

IMPLEMENTING RSA ALGORITHM FOR FULLY DISTRIBUTED CERTIFICATE AUTHORITY IN MANET

Ahmad Alomari¹

ABSTRACT.

Mobile wireless ad hoc networks that are resistant to impersonating nodes are necessary for distributed systems used in security applications. Many secure protocols in mobile ad hoc networks depend on the public key infrastructure. Nodes in MANETs are still vulnerable to different kinds of attacks so multiple certificate authorities (CAs) distributed over the network, each with a periodically updated share of the private key, are usually adopted as a solution. Establishing a distributed virtual CA is an important tool to ensure the security of the mobile ad hoc networks. This article proposes a new scheme for RSA key-sharing scheme based on threshold secret sharing algorithm. In this scheme, the sub secrets are covered when the MANET makes the reconstruction of the polynomial function.

Keywords: MANET, RSA, Certificate Authority.

1. INTRODUCTION

The Mobile Ad-Hoc Networks (MANETs) are independent systems of mobile nodes interconnected by wireless links. Instead of using fixed access point or base stations, intermediate mobile nodes in the MANET act as mobile routers to support connectivity to other mobile nodes that are out of each other's range. The mobile routers are free to move randomly and organize themselves arbitrarily. This inherent flexibility allows for ease of deployment. These networks were originally conceived mostly for military purposes, but because of their inevitable flexibility that they offer they have become also appealing to various commercial applications such as convention meetings, electronic classrooms and search-and-rescue, etc. A side effect of this flexibility is the ease with which a node can join or leave a MANET.

Most security mechanisms are based on Symmetric Encryption or Asymmetric Encryption. In the first the source node encrypts the message using a secret key and the destination node decrypts the message using the same key. So the participant nodes involved in communication have to possess the same secret key before the communication can begin. The symmetric encryption requires that the communication channel over which the distribution of the secret keys takes place must be secure. On the other hand the public key encryption schemes depend on the use of two different keys. Each party generates a public/private key pair. The Source node encrypts a message using the private key and the destination node uses the public key of the sender to decrypt that message. Also, the participant nodes require each other's public keys before starting the communication. Public key encryption does not impose as strict conditions as symmetric encryption on the communication channel used for the key exchange. Public key encryption schemes only require an authenticated channel, as opposed

¹ PhD Student, Faculty of Mathematics and Computer Science, University of Bucharest, Bucharest, Romania alomari.jordan@gmail.com

to a secure channel, for the distribution of public keys. A trusted Certificate Authority (CA) is typically deployed in the security infrastructure to validate the authenticity of the public keys. Before distributing its public key to the intended parties, a node requests the CA to authenticate its key. The CA then issues a digital certificate binding the public key (contained in the digital certificate) to that specific node. The CA uses its own private key to sign this digital certificate. Any other node with the authentic public key of the trusted CA can verify the certificate and thereafter use the public key of the node and be sufficiently sure that it indeed belongs to that node.

The decentralized CA proposal can be classified into two categories: 1) partially distributed CA, 2) fully distributed CA. In the partially distributed CA approach [1], only some of the nodes in the network are pre-selected to serve as CAs at the network setup phase. In the fully distributed CA approach [2], all nodes in the network are provided as a service node with a sub private key to achieve the functionality of the CA. CA services can be obtained from the neighboring nodes. However, it is difficult to manage and protect the shares since a large number of shares are present in the network. Also, in practice, it is not reasonable to assign CA responsibilities to all nodes in the network.

In this paper we propose implementing a Fully Distributed Certificate using RSA cryptographic in Mobile Ad Hoc Network (MANET).

2. RELATED WORKS

As MANETs are dynamic and have a much-dispersed structure they are prone to many routing attacks. The most common attacks present in the existing systems are flooding, black-hole, wormhole attacks. Present system has been designed only by considering the work ability and to avoid overhead caused by the transactions of packets through the network. But these systems are more vulnerable to attacks during the routing of packets from one node to other (i.e. source to destination).

Wide research has been conducted on MANETs for providing security solutions against attack on the basis of cryptographic scheme. The basic cryptographic schemes are public and private key cryptography. As MANETs are dynamic in nature, private key cryptography cannot be a reliable solution because the keys are to be sent through the channel for the receiver to decrypt the message. Even using Diffie–Hellman key exchange for the key it takes three messages to come to a mutual key. This introduces lots of packets in the network that may lead to network congestion. On usage of public key cryptography, the efficient algorithm RSA comes under concern because it is reliable and secure when compared to other public key cryptographic systems. Earlier in the literature, this secret key sharing schemes has been used in multi-path routing where the generated keys are divided into ‘n’ shares and each share takes a separate route to destination. Even if any of the ‘n’ shares has been lost either due to network congestion or by any malicious activity by an attacker or intruder, with the help of ‘n-1’ shares, we can generate the secret key at the destination. By using RSA based threshold cryptography [3] (RSA-TC), Lagrange’s interpolation and the generation of polynomial is for generating partial keys.

The sender transmits these partial keys into multiple routes to destination, along with the shared value. After receiving “t” or more partial keys, the receiver selects “t” keys from the

values received for the deciphering of the message. The receiver encrypts the shared value with the sender's public keys 'e', and transmits it to the sender along various paths. The sender then calculates the values using Lagrange's interpolation for the RSA's "N" parameter, where 'N' is the product of very large prime number generated at random, is sent back to the receiver. Then the receiver applies the shared value to the partial keys and, by collecting all results, he can decipher the secret message. The threshold cryptography based on secret sharing also uses Elliptic Curve Cryptography (ECC) instead of RSA. Here the shared value may be split also after the degree of encryption. The message is split in 'n' pieces. As by ECC, the point exponentiation takes maximum resources and time, while point addition takes the minimum. In ECC-TC [4], the key value is not shared because every value in ECC is in the form of points and for points Lagrange's interpolation is not possible.

A. Amuthan, B.Aravind Baradwaj, proposed Secure Routing Scheme in MANETs using Secret Key Sharing. [5] They propose a new solution for the secure routing of all tree based multicast routing protocols such as MAODV, ADMR, etc, against attacks like flooding, wormhole, black-hole attack etc, in this scheme, keys are generated by source and transmitted to the client nodes in the network. Interpolation concept under the finite field provides a promising outcome for securing the network. The proposed scheme is based on Shamir secret sharing scheme with encrypted transmission of keys. As the transmission of keys to the participant nodes is done using RSA public key encryption algorithm, it is not vulnerable to attacks like replay attacks, and other spoofing.

Y. Dong , Victor O. K. Li , Lucas C. K. Hui, S. M. Yiu introduced Dynamic Distributed Certificate Authority Services for Mobile Ad Hoc Networks [6] They proposed a new framework to provide distributed authority services in cluster-based MANETs. In each cluster, a set of nodes is chosen as CAs. The size of the CA set is adaptive to network changes. We further require the shares in different clusters to be independent, and periodically updated.

3. PRELIMINARIES

I. RSA cryptographic algorithm

RSA systems, developed by MIT's Ronald Rivest, Adi Shamir and Len Adleman in 1978, are the first reversible public key cryptosystems, which can be used for encryption and digital signatures.

In the RSA algorithm, select two different large prime numbers p and q , and so $n = p \cdot q$, then the Euler function of n is $\phi(n) = (p-1)(q-1)$. Select an integer e to meet $0 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$, and to calculate an integer d to satisfy $ed \equiv 1 \pmod{\phi(n)}$, and to make n and e as public key known to public, and d to be kept secretly as secret key.

RSA encryption process: encoding plaintext to be encrypted into an integer m ($0 < m < n$), the ciphertext $C \equiv m^e \pmod{n}$ Decryption process: the plaintext $m \equiv C^d \pmod{n}$. RSA signature process: $\text{sig}(m) \equiv m^d \pmod{n}$. RSA validation process is: $m \equiv C^d \pmod{n}$.

II. Shamir [t,n] Threshold scheme

The Shamir secret sharing scheme [7] is designed to divide the system's secret key into “n” pieces called sub-secrets and distribute them to “n” members for preserving. When any number less than “t” numbers of members put their sub-secrets together, the system's secret key can be recovered by calculating. However if the numbers is less than “t”, the system's secret key cannot be recovered in any case.

Assured a_0 is the system's secret key to be divided and distributed, select $t-1$ random numbers $a_1, a_2, \dots, a_{t-1}$ in the finite field $GF(p)$, then build a $t-1$ order polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{t-1} x^{t-1}$$

The identity information of each member D_i can be a polynomial in input, then $y_i = f(D_i)$, $i = 1, 2, \dots, k$, so get n pairs (D_i, y_i) . y_i is the sub-secret for member D_i and is distributed in secret channel to member D_i for saving. When any k numbers of pairs (D_i, y_i) are put together, the system's secret key a_0 can be recovered by Lagrange interpolation formula. For t pairs (D_i, y_i) , $i = 1, 2, \dots, t$, the $t-1$ order polynomial $y_i = f(x)$ can be uniquely determined, namely

$$f(x) = \sum_{i=1}^t y_i \prod_{i \neq j} \left(\frac{x - D_i}{D_i - D_j} \right)$$

The system's secret key a_0 can be recovered.

$$a_0 = f(0) = \sum_{i=1}^t y_i \prod_{i \neq j} \left(\frac{D_i}{D_i - D_j} \right)$$

4. IMPLEMENTING FULLY DISTRIBUTED CERTIFICATE AUTHORITY BY USING RSA CRYPTOGRAPHY

Our fully distributed CA is based on an approaches described by Luo and Lu in [2] and by Dawoud and Johann in [8]. In this section, we briefly describe their approach and point out corrections to their original algorithms. We propose a fully distributed certificate authority use RSA cryptography which it depend also on the covered of the sub-secret key when the nodes in MANET use the threshold $([t,n])$ to reconstruct the private key of MANET (SK).

To make the certificate for mobile ad hoc network the dealer who initiates the network has to follow steps:

- - Select two large prime number p, q and calculated $n = p \cdot q$ and compute $\varphi(n) = (p-1)(q-1)$.

- - Select the random number e as the public key of the mobile ad hoc network PK to satisfy the equation $\gcd(e, \varphi(n)) = 1$.
- - Compute the private key $d = e^{-1} \bmod \varphi(n)$ which satisfies the equation $ed = 1 \bmod \varphi(n)$.
- - Pick the public key and the private key for the mobile ad hoc network.

I. Initialization certificate authority

The dealer use Diffie-Helman key exchange protocol to initialize the certificate authority for the nodes in MANET

- Select two different large prime number w and z and calculate $T = w \cdot z$ and $\varphi(T) = (w - 1)(z - 1)$, and compute the primitive element g in the finite field F_T .
- Pick number v_0 that satisfy $\gcd(v_0, \varphi(T)) = 1$ after that compute h value which it satisfy the equation $v_0 h \equiv 1 \pmod{\varphi(T)}$.
- After that, the dealer initialize the coalition nodes $(D_1, D_2, \dots, D_n)$ and generate random value v_i as sub secret to satisfy the condition if $i \neq j$ then $v_i \neq v_j \neq v_0$.
- Compute $Q = g^{v_0} \pmod{T}$ and $X_i = g^{v_i} \pmod{T}$ values, so $q_i = X_i^{v_0} \pmod{T}$, where q_i is the calculated sub secret value for each node D_i in MANET.
- The dealer distributes sub secret value v_i to each node D_i through the secure routing and makes h, T, Q public.
- After that the dealer generates n - order polynomial followed by using Lagrange interpolation on MANET private key pair $(0, SK)$ and n pairs (D_i, q_i) .

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

According to the threshold scheme $[t, n]$ the dealer makes $n - t + 1$ numbers of coefficient $(a_t, a_{t+1}, \dots, a_n)$ public.

II. Reconstruction of the secret key (SK):

To reconstruct the secret key (SK) it needs at least " t " nodes in MANET $(D_1, D_2, \dots, D_t)$ with their sub secrets $(v_1, v_2, \dots, v_t)$ provided. The coefficient $(a_t, a_{t+1}, \dots, a_n)$ and public information h, T, Q is acquired.

In the “t” coalition of mobile nodes in MANET each node D_i ($i = 1, 2, \dots, t$) calculates $q_i = Q^{v_i} \pmod T$ and applies Lagrange interpolating on the point that “t” pairs $(D_1, q_1), (D_2, q_2), \dots, (D_t, q_t)$ then get the $t - 1$ order polynomial

$$f(x) = \sum_{i=1}^t q_i \prod_{i \neq j} \frac{x - D_j}{D_i - D_j}$$

where $f(0)$ is the secret key (SK).

III. Certificate Renewal

Since certificates are only valid for a limited time they need to be renewed before they expire. When a node D_i has to renew its certificate, cert requests a certificate renewal from a coalition of t neighbor nodes. Each node in this coalition checks that the old certificate has not already expired and that it has not been revoked. If it has been revoked, then the nodes ignore the request, otherwise the request is granted; each of these t server nodes generates a partial certificate with a new expiration date and returns it to node D_i . Node D_i then combines the t partial certificates to obtain its updated certificate cert-updated. If any of the nodes are compromised they may generate an invalid partial certificate, which they then send to the combiner. The certificate produced by the combiner will then also be invalid. The node will need to update its certificate with the new public key. If the node changes its private and public keys, this is accomplished in a similar way as the renewal of the certificate.

In another hand When the set of nodes $(D_1, D_2, \dots, D_n)$ is changed to $(D'_1, D'_2, \dots, D'_n)$ and the value from threshold is adjusted from t to t' that means all the MANET here need to be reconstruct. The dealer re-calculates the public information and the MANET shared secret will be updated. The sub secret v_i kept by the nodes is not need to be replaced D_i the dealer makes Lagrange Interpolation again on the point $(0, SK)$ and n' pairs (D'_i, q'_i) and calculate n' -order polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ and make $n' - t' + 1$ coefficients $(a_t, a_{t+1}, \dots, a_n)$ public.

IV. Certificate Revocation

The issued certificate can be revoked by very node if it believes that the certificate does not posses a valid user-key. Also the node can even revoke its public key if it believes it is compromised.

We propose two certificate revocation schemes: explicit and implicit.

In the explicit revocation scheme, the revocation of an issued certificate is made by an explicit revocation statement issued by the node. The user does not need to send the revocation to all the nodes because each node has a list of nodes that request updates for the certificates that it issued. So the revocation is sent only to the nodes that regularly update it. This certificate revocation will reach other nodes as well, but with a delay of the certificate exchange convergence time.

The implicit revocation scheme is based on the expiration time of the certificates. Each certificate contains its issuing time and a validity period (VP), which typically lasts several days. After this period passes, the certificate is not considered valid anymore. For this reason, it is very important to correctly assign the length of VP. Assuming that a node is able to establish communication with any certificate issuer at some time within a certificate validity period, that certificate updates will be exchanged regularly and nodes will be able to update their certificate repositories. If within the given period a node is not able to update some of the certificates in its updated local repository, the node can reconstruct it by using only the certificates available for update.

The described revocation schemes enable nodes to know the status of the certificates in their updated certificate repositories and to be informed, with some delay, of their revocation of other certificates. Key revocation grants users the possibility to perform authentication with a higher confidence in the validity of the certificates, but also in the correctness of the user-key bindings contained in the certificates because of their limited validity period and allows each user to react to any detected misbehavior by issuing a revocation statement.

Key revocation is based on the same scheme as for certificate revocation: If a node believes that her private key has been compromised, it revokes its corresponding public key by notifying the nodes that issued certificates to her. These nodes will then use the certificate revocation mechanisms to revoke the certificates that contain the public key in question.

We should also note that the nodes have strong incentives to maintain their updated certificate repositories, in order to provide sufficient proof of the authenticity of their public keys to other users and to be able to correctly authenticate other keys.

5. SECURITY OF THIS SCHEME:

The sub-secret here recovered by the value $q_i = Q^{v_i} \pmod{T}$ by using the Diffie-Hellman key exchange protocol. The v_i value is the only the secret to be kept by each node in MANET. The attacker wants to compute v_i by g^{v_i} or compute v_0 by g^{v_0} and then compute $g^{s_0 s_i}$ and this is very hard to make this for just one node in MANET because it depends on the discrete-logarithm problem.

In another part dynamic threshold secret sharing scheme $[t, n]$ is actually based on Shamir's secret sharing scheme, the security of the system's private key is assuming that there are no more than t service nodes captured. In this scenario, any $t-1$ calculated sub-secrets $(q_1, q_2, \dots, q_{t-1})$ will provide no information about the protected system's private $SK = (q_0)$.

It is impossible to be aware of any information of the system's private key by the cooperation between any $t-1$ nodes.

6. CONCLUSION

In Mobile Ad Hoc Network, it is convenient to establish a PKI and CA mechanism by using distributed key management schemes. This article proposes a fully distributed certificate authority use RSA cryptography which it depend also on the covered of the sub-secret key when the nodes in MANET use the threshold $([t,n])$ to reconstruct the private key of MANET (SK).

7. REFERENCES:

- L. Zhou and Z. J. Haas, Securing Ad Hoc Networks. IEEE Networks, Volume 13, Issue 6 1999.
- H. Luo and S. Lu, .Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks., Technical Report200030, UCLA Computer Science Department 2000[5] J-P. Hubaux, L. Buttyán and S. Capkun.
- Sarkar, B.Kishu, S.Mishra, M.S.Obaidat, "Chinese Remainder Theorem Based RSA - Threshold Cryptographyin MANET Using Verifiable Secret Sharing Scheme",IEEE International Conference on Wireless and MobileComputing, Networking and Communications (WiMob),pp. 258-262, November 2009.
- L. Ertaul and N. Chavan, "Elliptic Curve Cryptography based Threshold Cryptography (ECC-TC) Implementationfor MANETs", International Journal of Computer Scienceand Network Security, vol.7, No.4, April 2007.
- A. Amuthan, B.AravindBaradwaj, proposed Secure Routing Scheme in MANETs using Secret Key Sharing International Journal of Computer Applications (0975 – 8887) Volume 22– No.1, May 2011
- Y. Dong , Victor O. K. Li , Lucas C. K. Hui, S. M. Yiu introduced Dynamic Distributed Certificate Authority Services for Mobile Ad Hoc Networks This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.
- Shamir A. How to Share a Secret[J].Communications of the ACM,1979,24(11):612-613.
- Dawoud S., Johann van der Merwe,Fully Distributed Authority-Based Key Management for Mobile Ad Hoc Networks,www.iiis.org/CDs2012.