CERTIFICATE LESS KEY MANAGEMENT SCHEME IN MANET USING THRESHOLD CRYPTOGRAPHY

Shaheena Khatoon[1] and Balwant Singh Thakur[2]

[1]School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, India
[2] School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, India

ABSTRACT

In mobile adhoc networks (MANETs) an efficient and secure key management scheme is extremely crucial. Key management schemes for MANETs are mainly based on identity-based public key cryptography (ID-PKC) or certificate-based public key cryptography, both of which has their inherit problem. The ID-PKC has the key escrow problem and certificate based cryptography have a high computational costs of certificates deployment. In this paper, we present a distributed key management scheme, in which a combination of certificate less public key cryptography (CL-PKC) and threshold cryptography is employed. The scheme proposed in this paper not only achieves several enhanced security attributes for key management in MANET but also eliminates the need for certificate-based public key distribution and the key escrow problem efficiently.

.

KEYWORDS

Key Management, MANETs, Key Escrow, Certificate less Cryptography, Threshold Cryptography.

1.INTRODUCTION

Key management are mainly based on public key infrastructure (PKI) [[1]- [4]] and identity-based public key cryptography (ID-PKC) [[5]- [7]]. But they both have some inherent drawbacks. In an ID-based cryptography system, users private keys are generated by a key generation center (KGC), which means the KGC knows every users' keys this is known as the key escrow problem while in the public key cryptography system, a certificate authority is required to issue certificates between users public keys and private keys to ensure their authenticity, thus increasing computational cost. To avoid these problems in the existing key management system, Satttam et al proposed [8] certificate less cryptography systems which eliminate both the problem i.e. the KGC does not know users' keys the public keys do not need to be certified. Essentially, certificate less cryptography relies between the public key cryptography and ID-based cryptography. In this paper, to implement CL-PKE over MANET and to make it practical, we incorporate the ideas of Shamir's secret sharing scheme [9] , Threshold Cryptography [10]and Satttam et al [8]. Our contribution is to apply the existing certificate less cryptography into MANET using a threshold secret sharing scheme to obtain an efficient and secure MANET scheme.

2. RELATED WORK

In the year 1999, Zhou and Hass [1] describe a partially distributed PKI based solution of key management in MANETs which used certificate-based cryptography and (t, n) threshold cryptography. They used Shamir's [9] threshold cryptography which can distribute trust among a set of servers to build a highly available and secure key management service. Then in the year 2002 Luo et al [3] proposed a fully distributed authority scheme which is a modification of partially distributed certificate authority scheme. The fully distributed authority scheme also makes use of the threshold secret sharing scheme like the partially distributed scheme.

Then in the year 2009, Khalili et al .in [5] provided a key distribution mechanism which combines the use of ID-PKC and threshold cryptography. The advantage of this scheme is this that it avoids the need for users to generate their own public keys and distribute these keys throughout the network, since the user's identity acts as her public key. Besides that, users only need to propagate their identities instead of the certificates. This can lead to huge savings in bandwidth. However, the usage of ID-PKC instead of certificates also results in a few weaknesses. One major weakness is that the key escrow problem since distributed PKG knows all user's private keys. The compromise of the PKG's master key could be disastrous in an ID-PKC system and usually more severe than the compromise of a CA's signing key in a traditional public key cryptography. For these reasons, for these reason in this paper we propose CL-PKC the KGC in CL-PKC supplies a user with a partial private key that the KGC computes from the users identity and a master key. The user then combines the partial private key with some secret information to generate the actual private key. Consequently the KGC does not have access to the user's entire private key.

3. PRELIMINARIES

3.1. Certificate less Public Key Cryptography

The idea of CL-PKC is proposed by Al-Riyami and Peterson [8] with the original motivation of eliminating the inherent key escrow problem of ID-PKC. In CL-PKC, the KGC supplies a user with a partial secret key which the KGC computes from the user's identity and a master key, and then the user combines its partial secret key and the KGC's public parameters with some secret information to generate its actual secret key and public key respectively. In this way, a user's secret key is not available to the KGC.

3.2. Threshold Secret *S*haring

Secret sharing scheme allows a secret to be shared among a group of users which are also called shareholders. The secret is shared in such a way that no single user can deduce the secret from his share alone. In order to construct the secret, a user needs to combine a sufficient number of shares. (t, n) threshold secret sharing represents that the secret is distributed to n share holders, and any t or more users can reconstruct the secret from their shares, but t-1 or fewer users cannot get any information about the secret. Here, k is the threshold parameter such that $1 \leq t \leq n$. The first threshold secret sharing scheme Identity based security schemes for ad hoc routing network was proposed by Shamir [9] in 1979, which is based on polynomial interpolation. To distribute a secret S among n users, a trusted authority chooses a large prime q, and randomly selects a polynomial $f(x) = S + a_1x\ldots + a_{t-1}x^{t-1}(\text{mod}q)$; where L_i $a_1,\ldots\ldots, a_{t-1} \in Z_q$. The trusted authority

computes each user's share by S_i =f(i) and securely sends the share S_i to user i. Then any k users can reconstruct the secret by computing:

$$S = \sum_{i=1}^{t} Si\, Li(modq),$$

Where, $L_i = \prod_{j=1, j\neq i}^{t} -j/(i-j)(modq)$.

4. PROPOSED SCHEME

We incorporate the work of Satttam et al [8] and adopt it to MANET key management with CL-PKE. The scheme is as follows:

4.1. Set up

1. Run the IG generator on an input k, it outputs (G_1, G_2, e) where G_1 and G_2 are groups of prime order q, $e: G_1 \times G_2$ is a pairing.
2. Choose an arbitrary generator $P \in G_1$.
3. Select a master private key s uniformly at random from Z_q^* and set $P_{pub} = sP$.
4. Choose a cryptographic hash function $H_1 : \{0,1\}^* \rightarrow G_1$.

Finally, the KGC publishes the public parameters as: (G_1, G_2, p, q, P, P_{pub}, and H_1).

4.2. Key Generation

To obtain the public key and corresponding private key a user A select its partial secret $x_A \in Z_q^*$ and presents the identity to key generation service. A gets its partial private key $D_A = sQ_A$ where $Q_A = H_1(ID_A) \in G_1$, and then A calculates its full private key as $S_A = x_A D_A = x_A sQ_A$ .The corresponding public key is X_A, Y_A where $X_A = x_A P, Y_A = x_A P_{pub} = x_A sP$. A verifies the algorithm by $e(D_A, P) = e(Q_A, P_{pub})$

4.3. Key Agreement

Suppose node A and B wants to securely communicate with each other, since ID_A, ID_B public key of A and B are all known information node A randomly choose a value $a \in Z_q^*$ and sends $T_A = aP$ to B.Simalarly B randomly choose a value $b \in Z_q^*$ and sends $T_B = bP$ to A. After the above messages are exchanged both entities checks the validity of other public key. A checks $e(X_B, P_{pub}) = e(Y_B, P)$ and B checks $e(X_A, P_{pub}) = e(Y_A, P)$ .Then A calculates the K_{AB} = $e(Q_B,Y_B)^a e(S_A,T_B)(x_A P_{pub}, X_B)$ and B calculates $K_{BA} = e(Q_A, Y_A)^b e(S_B, T_A)\, e(X_B P_{pub}, X_A)$ .It is easy to verify $K_{AB} = K_{BA}$

K_{AB} $= e(Q_B,Y_B)^a e(S_A,T_B)e(x_A P_{pub},X_B)$
$= e(Q_B,x_B sP)^a e(S_A,T_B)e(x_A sP, x_B P)$
$= e(Q_B,P)^{x_B sa} e(S_A,T_B)e(P,P)^{x_A sx_B}$
$= e(x_B sQ_B, aP)e(S_A,T_B)e(x_B sP, x_A P)$
$=e(S_B, T_A)\, e(S_A,T_B)e(X_B P_{pub}, X_A)$

K_{BA} $= e(Q_A,Y_A)^b e(S_B,T_A)e(x_B P_{pub},X_A)$
$= e(Q_A,x_A sP)^b\, e(S_B,T_A)e(x_B P_{pub},X_A)$
$= e(Q_A,P)^{x_A sb}\, e(S_B,T_A)e(x_B P_{pub},X_A)$
$= e(x_A sQ_A, bP)\, e(S_B,T_A)e(x_B P_{pub},X_A)$
$=e(S_A, T_B)\, e(S_B,T_A)e(x_B P_{pub},X_A)$.

Hence $K_{AB} = K_{BA}$

4.4.Key Revocation

Key revocation is the process by which compromised node is removed from the network without effecting the working of network. Suppose a node A is detected abnormal in the network then any t of n D-KGCs jointly execute key revocation process against the node A in the following way

1) The t D-KGCs generate a partial revocation sQ_A .

2) The leader constructs a complete revocation through Lagrange interpolation as: $ID'_A = \sum_{t=1}^{t} S_i L_i Q_A$ Where, $L_i = \prod_{j=1, j\neq i}^{t} -j/(i-j)(mod q)$.

3) The leader informs other nodes in the network than A has been corrupted by sending ID_A, ID'_A .

4) Nodes verify the equation $e(ID'_A, P) = e(Q_A, P_{pub})$, if it holds node A is recorded in the memory any future communication is denied with it.

5.CONCLUSIONS

In mobile adhoc networks (MANETs) an efficient and secure key management scheme is extremely crucial. In this paper we proposed a new approach for key management which uses both certificate less public key cryptography, which reduces the computational cost and threshold secret sharing schemes for enhancing the security of network. Certificate less public key cryptography has two benefits ,firstly it exclude the need of certificating authority for certificate deployments, secondly it preserves the desirable properties of identity-based key management scheme and eliminates key escrow problem. In addition to this we completely removed a trusted third party to distribute the public keys, hence increasing the tolerance of the network to compromised nodes and also saving network bandwidth.

ACKNOWLEDGEMENTS

We would like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

[1] Zhou, L.D and Hass Z.H, 1999 Securing ad hoc networks. IEEE Networks Vol.13, pp. 24-30.
[2] Kong, J.J., Zerfos, P., Luo, H.Y., Lu, S.W., and Zhang, L.X. 2001, Providing robust and ubiquitous support for mobile ad hoc networks. International Conference on Network Protocols.
[3] Luo, H.Y., Zerfos, P., Kong, J.J., Lu, S.W., and Zhang, L.X., 2002, Self-securing ad hoc wireless networks. International symposium on computers and communications
[4] Capkun, S., Buttyan, L., and Hubaux, P., 2003, Self organized public key management for mobile adhoc networks. IEEE Transaction on mobile computing.
[5] Khalili, A. Katz, J. and Arbaugh, W.A., 2003,Toward secure key distribution in truly ad hoc networks. Symposium on application and the Internet Workshops.
[6] Deng, H.M., Mukerjee, A, and Agrawal, D.P., 2004 Threshold and identity based key management and authentication for wireless ad hoc networks. International conference on information technology: coding and computing.
[7] Deng, H.M., and Agrawal, D.P., 2004. TIDS: threshold and identity based security scheme for wireless adhoc networks. Ad hoc networks.
[8] Sattam, S. Al- Riyami and Paterson, K.G., 2003, Certificate less public key cryptography. Advances on Cryptology Asia crypt.
[9] Shamir, A., 1979. How to Share a Secret, Comm. ACM, vol. 22.
[10] Desmedt, Y. and Frankel, Y.,1989,Threshold cryptosystems, Advances on Cryptology-crypto, vol.435.

Authors

Shaheena Khatoon received the B.Sc.,M.Sc. and MPhil degree in Mathematics form Pt.Ravishankar Shukla University, Raipur.Chhattisgarh, India in 2005, 2007 and 2009. She joined School of Studies in Mathematics, Pt.Ravishankar Shukla University, Raipur, India for her research work.

Balwant Singh Thakur Professor, School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C. G.) India. His field of interest are Non Linear Operator Theory and public key Cryptography. He and his research scholars are recently working on many branches of public key cryptography.