Verifiable Secret Sharing Authentication Scheme without Trusted Center for Mobile Ad Hoc Network

Zu-ping ZHANG and Yang SONG
School of Information Science & Engineering, Central South University, Changsha, China
*Corresponding author

Keywords: Mobile ad hoc network, Secret sharing, Authentication.

Abstract. Mobile ad hoc network is an autonomous network of several mobile nodes that don’t rely on any base station facilities and management organizations. Due to mobility of the nodes, the network topology may dynamically change over time. Compared with traditional network mobile ad hoc network with distributed characteristics is more vulnerable and unsafe. Thus Safety certification research of mobile ad hoc network is the essential research. In this paper, with secret sharing a verifiable authentication scheme without trusted center is proposed, which can confirm the legitimacy of the every node in the mobile ad hoc network. So as to ensure information security of the network system.

Introduction

Mobile ad hoc network (MANET) is an autonomous set of mobile nodes that communicate with each other over relatively bandwidth constrained wireless links [1]. The security objective including availability, confidentiality, integrity and non-repudiation is similar to traditional network [2]. Due to the frequent changes of topology for MANET without centralized network management facilities, MANET encounters many security threats that traditional network do not encountered [3]. 1) Conventional network authentication mechanisms is difficult to implement with the difficulty of distinguishing the node’s legitimacy. 2) It is impossible to prevent and defend against security attacks at all times because of the high flexibility and randomness of the nodes for MANET. 3) Nodes of MANET communicate with each other with vulnerable wireless links, which makes data packets are more vulnerable to eavesdropping, tampering and encountering other attacks. The above-mentioned characteristics of MANET have led to more and more attention to identity authentication. Meanwhile many authentication schemes have been proposed.

Authentication Scheme of MANET

Currently, there are two main methods for network node authentication: the authentication mechanism based on the public key certificate and the authentication mechanism based on trusted management. Various authentication schemes belong to two above-mentioned mechanism are proposed. Zhou et al. [4] proposed key management scheme based on Certificate Authority (CA), which flexibly applied the (k, n) threshold secret sharing system to distribute the centralized CA authentication function. Each network node of MANET assumes partial authentication function. Luo et al. further pointed out the flaw of (k, n) threshold scheme. If the K value is very large, MANET system request a number of combined nodes to achieve a more secure public key certificate authentication mechanism. However, it is difficult to get many nodes that meet the conditions at the same time. On the other hand, once the attacker controls parts of special nodes, the entire authentication mechanism will be completely invalid. Therefore, the localized CA function authentication scheme is proposed [5,6]. There is another distributed trust management mechanism: PGP trust model [7]. Every node in the network needs to issue it’s public key certificate. If other nodes are trusted, public key certificate signed for them will be issued by the node. Once two nodes need to implement authentication, they must first find out a chain of trust relationships between them.
Otherwise, authentication cannot be achieved. Srdjan et al. applied the authentication mechanism of PGP trust mode to MANET [8]. Every node of MANET signs two types of certificates, one for itself and the other for other nodes that it trusts. When they need to be authenticated, the two nodes need to exchange their respective certificate stores to find out the trust links that exist between them. The trust relationship determines the direction of authentication. There are also many other MANET authentication schemes [9-11].

Verifiable Secret Sharing Authentication Scheme without Trusted Center

Verifiable secret sharing authentication scheme [12] without trusted center is proposed in this paper with characters of MANET. In this scheme, all participants of MANET do not rely on the management of any trusted center. Every node holds a secret share factor that to create secret shame. All nodes are mutually dependent on each other and restrict each other. They can obtain their own secret shares which can generate partial signatures by exchanging their respective secret share factors. Finally, group signature is formed by synthesizing partial signature. During the signing process, the private key of the group is not exposed. Meanwhile the validity of the signature can be verified. Therefore MANET network nodes can be authenticated to ensure information security of MANET.

Preparation Phase

Each participating network node of MANET including n nodes represents a participant $p_i$ ($0 < i \leq n$). $p_i$ randomly selects a positive integer $z_i$ ($Z = \{z_1, z_2, \ldots, z_n\}$), where $(z_i, z_j) = 1, (i \neq j)$. Select two large prime numbers $h$ and $d$ to satisfy $(z_i, d) = 1, i = 1, 2, \ldots n$. Additionally, integer domain generator $g$ is also needed.

1) $p_i$ randomly selects $y_i$ and an integer $C_i$ which satisfy the below condition:

$$0 < y_i < \left\lfloor \frac{d}{n} \right\rfloor,$$  \hspace{1cm} (1)

$$0 \leq C_i \leq \left\lfloor \frac{[N/d] - 1}{n} \right\rfloor,$$  \hspace{1cm} (2)

where $N = \prod_{i=1}^{t} z_i > d \prod_{i=1}^{t-1} z_{n-i+1}$.

$p_i$ calculates $X_i$ and $\lambda_{ij}$:

$$X_i = y_i + C_i d,$$  \hspace{1cm} (3)

$$\lambda_{ij} = X_i \mod d_j,$$  \hspace{1cm} (4)

where $y_i$ is sub-secret of node as their respective private key. $\lambda_{ij}$ is secret share factor to guide the generation of secret share.

2) $p_i$ calculates group public key and group private key:

$$Y = \sum_{i=1}^{n} y_i \mod d,$$  \hspace{1cm} (5)

$$X = \sum_{i=1}^{n} y_i.$$  \hspace{1cm} (6)

3) Received $\lambda_{ij}$ providing by other nodes, $p_i$ calculates secret share $M_i$ to generate signature:
\[ M_j = \sum_{i=1}^{n} \lambda_{ij} \mod z_j = \sum_{i=1}^{n} X_i \mod z_j. \] (7)

**Partial Signature Phase**

k nodes generate their partial signature by using their secret share with Chinese remainder theorem (CRT). The generation of partial signature is dependent on sub-secret of \( p_i \), so k nodes send their partial signature to synthesizer.

1) \( p_i \) calculates modulus \( \mu_i \) to synthesize signature:

\[ \mu_i = g^{x_i} \mod d. \] (8)

2) \( p_i \) calculates partial signature \( S_i \) with CRT:

\[ S_i = Z_i \cdot t_i \cdot M_i \mod Z, \] (9)

where \( Z = z_1 \times z_2 \times \cdots \times z_n, \ Z_i = Z/z_i, \ t_i \) is a multiplicative inverse of \( Z_i : Z_i \times t_i \equiv 1 \mod z_i, \ i = 1, 2, \cdots, n. \) With condition of mod Z the signature synthesized by k nodes is uniquely determined.

3) \( p_i \) generates the partial signature with the message \( D \) then sends \((D, u, \tau_i)\) to the synthesizer.

\[ \mu = \prod_{i=1}^{t} g^{x_i} \mod h \] (10)

\[ \tau_i = X_i \cdot D + \mu \cdot M_i. \] (11)

**Synthesis and Verification Phase**

The synthesizer calculates

\[ \Gamma = \left( \sum_{i=1}^{t} \tau_i \mod Z \right) \mod d \] (12)

after receiving k signature \((D, u, \tau_i)\).

\((D, u, \tau_i)\) is a group signature of message \( D \). All MANET nodes can verify signature signatures with the group public key. The verification formula is as follows:

\[ g^{\Gamma} \equiv \mu^D \cdot Y^u \mod h. \] (13)

If the above equation is true, the signature synthesized by network nodes is valid. The Authenticity of nodes especially the new nodes for MANET is verified. On the other hand, the process of signature synthesis is also an encryption process for information of the MANET, which effectively protects the information security of the network.

Verification instructions:

Assuming \( W = \sum_{i=1}^{n} X_i \), k nodes holds their own secret share \( M_i \) which satisfies the below congruence equation:

\[ W \equiv M_i \mod z_i, i = 1, 2, \cdots, t \] (14)

With above-mentioned public parameters and conditions, we can obtain:
So \( W = \sum_{i=1}^{n} X_i = \sum_{i=1}^{m} y_i + d \cdot \sum_{i=1}^{n} C_i < d + N - d = N \). 

So \( 0 < W < N \). Here \( N \) is the product of \( z_i, i = 1, 2, \cdots n \) when \( k \) is minimum. The equation

\[
Z = \prod_{i=1}^{t} z_i \geq N
\]

guarantees that \( W \) is unique on condition of mod \( Z \), which means the below equation has the unique root according to CRT:

\[
W = \sum_{i=1}^{t} Z_i \cdot t_i \cdot M_i \mod Z = \sum_{i=1}^{t} S_i \mod Z.
\]

So the process of signature synthesis verification is as follows:

\[
\Gamma = \left( \sum_{i=1}^{t} t_i \mod Z \right) \mod d
\]

\[
= \left[ \sum_{i=1}^{t} (X_i \cdot D + \mu \cdot M_i) \mod Z \right] \mod d
\]

\[
= \left( D \cdot \sum_{i=1}^{t} X_i + \Gamma \cdot \sum_{i=1}^{t} M_i \mod Z \right) \mod d
\]

\[
= \left( D \cdot \sum_{i=1}^{t} X_i + \Gamma \cdot Z \right) \mod d.
\]

In addition

\[
W = X + \sum_{i=1}^{n} C_i d \equiv X \mod d,
\]

where \( d \) is much larger than \( \mu, D \cdot \sum_{i=1}^{t} X_i \) and \( X \), therefore

\[
\Gamma = D \cdot \sum_{i=1}^{t} X_i + \mu \cdot X
\]

\[
g^\Gamma \equiv g^{D \cdot \sum_{i=1}^{t} X_i + \mu \cdot X}
\]

\[
\equiv g^{D \cdot \sum_{i=1}^{t} X_i} \cdot g^{\mu \cdot X}
\]

\[
\equiv \mu^D \cdot Y^\mu \mod h.
\]

Security Analysis

In the proposed scheme, all participants of MANET do not rely on the management of any trusted center. All corresponding parameters are randomly selected by every node. The security contribution of the proposed scheme is as follows:

1) All nodes participating in verification of MANET randomly selects parameters. All private keys are known only to themselves. The generation of secret shares and group private keys depends on the private key of network node and no one knows the private group key, which successfully avoids the authoritative deception of the trusted center.
2) All MANET nodes participating in verification of the proposed scheme must provide authentic secret shares. Once the secret shares are false they will attain incorrectly signature during the sub-secret generation phase, which causes verification can't pass in the final verification phase.

3) The group private key is secure. Only when all MANET nodes work together can the group private key be obtained, which causes any single node cannot obtain the group private key at all.

4) The private key of all MANET nodes in the whole process of key management is safe. To attain the private key through the published related information is a problem of discrete logarithm, so the private key is secure.

**Conclusion**

A verifiable secret sharing authentication scheme without trusted center for MANET nodes in this paper. All network nodes do not rely on organization of any trusted center. Meanwhile every network node holds a secret share factor. All participants are mutually dependent on each other and also restrict each other. Exchanging their respective secret share factors with others can generate their own secret shares in order to generate partial signatures. Finally, the group signature is obtained by synthesizing all partial signature. During the signing process, the private key of the group is not directly used or exposed, and the validity of the signature can be verified. Furthermore MANET nodes can be authenticated to ensure information security.

**References**


