Journal of Applied Sciences

ISSN 1812-5654

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 7 (12): 1638-1642, 2007
ISSN 1812-5654

Identity Authentication and Key Agreement Schemes for Ad Hoc Networks

Mohammad A. AL-Fayoumi and Sattar J. Aboud
Department of Computer Information Science, Faculty of IT,
The Middle East University for Graduate Studies, Amman, Jordan

Abstract: Identity authentication and key agreement schemes play significant role in ad hoc networks. In this study, a new identity authentication scheme relies on the threshold group signature is introduced. Compared with the current schemes it is secure, efficient and adaptable to a multi-hop feature of ad hoc networks. In addition, a new key agreement scheme based on the threshold cryptography using the Lagrange interpolation theorem is suggested, its efficiency and security are examined and is claimed to be more efficient than the existing schemes.

Key words: Ad hoc networks, key agreement, identity authentication, threshold group signature, multi-hop, shares key, identity certificate

INTRODUCTION

An ad hoc network is often defined as an infrastructures network, denoting a network without the usual routing infrastructure like fixed routers and routing back-bourn (Yao and Zeng, 2004; Mauve *et al*., 2001; Stjmenovic and Lin, 2001). Mobile ad hoc networking offers convenient infrastructureless communication over the shared wireless channel (Jayakumar and Chellappan, 2005). A group of networking devices communicates among one another using wireless radios and operates by following a peer-to-peer network model. The nature of such a network makes them vulnerable to security attacks. Examples of attacks include passive eavesdropping over the wireless channel, denial of service attacks by malicious users and attacks from compromised entities or stolen devices. Unlike wired networks where an opponent must gain physical access to the wired link or sneak through security holes at firewalls and routers, wireless attacks may come from anywhere along all directions (Luo *et al*., 2002). The infrastructureless ad hoc network will not have a clear line of defense and each user must be prepared for encounters with an opponent. Therefore, a centralized or hierarchical network security solution (Aresenault and Turner, 2000) does not work well in mobile ad hoc networks.

Security is a crucial matter for ad hoc networks, especially for security sensitive uses for example battleground. Ad hoc networks are usual dynamic peer networks. The specific security requirements of dynamic peer networks such as key management are yet considered as open research challenges (Bettstetter and Friedrich, 2003). Newly, a number of key agreement protocols regarding dynamic peer networks are suggested. For example the key agreement protocols that are obtained by extended the known Diffie-Hellman key exchange scheme to groups of *n* users is described in (Ateniese *et al*., 1998a). Two key agreement protocols relied on the threshold scheme employing Lagrange interpolation theorem, are introduced in (Desmedt, 1994; Pieprzyk and Li, 2000). Another key agreement protocol relied on the octopus scheme is presented in (Lang *et al*., 2003).

Identity authentication is another significant area of research for the security of ad hoc networks. The valid certificate authority can efficiently stop the impersonation attacks. The centrally disciplined trust communications managed by a one certificate service is a specific point of failure. So we should employ a distributed authority certificate in which the trust is managed by many authorities. The concept of distributing a certificate authority all around the network is presented in (Zhou and Hass, 1999; Luo *et al*., 2002). The scheme that provided a method to authenticate the partitioned of ad hoc networks is introduced in (Kaliaperumal, 2003). Also an identification protocol is suggested in (Khalili *et al*., 2003) that allow efficient and flexible key distribution whilst respecting the restrictions of ad hoc networks.

The objectives of this study are:

- Introduce a new identity authentication protocol relies on the threshold group signatures.

Corresponding Author: Mohammad A. AL-Fayoumi, Department of Computer Information Science, Faculty of IT, The Middle East University for Graduate Studies, Amman, Jordan

- Develop a new key agreement protocol based on the threshold encryption using the Lagrange interpolation theorem.
- Compare these proposed schemes with the current schemes from security and efficiently point view
- To make these schemes more adaptable with the multi-hop characteristics of ad-hoc networks.
- To guaranteed the privacy of the basic group key and identify certificate by the intractability of computing discrete logarithm.

For an ad hoc network, there are many special properties we should follow, such that architecture, dynamic, distributed, multi-hop, etc. The great benefit of the suggested protocols is to achieve secure communication while following these properties.

THE PROPOSED KEY AGREEMENT SCHEME

For ad hoc network, it is necessary to distribute essential keys between numbers of users. However, the ad hoc network is a dynamic peer-to-peer network and the key infrastructure should therefore be supplied in a distributed technique. The suggested protocol is to establish the key service in ad hoc networks. An efficient key agreement protocol is introduced using the multi-hop property of the ad hoc networks.

To start with, assume that there are just several users in the network; these users require common group session keys to communicate mutually. So each user equally contributes to establish the group key. In addition every user has a regular private password w. This password is just used at the establishment of the group session key. Also, assume that p is the large prime and a is the generator of GF(q) with order q, suppose q is a large prime number and GF(q) is a finite field. Every user u_i in the ad hoc network selects randomly a prime number. But when there are t users in the network, u_1 finds $w * a^{s_1}$ mod p and sends the outcomes to u_2. The shares key

$$s = \sum_{i=1}^{t} s_i$$

of this network can be calculated corresponding to Lagrange interpolation theorem. Where t the number of users in the network and can be computed by how many hi messages are received from other users. So each user u_i gets a series of t users (s_1, i,... s_t, i) and computes his share

$$s_i = \sum_{i=1}^{t} s_i \bmod q.$$

In fact the polynomial

$$F(x) = \sum_{i=1}^{t} f_i(x) \bmod q$$

presents the last formula contributed by all of users and $s_i \equiv F(i) \bmod q$. So, all users can work out the group key after they received all shares transmitted by other users. Then every following user u_i for 1<i<t receives $w * a^{s_1 \cdots s_i - 1} \bmod q$ and multiplies the result to the power s_i to find $w * a^{s_1 \cdots s_i} \bmod p$. Then $w * a^{s_1 \cdots s_i} \bmod p$ together with $w * a^{s_1}, w * a^{s_2}, \ldots, w * a^{s_i}$ is sent to u_{i+1}. The last user u_t receives

$$(w * a^{\prod_{i=1}^{t-1} s_i}) \bmod p$$

and multiplies the result to the power s_t to compute

$$s^{-} \equiv w * a^{\prod_{i=1}^{t} s_i} \bmod p \cdot$$

In addition, u_t also receives $w * a^{s_1}, w * a^{s_2}, \ldots., w * a^{s_{t-1}}$, Thus u_t finds the $r_{i,t} \equiv a^{s_{i1} * s_t} \bmod p, \text{for } i \neq t$. On behalf the entire group, u_t transmits the group session key $s^{-} = r_{i,t}, wa^{s_t}$ to $u_i (i \neq t)$ in the network. So every user knows the group session key $s \equiv s^{-} u^{-1} r_{i,t}^{-1}$ mod p. This situation is more like to the actuality of ad hoc networks since one important property of ad hoc networks is multi-hop. Figure 1 shows the process of the proposed key agreement protocol.

Security Analysis: For the security examination we gain from the modular design of proposed system using well known cryptography schemes. Although all attacks of the schemes are verified to be prevented. The security analysis is obliviously constructions as we stay away from interaction among the schemes as can as possible. We now plan the proofs that the new schemes own several security characteristics, If not providing a specific suggestion, we suppose that all users do not conspire with every other.

Theorem 1: This suggested scheme gives great punctual security.

Proof 1: For the adversary unknowing the password, he can not find any helpful data during the messages sent among the users, since every message is encrypted by the password *w*. Even if the opponent shared the password w, he mostly can calculate

$$w * a^{\prod_{i=1}^{t-1} s_i} w^{-1} \equiv a^{\prod_{i=1}^{t-1} s_i}$$

mod p instead of the shares key. The intermit messages are not useful to find the shares key. When the last user u_t transmits the group key to each user u_i, he encrypts the message with w and $r_{i,t}$ contemporarily. It is obvious that $r_{i,t} \equiv a^{s_i s_t}$ mod p is hard to solve relied on the difficulty to

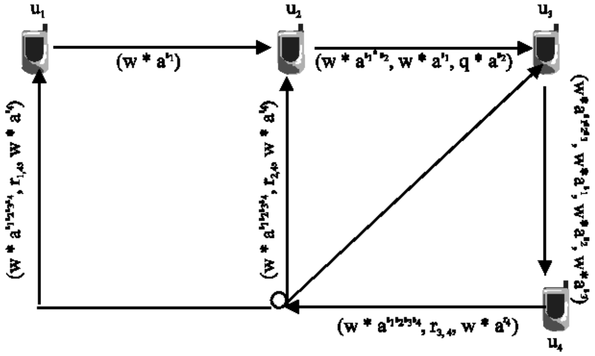
u1
u2
u3
u4
(w * a^r1)
(w * a^r1*r2, w * a^r1, q * a^r2)
(w * a^r1r2r3r4, r1,4, w * a^r1)
(w * a^r1r2r3r4, r2,4, w * a^r2)
(w*a^r3, w*a^r2, w*a^r1, w*a^r1r2r3)
(w * a^r1r2r3r4, r3,4, w * a^r4)

Fig. 1: The proposed key agreement protocol

compute the Diffie-Hellman problem in prime order subgroups except for the two users u_t and u_i.

Theorem 2: The suggested scheme sustains the share independence between the groups.

Proof 2: Corresponding to the suggested scheme, every user u_i transmits u_i to the next user. Even if $w * a^{s_i}$ can be found with w, the share s_i is yet not unperceivable to other users relied on the difficulty of solving the discrete logarithm problem.

In this scheme, just about 2(n-1) rounds are required for establishing the shares key, the traffic between the networks is significantly decreasing. But it is obvious that the proposed scheme has the less communication than the other existing schemes, it grows the complexity cost for every one.

THE PROPOSED IDENTITY AUTHENTICATION PROTOCOL

In the pervious section, we only concentrate on the establishment of the shares key and we do not focus on the identity authentication. But when a single user is compromised and exposed by the authentic users, there must be a method to insulate the user. Thus a new identity authentication protocol is suggested to face this difficulty. It gives a distributed way to publish the authority certificate to each user.

For a considerable ad hoc network, it is more suitable when the new user just requires few of the users those are near to him to publish the authority certificate. Thus we suggested a(t, w) threshold group signature scheme to achieve this work, such that t is the threshold value and w is the number of users in the network. The first part of the protocol can be organized as follows:

Each user selects a polynomial with order mostly t-1,

$$f_i(x) = a_{i,t-1}x^{t-1} + ... + a_{i,1}{}^{x+a_i},$$

such that coefficients $a_{i,j} \in GF(q)$ are selected randomly for i = 1, ..., t where t is the threshold value discussed by the all users. However, n is a large composite modulus where n = p*q such that p and q are large prime numbers. Each user u_i has its unique series integer number i. Then, u_i determines the shares key $s_{i,j} = f_i(j) \bmod \theta(n)$ such that $\theta(n) = (p-1)(q-1)$ and communicates $s_{i,j}$ to the user $u_j(j = 1,..., u)$ $j \neq i$. Thus each user u_i gets a series of w users $(s_{1,j,..,} s_{w,j})$ and calculates his share

$$s_i \sum_{j=1}^{w} s_{j,i}$$

such that $s_i = F(i)$ and the polynomial

$$F(x) = \sum_{i=1}^{w} f_i(x)$$

mod θ(n) denotes the last formulae contributed by the entire users. Though, more than t users can find out the share key, we do not permit them to rebuild the key since we do not require each user knows the shares key. Instead, one user is selected for the trusting user and the user can ask for other t-1 users to detect the share key. Then we require the keys issued by this trusting user. Assume that u_1 is the trusting user and gathers the sub-secrets form other t-1 users. Then the user can find out the shares key corresponding to the Language interpolation theorem.

Gullious-Quisquater (Guillou and Quisquater, 1990) suggested a digital signature algorithm relied on the difficulty of integer factoring. We enhanced this algorithm and suggested a novel group signature scheme to suit the authentication of ad hoc networks. Again we use n as a composite integer modulus, b is a arbitrary integer prime number less than θ(n), g is a generator of z_n^* with order θ(n) and t is a arbitrary integer number of z_n^*, z_n^* is the multiplicative group of z_n, h(.) is a one way hash function. The user secret key is $x = g^t \bmod n$ and v is the public key such as $x^b*v \equiv g^{-tb}$, where $v \equiv g^{-tb} \bmod n$. The keys n, b, v and function h(.) are made public and the other keys are private.

We perceive that just user u_1 can gather the sub privates and find the shares key. However, u_1 requires announcing the public group key $v \equiv g^{-tb} \bmod n$ and c is the group key discussed by all users. Once u_1 transmitted all of the keys, he deletes secret key $v \equiv g^c \bmod n$, if a private key is recovered by opponents later, u_1 plays as a typical user. Assume a new user joints the network for the first time; this user must ask for an authority certificate from the users presented in the network. The steps are as follows:

A new user u_n transmits his demand to the next users. But if more than t users respond and are eager implement

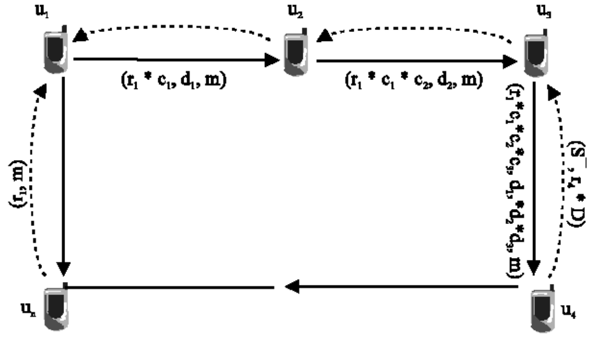

Fig. 2: The proposed identity authentication protocol

out the authentication process, u_n terminate transmitting. Then u_n chooses t users as his authentication users and chooses the first user and last user. The medial users are not decisive so their series can be arbitrary. Given that the t users $\{u_1, u_2, ..., u_t\}$ generate the set A. So u_n builds the session key r_t as well as u_t in advance. Then u_n transmit the message m, the series numbers of set A and the integer r_1 to u_1. Then u_1 selects a random d_1 and calculate

$$c_1 \equiv d_1 * g^{s_1 \prod_{i \neq 1} \frac{-i}{1-i}} \bmod n,$$

such that s_1 is a share key hold by u_1. After that u_1 calculates $r_1 * c_1$ and transmits (r_1*c_1,d_1,m) to u_2. The u_2 picks an arbitrary number d_2 then finds

$$c_2 \equiv d_2 * g^{s_2 \prod_{i \neq 2} \frac{-i}{2-i}} \bmod n.$$

Next u_2 transmits $(r_1*c_1*c_2,d_1*d_2,m)$ to the subsequent user. Similarity, u_t the last user to link with the authentication process, obtains the result

$$(r_1 \prod_{i=1}^{t-1} c_i, \prod_{i=1}^{t-1} d_i, m)$$

transmitted by u_{t-1}. Thus u_t plays an essential role in the creation of certificate authority. Also u_t chooses an integer number d_t and finds

$$c_t \equiv d_t * g^{s_t \prod_{i \neq t} \frac{-i}{t-i}}$$

mod n, then hecomputes

$$D \equiv \prod_{i=1}^{t} d_i^b \bmod n,\ h = h(m,D) \text{ and } s^- \equiv (r1 \prod_{i=1}^{t} ci) \bmod n,$$

r_t is a private shared key by u_t and u_n. Lastly u_t transmit (s^-, r_t*D) to u_n. Then u_n calculates $D = (r_1 * D)r_t^{-1}$ mod n, $s = (s^- * r_1^{-h}$ mod n and gets the last authority certificate (s, D). To verify the signature, u_n check if $D^h \equiv s^b v^h$ mod n. If true, then u_n accepts the group signature (s, D) as his authority certificate. But if not, u_n reject the group signature and asks for another authority certificate. Figure 2 shows the identity authentication protocol.

Security evaluation: We now plan the proofs that the new scheme owns several security characteristics. If not provided a specific suggestion, we suppose that all users do not conspire with every other.

Theorem 3: The proposed authentication protocol gives the share key independence.

Proof 3: The first user u_1 transmits $(r_1* c_1, d_1, m)$ to the second user u_2, such that r_1 is the private shared key by u_1 and u_2. The u_2 can not recover the actual share key s_1 kept by u_1. Similarity, the next users also can not decipher the other users' shares key.

Theorem 4: No one in this proposed scheme perceives the authority certificate of u_n.

Proof 4: The u_t forms the last group signature such that u_t has the possibility to obtain the identity certificate of u_n. However u_t does not perceive the private r_1 shared key by u_n and u_1. So u_t does not get the identity certificate of u_n. While u_1 perceives the private r_1, but he can not perceive the random integer number D and can not calculate the hash function h. So u_1 can not recover s from the authority certificate s^- even if s^- is sent by u_1 to u_n.

Theorem 5: If the formula $D^h = s^b * v^h$ mod n retains, the identity certificate (s, D) is true.

Proof 5: From the explanation above, we identify that:

$$s = (\prod_{i=1}^{t} c_i)^h = g^{c*h} (\prod_{i=1}^{t} d_i)^h \bmod n$$

$$D = (\prod_{i=1}^{t} d_i)^b \bmod n$$

and $v = g^{-c*b}$ mod n. So if

$$s^b * v^h = g^{c*h*b} (\prod_{i=1}^{t} d_i)^{h*b} * g^{-c*h*b} = (\prod_{i=1}^{t} d_i)^{h*b} = D^h \bmod n$$

retains, it is proof that the identity certificate (s, D) is true.

CONCLUSION

The suggested key agreement scheme is appropriate to create a group session key. In general the first users of the ad hoc network are considers trustful and honest. So employing the suggested key agreement protocol can rapidly establish the session key, since the message can be transmitted with out encryption. However, after the ad hoc network has run for a while, the suggested key agreement protocol can provide great security and meet the need to efficiently build the session key. It needs just 2(n-1) rounds highly decreases the traffic in the network.

In the proposed protocol, the fixed password w greatly reduces the time complexity required (Ateniese *et al*., 1998b). Compared with the protocol suggested in (Ateniese *et al*., 1998b), we do not require refreshing the group session key each time when a new user connects the network, since the group session key created by the proposed protocol is just employed for group communication. The group session key can be transmit to another users encrypted by the fixed password *w* straight. For valuable discussion among two users after the authority certificate is checked out, the two users will assign a new session key by Diffie-Hellman scheme. In addition, we developed a zero knowledge scheme to reuse the authority certificate. All these protocols enhance the efficiency of the suggested protocols. Concerning the authentication scheme, the discrete logarithm algorithm is employed in the proposed protocol whereas threshold RSA scheme is employed by (Luo *et al*., 2002). Since, it is well known that threshold RSA scheme requires additional time complexity compared with the discrete logarithm problem (Hezberg *et al*., 1995). Consequently the proposed identity authentication protocol is more efficient compared with the scheme in (Luo *et al*., 2002).

REFERENCES

Aresenault, A. and S. Turner, 2000. Internet X.509 public key infrastructure. draft-ietf-pkix-roadmap-06.txt

Ateniese, G., M. Steiner and G. Fsudik, 1998a. Authenticated group key agreement and friends. Proceedings of the 5th ACM Conference on Computer and Communications Security, ACM., pp: 17-26 .

Ateniese, G., M. Steiner and G. Fsudik, 1998b. Key agreement protocol in ad hoc networks, Communication Technology Proceedings, ICCT, International Conference on, IEEE, 1: 296-301.

Bettstetter, C. and B. Friedrich, 2003. Time and message complexities of the generalized distributed mobility adaptive clustering (GDMAC) algorithm in wireless multihop network. Proceeding of IEEE Vehicular Technology Conference, Jeju, Korea, pp: 22-25.

Desmedt, Y., 1994. Threshold cryptography. Eur. Trans. Tele-commun., 5: 449-457.

Guillou, L. and L. Quisquater, 1990. A paradoxical identity based signature scheme resulting from zero knowledge, Advances in Cryptology Proceedings, LNCS, Springer Verlag, pp: 216-231.

Hezberg, H., D. Jarecki, H. Krawzyk and M. Young, 1995. Proactive secret sharing or: how to cope with perpetual leakage, Crypto ’95, Lecture Notes in Computer Science, Springer-Verlag.

Jayakumar, C. and C. Chellappan, 2005. A ware energy efficient routing protocol for wireless ad-hoc network. Asian J. Inform. Technol., 4: 578-582.

Kaliaperumal, S., 2003, Securing authentication and Privacy in ad hoc partitioned networks. Applications and the Internet Workshops. Proceedings of Symposium, IEEE, 27-31, pp: 354-357.

Khalili, A., J. Katz and W. Arbaugh, 2003. Toward secure key distribution in truly ad hoc networks. Applications, Symposium, IEEE, 27-31, pp: 342-346.

Lang, W., M. Zhou and K. She, 2003. Key agreement protocol in ad hoc network. Communication Technology Proceeding. ICCT 2003, International Conference on IEEE, 18: 296-301.

Luo, H., P. Zerfos, J. Kong, S. Lu and L. Zhong, 2002. Self securing ad hoc wireless networks, 7th IEEE Symposium on Computers and Communications (ISCC'02), Italy, pp: 567-574.

Mauve, M., J. Widmer and H. Hartenstein, 2001. A survey on position-based routing in mobile ad-hoc networks. IEEE Network, 15: 30-39.

Pieprzyk, J. and C. Li, 2000, Multiparty key agreement protocols. IEE Proceeding. Computers and Digital Techniques, 147: 229-236.

Stjmenovic, I. and X. Lin, 2001. Power aware localized routing in wireless networks. IEEE Transaction on Parallel and Distributed System, 12: 1122-1133.

Yao, J. and G. Zeng, 2004. Key agreement and identity authentication protocols for ad hoc network. Proceeding of IEEE ITCC International Conference on Information Technology, 5-7, Las Vegas, Nevada, USA., pp: 720-724.

Zhou, L. and Z. Hass, 1999. Securing ad hoc networks. IEEE Networks, 13: 24-30.