Seventh International Conference on Computer and Information Technology

An Effective Trust Establishment Scheme for Authentication in Mobile Ad-Hoc Networks

Guojun Wang[1,4], Qiong Wang[1], Jiannong Cao[2], Minyi Guo[3,4]

[1.] *School of Information Science and Engineering, Central South University, Changsha, Hunan Province, 410083, China*
csgjwang@mail.csu.edu.cn, wangqiong1008@gmail.com

[2.] *Department of Computing, Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong*
csjcao@comp.polyu.edu.hk

[3.] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, China*
guo-my@cs.sjtu.edu.cn

[4.] *School of Computer Science and Engineering, University of Aizu, Aizu-Wakamatsu, Fukushima 965-8580, Japan*
{csgjwang, minyi}@u-aizu.ac.jp

Abstract

Distributed authentication has the property of high security compared with existing authentication schemes. However, its success ratio for authentication may be not high, especially in large-scale Mobile Ad-Hoc Networks (MANETs). In order to address this issue, we propose a hybrid authentication scheme which integrates the chained authentication with the distributed authentication. When a node can't find enough authentication nodes in its one-hop neighborhood to authenticate itself, it requests its neighboring nodes to find a certificate chain to do so through the chained authentication. Hence, our scheme overcomes the drawbacks in terms of success ratio for authentication. Theoretical analysis and simulation studies show that, compared with the chained authentication schemes, our scheme is more scalable and it can increase the success ratio for authentication, without sacrificing the security requirement.

Keywords: Authentication, Cryptography, Secret Sharing, Trust Transfer, Mobile Ad-Hoc Networks

1. Introduction

In recent years, there has been considerable interest in Mobile Ad-Hoc Networks (MANETs) with the development of wireless communication technology. Authentication is one of the most important and challenging issues in MANETs. The scarcity of computation and communication resources and the lack of secure network infrastructures present major challenges for deploying applications in such a network.

Many authentication schemes have been proposed in the literature based on features of MANETs [2][3][5][10][11], which usually employ cryptography and secret sharing to achieve security.

Traditional network authentication solutions usually need the support of a trusted third party or called a Certificate Authority (CA) [1]. A CA is assumed to be responsible for authenticating all the nodes in the network, such as Kerberos and X.509 scheme. However, the centralized server suffers from a single point of service denial and compromise.

As we know, the distributed authentication scheme improves security by composing otherwise untrustworthy individual nodes into a trustworthy aggregation of nodes. The authentication service remains available even if some of these nodes have been compromised. In the literature, researchers attempted to apply the distributed authentication scheme into MANETs. Zhou and Hass [2] proposed a partially distributed authentication scheme that utilizes (n, t) threshold scheme to distribute the key shares of the CA over a number of servers. The (n, t) threshold scheme allows any t servers out of n servers to recover the secret key of the system in a collaborative manner.

0-7695-2983-6/07 $25.00 © 2007 IEEE
DOI 10.1109/CIT.2007.55

The n nodes which have the key shares compose a CA, among which any t nodes form an effective set. Similarly, a mobile adversary has to capture at least t nodes in order to crack the secret key of the system and it needs to destroy (n-t+1) share holders in order to turn off the certification service. This scheme is robust against the mobile adversary by using secret division. Although this scheme possesses high security, the authentication service of distributed scheme is not always available in some cases. For example, t authentication nodes may not be available in sparse areas of the network, thus leading to the failure of authentication.

Kong et al [3] improved the aforementioned scheme by proposing a locally distributed authentication scheme. All the nodes in the network are allocated a partial encryption key and have the right to sign the system certificate. When a new node wants to join the network, it can find enough trustworthy nodes easily within its one-hop neighborhood. It is assumed that there are enough nodes in its one-hop neighborhood, and each neighbor has a partial key. This scheme efficiently improves the scalability of authentication and reduces the communication overhead among the neighboring nodes during the process of authentication. But the security is comparatively low, as a mobile adversary just needs to capture any t nodes to crack the system secret key. On the other hand, as the network becomes large, the number of authentication nodes in the network has to increase accordingly. It brings troubles in network maintenance and management, which restricts the scalability of the scheme.

Capkun et al [4] proposed a self-organized authentication system based on public key chain [6]. The idea of the public key chain is similar to PGP [7] in the sense that both of them form a trust chain by collecting the trust information. Each node in the network is its own authority and has capability to sign and verify the keys of other nodes. In this scheme, certificates are issued and stored by the nodes themselves, unlike in PGP, where the task is implemented by some online servers. Each node maintains a local certificate repository that contains a few certificates selected by the node according to an appropriate algorithm. However, as the capacity of the certificate repository is limited, the scheme can't ensure 100% success ratio for authentication. In order to increase the success ratio for authentication, each node has to store as many certificates as possible, which is not feasible in MANETs.

The authentication schemes in the above mentioned papers are just suitable to small or medium-scale MANETs which consist of tens or at most hundreds of mobile nodes in a small area. The distributed schemes can't ensure high service availability, and the chained authentication's randomicity makes it not secure enough. In fact, there is still very little research on security in large-scale MANETs.

In this paper, we propose a hybrid authentication scheme in large-scale MANETs. The role of the CA is taken by those network nodes with strong computation and communication capabilities. The nodes with general capabilities are called normal nodes. The proposed scheme can take advantage of high security of the distributed authentication schemes and effectively hides the mobility of mobile nodes. On the other hand, the proposed scheme can achieve high success ratio for authentication even in sparse areas by utilizing the flexibility of the chained authentication.

The rest of this paper is organized as follows. In Section 2, a hybrid authentication scheme is presented. We give theoretical analysis and simulation studies compared with existing schemes in Section 3. Finally, this paper is concluded in Section 4.

2. Hybrid authentication scheme

2.1. Basic Assumptions

We assume that there exist some nodes with strong computation and communication capabilities in the network. Each node v_i in the network has an unique identifier ID_i and is equipped with a pair of RSA public and secret keys $\{\underline{PK_i} / \underline{SK_i}\}$. All the nodes in the network have some kind of intrusion detection system which can efficiently detect the misbehaviors of their neighboring nodes. Each node in the network knows the system public key SPK, and trusts the certificate signed by the system secret key SSK. We assume that a mobile adversary can capture at most t-1 nodes within a share refreshing period. A legal node in the network stores two kinds of certificates: the system certificate which is used to validate the node, and the certificate which is issued and stored by the node itself to build trust relationship with other nodes. If a node u trusts a node v in its neighborhood, node u signs a certificate to node v. This process repeats until a trusted network is formed among the whole network.

2.2. Initialization of the network

We adopt an RSA-based mechanism as the basis of our work. The pair of RSA public and secret keys of the CA in the system are denoted as SPK/SSK, where SPK is the system public key and SSK is the system secret key. SSK is used to sign certificates for all the nodes in the network. A certificate signed by SSK can

be verified by the system public key SPK. Shamir's threshold secret sharing scheme [5] is adapted to divide SSK into key shares. N nodes are chosen to act as authentication nodes by threshold secret sharing. Assume GF(p) is a Galois Field, and a_1, a_2, …a_{t-1} are chosen in GF(p) to form an t-1 polynomial:

$$f(x) = SSK + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1} \bmod N$$

Then the node's identifier substitutes x in this polynomial to obtain $y_i = f(v_i) \bmod N$ (i=1,2,…,n)。 According to the property of Galois Field and Lagrange formula, there exists:

$$f(x) = \sum_{i=1}^{t} y_i \prod_{j \neq i} (x - v_j)/(v_i - v_j) \bmod N$$

When x=0, we can get that

$$f(0) = SSK = \sum_{i=1}^{t} y_i \prod_{j \neq i} v_j /(v_j - v_i) \bmod N$$

Then we get appending partial secret [8]

$$k_i = y_i \prod_{j \neq i, j=1}^{t} v_j /(v_j - v_i) \bmod N$$

Each k_i is stored by the corresponding node v_i which we called as the authentication node. Any t members of the authentication set can recover the secret via Lagrange interpolation. After the network initialization phase, the dealer which has disseminated partial secret destroys the secret information.

Each node creates the public key and the corresponding secret key by itself, and signs the certificates that it trusts. If a node u trusts a node v, and believes that a given public key PK_v belongs to node v, then u issues a public-key certificate in the form of (v, PK_v, T_{issue}, T_{expire})$_{SK}$, in which PK_v is bound to v by the signature of u. Certificates are issued with a limited valid time T_{expire}, and each certificate contains its issuing and expiration timestamps. At the beginning, each node's certificate repository just consists of the certificate which it issued to other nodes and the certificates that other nodes issued to it. The certificate exchange mechanism is adapted to speed up the trust building process in the network. A node u broadcasts the IDs of the certificates stored in its repository to its neighboring nodes. When a neighboring node receives the IDs, it sends back the IDs of the certificates stored in its repository to node u. Node u compares the IDs of two sets of certificates and sends back the certificates, which it has but the neighboring node doesn't have, to the corresponding neighboring node. This action is also done in the certificate renewal process (see below). When a node's certificate repository can't store any more certificates, the node deletes the older certificates according to their arrival time. Similar to the self-organized scheme [4], each node has two kinds of repository: updated repository and non-updated repository. The certificates in the updated repository should be renewed periodically. The certificates in the non-updated repository just need to be renewed when the corresponding nodes can't find a trust chain by merging the updated repository.

2.3. Authentication of the new nodes

When a new node w wants to join the network, it broadcasts a query request message to its one-hop neighbors for finding authentication nodes. If there exist t authentication nodes which trust the node within its one-hop neighborhood, a valid system certificate can be generated with Lagrange interpolation. However, it is possible that a new node fails to find t authentication nodes in its one-hop neighborhood, especially when it lies in a sparse network. This is the main reason why the existing partially distributed authentication scheme doesn't have high success ratio for authentication.

If the node w can't find t authentication nodes in its one-hop neighborhood to recover the system secret key SSK, then it tries to find enough paths to some authentication nodes beyond its one-hop neighborhood through trust transfer. The proposed hybrid authentication algorithm is shown in Fig.1.

```
Hybrid_ Authentication_ Algorithm( )
{
        initialize nodes in the network;
        new node w broadcasts authentication query to neighboring nodes;
        IF      node w receives t or more authentication replies   THEN
                w generates system certificate and joins the network;
        ELSE
                node w broadcasts proxy finding query to neighboring nodes;
                neighboring nodes search authentication node for node w;
        IF      node w gets t authentication replies    THEN
                w informs neighboring nodes to stop finding;
                w generates system certificate and join the network;
        ELSE
                 authentication fails;
}
```

Fig. 1 The hybrid authentication algorithm

New node w requests neighboring nodes randomly to find authentication nodes for it. The problem of finding enough authentication nodes is then delegated to some neighboring nodes, which are called the proxy nodes in the following. A proxy node accepts the request if it trusts the node. If a node, e.g. u, accepts the request, then it tries to find a certificate chain from itself to a certain authentication node.

The certificate chain has the following features:

(1) The first certificate on this path can be verified by node u.

(2) The last certificate binds the public key of the destination node, e.g. authentication node *v* in Fig 2.
(3) Each certificate on the path, except for the first certificate, can be verified by the public key bound in the prior certificate.

The finding process of trust chain between the two nodes is shown in Fig. 2.

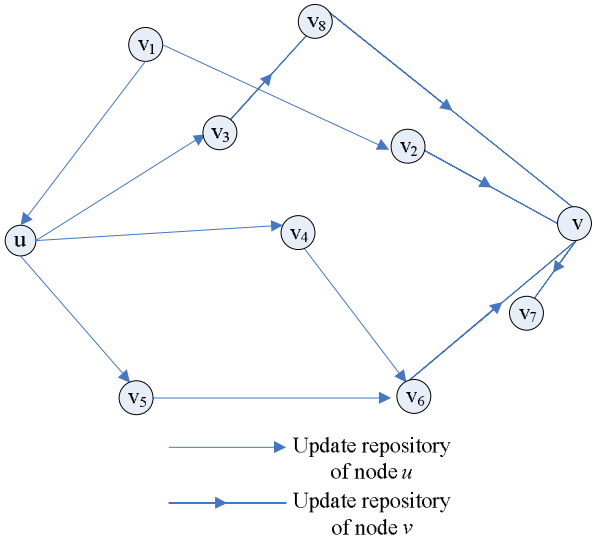

Fig. 2 Process of establishing trust chain

The certificates on the path are then used by *u* to authenticate *v*. If node *u* finds an authentication node through the above mentioned trust transfer process, it can establish a secure channel from itself to the authentication node. Node *u* can send the partial key signed certificate directly to new node *w*, or can just send the public key of authentication node *v* to node *w*. If node *u* finds that it can't find a trust chain to any authentication node, it also sends a message to inform node *w*. In this way, the authentication time can be reduced. After getting partial key signed certificate, new node *w* first validates the signature with verifiable secret sharing scheme (VSS) [9]. If the signature is valid, *w* reserves the certificate, and waits for the next partial signed certificate. When new node *w* gets *t* partial key signed certificates, it merges them to recover SSK, and joins the network successfully. After that, new node *w* informs neighboring nodes to stop finding authentication nodes. The CEF protocol [8] is also used to prevent the exposure of partial key in the certificate sign process.

2.4. Certificate renewal

Secret sharing alone can't ensure security because it can't defend against mobile adversary which compromises one authentication node for a limited time and then moves to the next node to do the same thing. Over time, a mobile adversary can compromise enough authentication nodes and then recover the SSK. Share refreshing is adapted to enhance security. Because new shares cannot be combined with old ones to recover the secret, a mobile adversary must compromise enough authentication nodes within the share refreshing period. This ensures security even in a more malicious environment.

Each certificate of a node is bound with a valid time period. A node renews its certificate before it expires. Besides, the certificate also needs to be renewed when the corresponding node's secret key is changed. The certificates in the network are renewed by the corresponding issuing node. Every node reserves its certificate issuing history. If a certificate will expire in the near future and the issuer believes that the node-key bound in the certificate is still valid, the issuer issues a new edition of the certificate which bound a new valid time period and the same node-key relation.

The renewal process of system certificate is similar to the authentication process, both of which need to get at least *t* partial key signed certificates and then merge the partial signed certificates to an valid system certificate.

2.5. Certificate revocation

There are two kinds of certificate revocation mechanisms: explicit revocation and implicit revocation. Explicit revocation means that the node-key relationship should be released before the bound valid time expires due to some special reasons, for example, the issuer finds that the key bound in the certificate is leaked. Then the issuing node sends an explicit revocation notification to which it has issued this certificate. Implicit revocation means that the valid time of the certificate expires, but the issuing node doesn't issue a new one. The issuing node usually renews the corresponding certificate before it expires, unless some misbehaviors of related nodes are detected

3. Theoretical analysis and simulation studies

In this section, we evaluate the performance of our proposed scheme from different aspects including security and success ratio for authentication. We also compare the performance of our proposed scheme with existing distributed authentication schemes.

3.1. Security analysis

Our scheme utilizes the CEF protocol [8] to achieve privacy in the process of secret merging. The real sign function is hidden by exponential switch as the information transferred in the network is transfiguration of partial key. Even though a mobile adversary collects t partial signed certificates during a share refreshing period, it's infeasible to figure out SSK, which is equivalent to RSA plain text attack. The difficulty of discrete logarithm problem in Galois Field ensures the security of our scheme. Meanwhile, in order to prevent malicious node from issuing wrong partial signed certificate, verifiable secret sharing [9] is adapted. Once node w receives a partial signed certificate, it verifies the validity of partial key before adding them together to recover SSK. In this scenario, malicious node can't disorder the recovering process. Wrong partial signed certificate can be detected as long as destination node gets it. It may be from a compromised node that is compromised by adversary or just a node that makes a mistake. Node w can directly discard the wrong certificate when it finds the certificate is invalid and then broadcast a signed state to notify the network about this authentication node's misbehavior.

In order to avoid adversary's mobile attack, the homomorphic feature of partial key is utilized to renew secret share periodically. Before a mobile adversary does its best to capture t authentication nodes, the partial key has been renewed during this period of time, then the t partial keys can not be used to recover SSK any more due to their different editions.

3.2. Success ratio for authentication

The success ratio for authentication (or success ratio for short) is defined as: the ratio of the number of times of new nodes successfully joining the network to the total number of times for joining requests.

In this paper, threshold secret sharing and the idea of trust transfer are combined to help finding authentication nodes through neighboring nodes. Certificate exchange scheme disseminates trust and enhances success ratio effectively. Chained authentication scheme can solve the authentication problem between any two nodes in the network, so it is integrated into our scheme.

Given that (n, t) threshold scheme is adopted, we denote the communication range of normal node as r, S means the size of the network, and the max-hop of trust chain is set as h, where h is a system parameter that can be adjusted according to specific network environment. We assume authentication nodes move randomly in the network. Then, the success ratio of the distributed authentication scheme is obtained by:

$$R_{DIS} = \sum_{i=t}^{n} \{C_n^t \times [\frac{r^2}{S}]^i \times [1 - \frac{r^2}{S}]^{n-i}$$

We can know from subsection 2.3 that the length of trust chain of node can reach h hops, including the link between new node and proxy node, so the success ratio of the hybrid authentication scheme can be represented as follows:

$$R_{HYB} = \sum_{i=t}^{n} \{C_n^i \times [\frac{(hr)^2}{S}]^i \times [1 - \frac{(hr)^2}{S}]^{n-i}\}$$

When r=200, S=5000m*5000m, Table 1 presents comparative results of the success ratio of distributed scheme and hybrid scheme under different numbers of authentication node and different threshold values. We also investigate the trend of success ratio when h is set as different values.

Table 1 Comparison of Success Ratio for Authentication

	t=3, n=500, n'=150	t=3, n=1000, n'=300	t=4, n=500, n'=150	t=4, n=100, n'=300
R_{dcs}	46.03%	79.56%	24.69%	65.75%
R_{hyb}/h=2	58.24%	94.11%	35.60%	85.43%
R_{hyb}/h=3	96.82%	99.99%	91.27%	99.94%

In order to validate theoretical analysis of our scheme, we simulate the scheme with C++. We first investigate how the network scale and the max-hops of trust chain influence the success ratio for authentication. The mobility patterns of sensor nodes follow random way-point model. In the simulations, the number of authentication nodes is set as 200, and

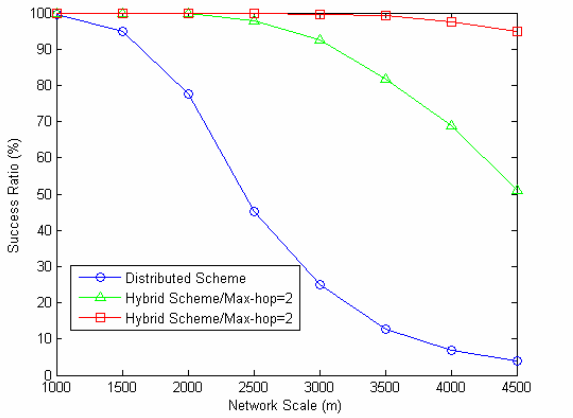

Fig. 3 Success Ratio vs. Network Scale when t=3, n=200, Mobility=10m/s

the threshold value t=3. As shown in Fig.3, if the

trust chain's max-hop reaches to 3 or more, the success ratio of our scheme is almost 100% even in sparse network. But the success ratio of distributed scheme decreases dramatically when the size of the network increases. Fig.3 indicates that our scheme is much more scalable than distributed scheme in terms of success ratio.

The stability of our scheme is also demonstrated in Fig.4. We observe that when the value of max-hops is determined, the success ratio of hybrid scheme is insensitive to the threshold value.

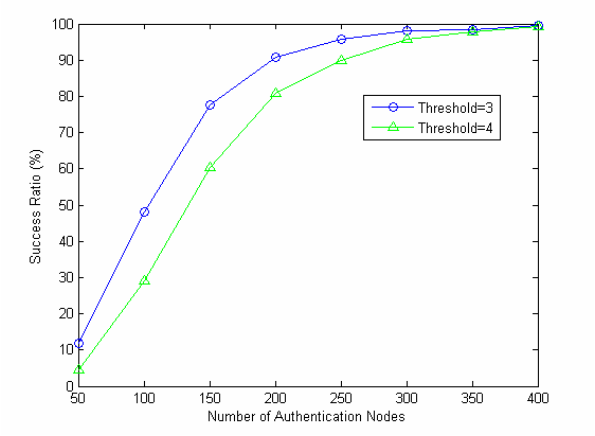

Fig. 4 Success Ratio vs. Number of Authentication nodes when *h*=3, *s*=5000, Mobility=10m/s

4. Conclusions

This paper presents a hybrid authentication scheme which combines the threshold scheme and the mechanism of trust transfer in a seamless way. The proposed scheme utilizes the transfer of trust relations to find authentication nodes, and then improves the success ratio for authentication effectively. The theoretical analysis and simulation results show the usefulness of the proposed scheme in improving the scalability without sacrificing the security. The proposed scheme can be used in large-scale mobile ad hoc networks, while most existing authentication schemes can only be used in small or medium-scale mobile ad hoc networks.

ACKNOWLEDGMENT

This work is supported by the National High-Tech Research and Development Plan of China (863 Plan) under Grant No. 2006AA01Z202, the Hong Kong Polytechnic University under the ICRG Grant G-YE57, the National Natural Science Foundation of China under Grant No. 60533040, and the Program for New Century Excellent Talents in University under Grant No. NCET-06-0686.

References

[1] J. Garman, Kerberos: The Definitive Guide, O'Reilly, 2003.

[2] L. Zhou, Z.J. Hass, "Securing Ad Hoc Networks," IEEE Network Magazine, 1999, 13(6): 24-30.

[3] J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," Proceedings of the 9thInternational Conference on Network Protocols (ICNP), Riverside, California, USA, 2001. pp. 251-260.

[4] S. Capkun, L. Buttyan, J. P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," IEEE Transactions on Mobile Computing, 2003, 2(1): 52-64.

[5] A. Shamir, "How to Share a Secret," Communications of the ACM, 1979, 22(11): 612-613.

[6] E.C.H. Ngai and M.R. Lyu, "Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks," Proceedings of 24th International Conference on Distributed Computing Systems Workshops - W4: MDC (ICDCSW'04), Hong Kong, China, 2004, pp. 582-587.

[7] A. Abdul-Rahman, The PGP Trust Model, Journal of Electronic Commerce, Vol. 3, 1997,pp. 27-31.

[8] Y. Xiong, F.-Y. Miao, W.-C. Zhang, "Secure Distributed Authentication Based on Multi-Hop Signing with Encryped Signature Functions in Mobile Ad Hoc Networks," ACTA ELECTRONICA SINICA, 2003, 31(2): 137-139.

[9] C. Cachin, K. Kursawe, A. Lysyanskaya, R. Strobl, "Asynchronous Verifiable Secret Sharing and Proactive Cryptosystems," Proceedings of the 9th ACM conference on Computer and Communications Security, Washington, DC, USA , 2002, pp. 88-97.

[10] Y. Tsai, S. Wang, "Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks," Proceedings of IEEE 60th Vehicular Technology Conference (VTC), Los Angeles, CA, USA, 2004, pp. 4716-4720.

[11] H. Luo, J. Kong, P. Zerfos, "URSA: Ubiquitous and Robust Access Control for Mobile Ad-Hoc Networks," IEEE/ACM Transactions on Networking, 2004, 12(6):1063-1079.