key refreshment run inter cluster, if a node does not receive any CH beacons, it own cluster and act as a CH of the cluster where it is in, then run the non-interactive protocol for member expansion in a secret sharing scheme will be run. Which is a New Secret Sharing Scheme (NS^3) derives from Refs [8]

B. Clustering in Ad Hoc Networks

In our protocol, firstly, a cluster is first formed based on the trust values of the neighbor nodes. Then, a cluster head that has the highest trust value in the cluster issues a trust value certificate for cluster member nodes. Cluster forming is carried out as follows. An ad hoc node evaluates its neighbor nodes' of neighbor nodes; each node chooses one node that has the highest value as its trust guarantor. Then, the chosen node becomes the cluster head and the chooser becomes a member of the cluster, a node of the second highest trust value is chosen, in this way, a cluster is formed the cluster head has the highest trust value among the cluster members. Figure 1 shows an evaluated trust value and chosen cluster head. After forming a cluster the cluster head plays the role of trust guarantor. The cluster head evaluates and guarantees the trust of the cluster member nodes.

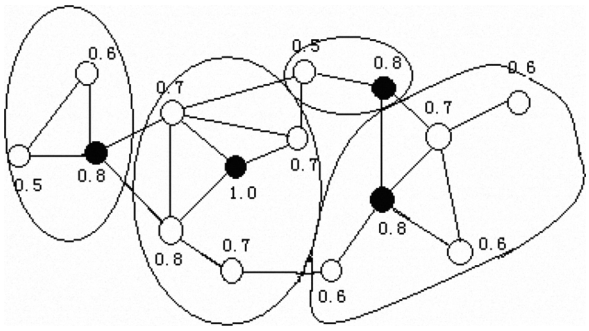


Figure 1 clustering scheme

When a member node requests it, cluster head issues the trust value certificate that contains the node's trust value. The member node uses the trust value certificate to show its trustworthiness to communicate with other. Detail of the trust evaluation metric can be seen in our former paper [9].

C. Intra Clusters Services

A single CA node could be a security bottleneck if it is not well protected, multiple replica of CA are fault tolerant, but the network is as vulnerable to be broken into single CA or even worse since breaking one CA means breaking all CAs, meanwhile it could be much easier for attackers to locate a target. In this paper, we use this NS^3 scheme among the cluster heads. In a wireless ad hoc network environment, more communications will bring longer time and lower success rate to the generation of new shares, and more difficulty to the key management. In this paper, we introduce a new secret share generation protocol among the cluster heads. at the beginning, we do not need all cluster heads to join dispensing procedure, only t nodes were chosen to generate the new secret share s_{t+1}, and then all the cluster heads can hold the secret shares. Suppose ElGamal cryptography is used for secret communication. GF(q) is the given finite field, g is its generator, and (g, g^d) is the public key, where d is the secret key, M is the message for sending. Group secret key is s, group public key is g^s .P_i hold the secret share S_i. The Lagrange polynomial is f(x). Let the new member be P_{n+1}, whose ElGamal encryption secret key and public key are d_{n+1} and g^{dn+1} respectively.

The new secret sharing scheme (NS^3):

1、Select two random integers e_i and l_i, and encrypt $s_i w_i(n+1)$ by e_i $K_i^0 = s_i w_i(n+1) e_i$, broadcast K_i^0 and g^{l_i}

（t broadcasts with 2t data）。

2、$for(j=1; j<=t;)$

$for(i=1; i<=t;)$

$if(j \neq i)$

Compute $K_i^j = K_i^{j-1} g^{(s+d_{n+1})l_j}$

Else $K_i^j = K_i^{j-1}$

End for i

Broadcast $K_i^j \quad i=1,2,.....t$

End for j

$M_i = K_i^t$

(t broadcasts with t (t-1) data)

3、$for(j=1; j<=t;)$

$for(i=1; i<=t;)$

$if(j \neq i)$

Compute $W_i^j = M_i g^{(s+d_{n+1})l_j}$

Else $W_i^j = 0$

End for i

Broadcast $W_i^j \quad i=1,2,.....t$

978-1-4244-3521-0/09/$25.00 ©2009 IEEE

End for j

(t broadcasts with t (t-1) data)

4、 $for(i=1;i<=t;)$

Compute $W_i^e = \sum_{j=1}^{t} W_i^j$,then decrypt W_i^e and M_i to get

$$W_i = S_i W_i(n+1) g^{(s+d_{n+1})(\sum_{j=1}^{t} l_j - l_i)} \sum_{j=1, j\neq i}^{t} g^{(s+d_{n+1})l_j}$$

$$Q_i = S_i W_i(n+1) g^{(s+d_{n+1})(\sum_{j=1}^{t} l_j - l_i)}$$

Broadcast W_i, Q_i

End for i

Compute $A = \sum_{I=1}^{T} Q_i$

(t broadcasts with 2t data)

5、 $for(i=1;i<=t;)$

Compute and broadcasts $Ag^{(s+d_{n+1})l_i}$

End for i

Compute $B = \sum_{i=1}^{t} Ag^{(s+d_{n+1})l_i} - \sum_{i=1}^{t} W_j$

(t broadcasts with t data)

6 、 $P_1, P_2 ..... P_t$ cooperate to decrypt B ,and get

$$C = \sum_{i=1}^{t} S_i W_i(n+1) g^{d_{n+1}\sum_{j=1}^{t} l_j}$$

where t times broadcasts with t data and Totally 6t broadcasts with 2t (t+2) q Bit length data.

D. Inter Cluster

Inter cluster services are services offered by a cluster head to the members of his cluster. As we know, each cluster head represents a central authority for his members. These services will be the same as the ones offered by a PKI. Since the cluster head is a certification authority for his members and it is to supposed provide each one with a valid certificate signed with his secret key. And the public key of CH is published to allow any node can authenticate any other node in the same cluster using the corresponding cluster head public key.

III. REACTION OF OUR SOLUTION TO TOPOLOGY CHANGING

A. When A Node Joins The Network.

The join operation is carried out as follows. First, the join node broadcasts a hello message. Any cluster head that receives the message sends a respond message to the node. The respond message of the head contains the number nodes, the CH's trust value; second, after receiving the response message from the cluster head, the join node sends to the cluster head the join message consisting of (node id, CH id, previous CH id, trust value, Id cert, "join message") .

The trust value and Id cert are described in the following. This step is also called the log-on procedure. That means a new node can join a network by becoming a guest node first and a full member later. This idea partly derives from References [4].

In order to log on, the new node firstly needs the trust value from its neighboring node's evaluation toward him. Each of these trust value is signed by the neighbor to guarantee its authenticity, and also includes a period of validity.

Trust value: = [node id, node trust value, neighbor node id, validity (t), sign]

When CHs are being asked for certificate shares by a new node, they first have to make sure that the issuers of trust value are really authorized to vouch for a guest, then they must check the trust value weather it is above the treadhood, then the CHs send their shares of an identity certificate if all the certificates are valid. After the new node collected enough certificate shares, it can complete its identity certificate.

Id cert: =node id, pub key, validity (t), signs (CHs)

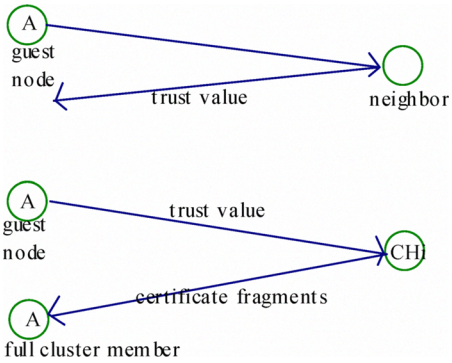


Fig.2. Authentication process

Now having its key signed, the new node is a full member. The CH sends the symmetric cluster key to the new node. Fig.2 illustrates the message exchange during a successful log-on.

If the joining node is not able to find any cluster head in a one-hop range, then the joining node has to construct the cluster with the neighbor node. The CHs run NS[3]. So the new CH can hold the secret share.

B. When A Node Leaves His Cluster

We assume that the removing of node u will not disconnect the network, if u is not a cluster head, it is in the cluster which cluster head is v, then v just applies member deletion to get new cluster key for the cluster. Assume node u is a cluster head. This avoids an expensive re-configuration of the cluster and possibly of the whole network. The CH can choose the node which had the highest trust value among the cluster member. Once a trust worthy successor is determined,

the old CH securely migrate its state to the successor and sends a signed broadcast message containing the new CH's identity. Nodes that do not receive this broadcast message will consider the CH beacons they receive after the change ad foreign. The new CH also holds the share of the network key. The CH also has to notify the members of the CHs about the CH delegation, which result from separating encrypted messages to each other CH. The old sharing of the network key will be unaffected. During the next refresh of the key shares, the new CH will be updated instead of the old one. However, if no CH successor can be found by the old CH, that means, this cluster will have no CH, then the members have to join neighboring clusters or form a new cluster after a new CH has been found.

IV. ANALYSIS

A. Security analysis

In [16] they already showed the key management protocols are secure, which guarantee that our hybrid key management protocol is secure. Therefore, in this section, we concentrate on the analysis of the communication complexity of our hybrid key management protocol, from the procedure of the new share distribution; one can see that all the results of each step is sent by the broadcasting, while all the data for keeping secret are managed by the generators. So the group key management is simple. Furthermore, among the cluster heads our protocol does not need the trusted center, the protocol only requires t(t is the threshold)participants cooperation and t times broadcasting to generate and only commits 6t broadcasts, it has been shown in[9], that the construction of clusters cost O(Δ) messages in which the Δ is the nodes' max degree, and notice that, in each cluster, since the cluster head can reach all its cluster members in 1-hop, the communication cost is also O(Δ), in the case of wireless ad hoc network, fewer communications lead to a higher probability of success distribution.

In an ad hoc network, it is possible that a node doesn't route a packet from the other nodes selfish nodes. In our model, a selfish node cannot have a high trust value because of the data delivery rate. By not providing packet for low trusted nodes, a network can encourage cooperation and reduce selfishness. Furthermore, between the cluster heads, security of the group key S is guaranteed by ElGamal cryptosystem, so every single member can't get S. When computing M_i, it actually performs encryption for S_i three times: its holder's encryption P_{n+1}'s encryption and group's encryption. In the process of synthesis to the new share, the computation of $S_i W_i(n+1)$ is nonlinear, so nobody can acquire any useful information of S_i. The result of every step is encrypted by group key, so P_{n+1} can't get S_i. At last, B, generated by the $P_1, P_2 \ldots\ldots P_t$, is the S_{n+1}'s encryption by P_{n+1}'s secret key, so $P_1, P_2 \ldots\ldots P_t$ can't get S_{n+1}. In sum, the NS^3 has a higher security.

B. Performance Analysis

1. Performance indicators

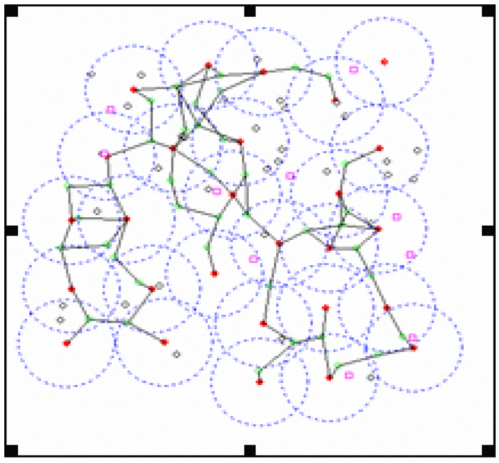
For the advantages measurement of key management performance of our scheme, we use nodes successful landing ratio and successful landing time as indicators. The successful landing ratio is defined as the count of successful landing nodes divided by the total number of the joining nodes. The successful landing time is defined as the hops which the node receives t certificate. According to the character of Ad Hoc Networks, we suppose that only a certain threshold value of node can send certificate 100%, but lower than the threshold value of the node transmits the certificate only by a certain probability. Comparison of the following three circumstances discussed:

(1) Based on the Trust Evaluation Clustering Algorithm, CH's trust value is greater than the threshold value, so node can request certification from CH.
(2) Based on Minimum ID Clustering, node can request certification from CH, but CH's trust value maybe be lower than the threshold value.
(3) Null Clustering Algorithm, node sends request to other all nodes, but there are many malicious nodes who will not transmit the request.

2. Simulation environment

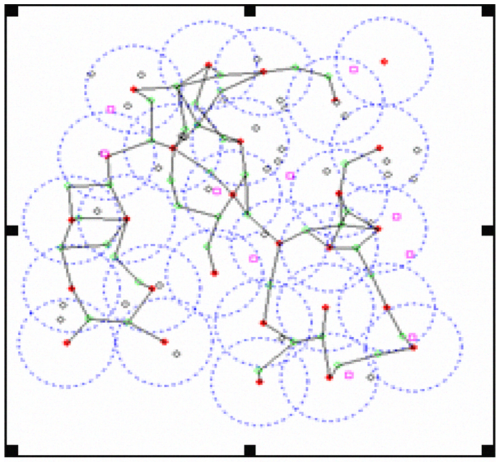
This paper uses VC++ 6.0 for simulation research. In this simulated environment, we don't consider the impact of the background noise, packet transmission errors and packet conflict on the clustering algorithm. Because simulation environment of the algorithms is all the same, it will not affect the accuracy of the results. And we suppose that the nodes transmit power (scope) are all the same.

There are N nodes randomly placed within the region of X * Y units, the movement direction of node is random, and the node speed is randomly between 0 and maxV. The number, transmission radius, speed, the number of the new node and the value of the threshold value t can be dynamically adjusted according to requirements. Now we randomly generate 100 nodes in the region of 300 * 300 units, choose maxV = 30 and the number of new nodes is 10.



(a) r = 40

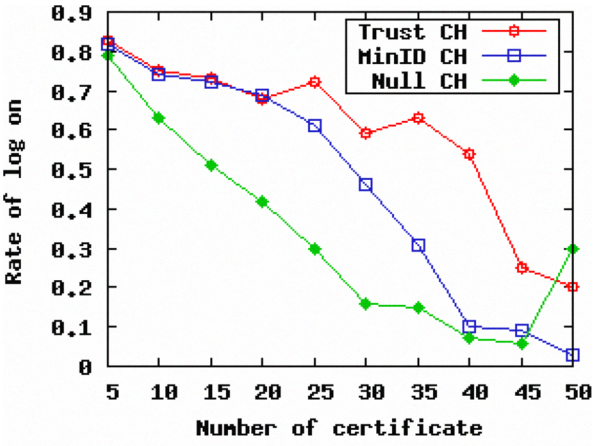
978-1-4244-3521-0/09/$25.00 ©2009 IEEE



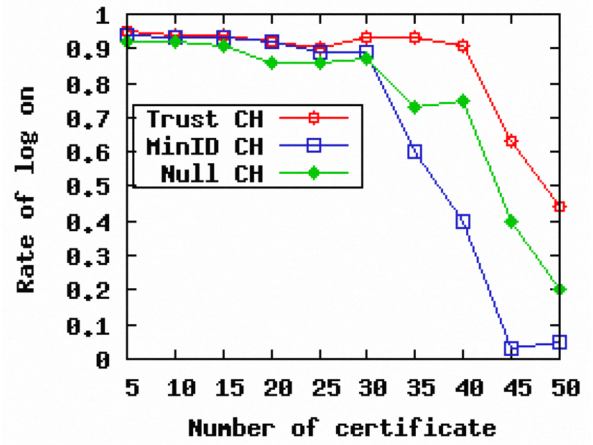
(b) r = 50

Fig.3 Clustering Scheme based on Trust Value

We analyze the successfully loading ratio and time along with the threshold value t change from 5 to 50 as the transmission radius r = 40, 50, the data results are achieved by the average of 10 group of 20 independence redundant.



(a) r = 40



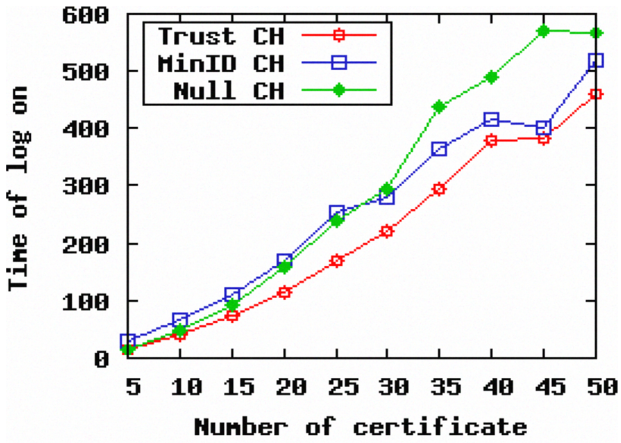
(b) r = 50

Fig.4 Rate of log on with different number of certificate

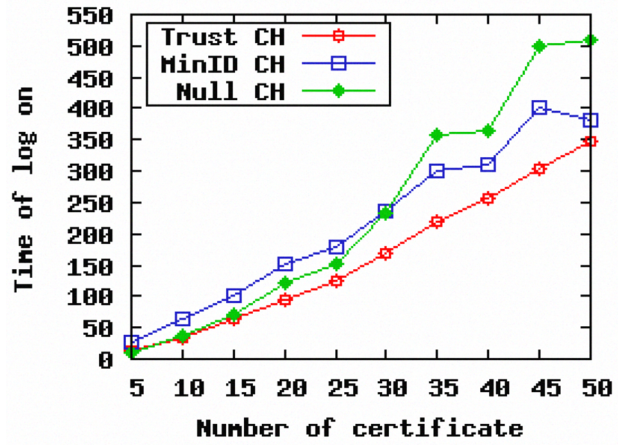
3. Result analysis

(1) The transmission radius is different，the network has different cluster structure. As shown in Fig.3, the example of the clustering based on trust value, when the radius r = 40 and r = 50.

(2) Supposes the successful loading needs the certificate number to take separately 5, 10, 15…… 50 altogether 10 groups. Fig.4 shows that how the successful loading rate varies with the number of certificate. Compared with the Minimum ID Clustering and Null Clustering Algorithm, Fig.5 shows that the successful loading rate of the clustering scheme based on trust value is better when radius r = 40. And when radius r = 50, the clustering scheme based on trust value has better performance also.



(a) r = 40



(b) r = 50

Fig.5 Time of log on with different number of certificate

(3) Supposes the successful loading needs the certificate number to take separately 5, 10, 15…… 50 altogether 10 groups. Fig.6 shows how the successful loading time varies with the number of certificate. As shown in fig.5, the curve of

our scheme is the lowest, because CH's trust value of our scheme is greater than the threshold value. And along with the certificate number increase, the successful loading time will also lengthen, but our scheme's rate of rise is obviously smaller than other two kinds of scheme.

Under the condition of the same certificate number, the transmission radius is influential to the network clustering structure. Fig.6 is the radius separately takes 30, 40, 50, the certificate number takes 30. Compared with the Minimum ID Clustering and Null Clustering Algorithm, the successful loading rate of our scheme is highest. Fig.7 shows how the successful loading time varies with the different transmission radius under the same conditions. And we can draw the conclusion that the successful time of our scheme is the minimum.

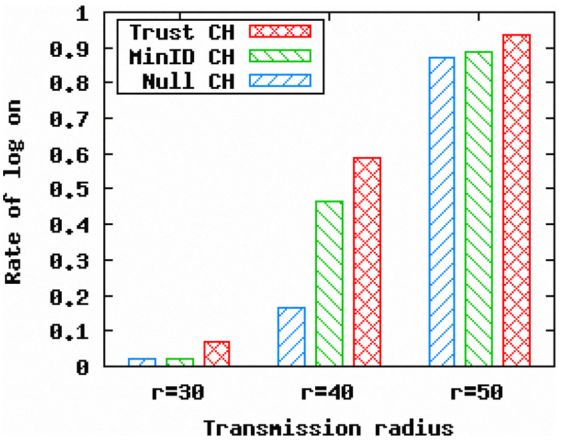


Fig.6 Rate of log on with different transmission radius

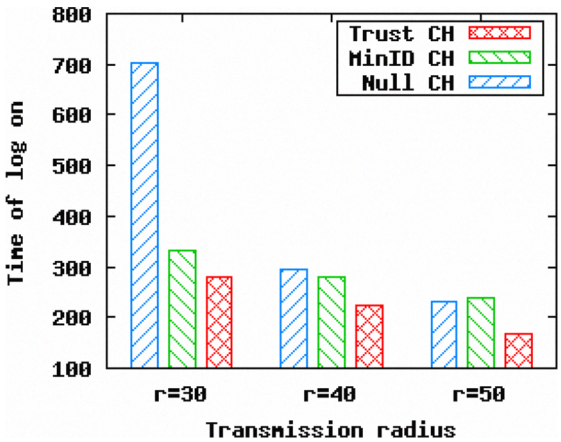


Fig.7 Time of log on with different transmission radius

V. CONCLUSIONS

In this paper, we introduced a clustered-based architecture for a distributed public key infrastructure that is highly applied to the characteristics of ad hoc networks. In order to adapt to the highly dynamic topology and varying link qualities in ad hoc networks, we consequently avoided any central instances that would form single points of attack and failure. Instead, the ad hoc network was divided into clusters. We proposed a new trust evaluation scheme in ad hoc networks. By doing this, we receive better efficiency and security. The cluster heads jointly perform the tasks of a certification authority. Our concept uses a proactive secret sharing scheme, which distributes the private network key to the cluster heads in the ad hoc network.

ACKNOWLEDGEMENTS

This work is supported by National Natural Science Foundation of China (60502047), Education Bureau of Fujian Province (JA07030), Natural Science Foundation of Fujian Province (2008J0014).

REFERENCE

[1]RAM R, JASON R. A brief overview of mobile ad hoc networks: challenges and directions. IEEE communications Magazine, May 2002, 40(5):20-22.

[2]A.Perring, R.Szewczy, J.D.Tygar, V.wen, and DE.Culler,"SPINS: security protocols for sensor networks," Wireless networks 8,521-534, 2002, Kluwer Academic Publications.

[3]B.Decleene,L.Dondeti,S.Griffin,T.Hardjono,D.Kiwior,J.Kurose,D.Towsley,S.Rasudevan, and C.Zhang." Secure group communications for wireless networks,"in proc.IEEE MILCOM01,oct.2001.

[4]Aldar C-F.Chan,"Distributed symmetric key management foe mobile ad hoc networks," IEEE INFOCOM 2004.

[5]L.Zhou and Z.J.Haas,"securing ad hoc networks,"IEEE Network,vol.13,no.6,pp.24-30,1999.

[6]M.Bechler,H.-J.Hof,D.Kraft,F.Puhlke,L.Wolf,"A cluster-based security architecture for ad hoc networks,"IEEE INFOCOM 2004.

[7]Seunghun Jin, Chanil park, Daeseon Choi, Kyoil chung,and Hyunsoo Yoon,"Cluster-based trust evaluation scheme in an ad hoc network,"EFRI journal, volume 27,Number 4,Auguest 2005.

[8]Dong P,Kuang xh,Lu XC,"A non-interactive protocol for member expansion in a secret sharing scheme,"Journal of software,2005,16(1):116-120.
http://www.jos.org.cn/1000-9825/16/116.htm.

[9] ZHANG Jing, XU Li, HUANG Rong-ning, "Trust Evaluation-Based Clustering Algorithm in an Ad hoc Network" . The proceeding of CTCIS2006. 2006.10

[10] Xu Li. Genetic algorithm simulated annealing based clustering in MANET, Advances in Natural Computation. Lecture Notes in Computer Science, 3610: 1121-1131, Springer Press. August 2005.

978-1-4244-3521-0/09/$25.00 ©2009 IEEE