Aug 16th, 3:25 PM - 3:45 PM

Wireless Networks: Certificateless ID-based authentication using threshold signature for P2P MANETs

Aasia Samreen
University of Karachi, Pakistan

Seema Ansari
Karachi Institute of Economics and Technology, Pakistan

Certificateless ID-based Authentication using Threshold signature for P2P MANETs

Aasia Samreen and Seema Ansari

***Abstract*—As far as the security of MANET (Mobile And Ad Hoc Network) is concerned, it depends upon the secure authentication especially for P2P MANETs. Identity based encryption was introduced to construct Public Key without requiring a certificate. Therefore, certificateless authentication combined with threshold digital signature and efficient key generation using identities such as IP address, are the challenging issues in front of researchers. In this paper we have addressed the problem of identity based secure authentication employing well-known RSA algorithm and secret sharing to generate threshold signature on a message.**

Keywords- Certficateless authentication, Identity-based encryption, Threshold signature, P2P MANETs, Secret Sharing

I. INTRODUCTION

A MANET (Mobile Ad hoc Network) is a collection of mobile nodes having the features such as self-organizing network, the network without pre-existing infrastructure, scalability and specific application support etc. As these systems are mainly application driven, hence often referred to as P2P ad hoc networks [16]. The absence of a centralized control in such systems requires an efficient self-key management framework and secure authentication policy. However each node has equal functionality, some of them are designated as super peers to perform confidential tasks like key generation, key distribution and issuing certificates [11]. Identity based cryptography is a specific type of asymmetric cryptographic technology [5] and is introduced by Shamir in 1984. For P2P ad hoc networks where nodes join and leave the network as according to their need forming ad hoc groups that must be dynamically manageable and adjustable. Along with provided proactive security, ID-based signature and authentication schemes combined with threshold cryptography full fill the needs of security such as verification and non-pre-interactive communication. The disadvantage of ID-based system is "key Escrow". Researchers have proposed the following solutions to the problem.

1. *Use of multiple key pairs*: Proposed solutions require two pairs of private and public keys, (PK_1, SK_1; PK_2, SK_2). A user creates (PK_1, SK_1) in an ordinary way and SK_2 is generated by a KGC (Key Generation Center) with the help of PK_2 that contains user id and a link between PK_1 and PK_2. The idea is to split the information so that a malicious KGC cannot escrow the key.
2. *Use of multiple KGC's:* One can implement this solution either applying *Secret Sharing* or *Secret Aggregation*. In secret sharing master key or user privet key is distributed among *n* KGC's and *t* of them can recover the key. This technique requires unselfish co-operation between KGC's as well as dealing with dynamic changes in the system. In secret aggregation a user selects an arbitrary set of KGC's assuming that these KGC's do not have pre-communication or do not have trust relationship .The id of user is divided among selected set of KGC's and each part if id (say ID_i) is associated with individual KGC that creates ID-based private key corresponding to id share.

As the recent research has shown the growing popularity of MANETs as well as the problem associated with these networks such as efficient use of limited resources, bandwidth constraints, limited battery and low computational power. With these problems the certificate management (issued by a CA) and verification, especially if a chain of certificates exists, become an overhead. Therefore we recommend a certificate less framework for an ID-based authentication scheme to provide secure and efficient transactions among mobile peers. Our proposed framework emphasizes on ad hoc groups management providing user authentication with threshold digital signatures and ID-based key management.

The paper is organized as follows: in section II related work has been mentioned, section III gives some preliminary details about secret sharing and other relevant techniques, section IV describes the proposed scheme while V presents performance analysis. The section VI gives the conclusion and the future perspective

II. RELATED WORK

The increasingly use of wireless and ad hoc networks has attracted the electronic community to develop and share the various applications for P2P MANETs. Secure authentication is one of the biggest challenges for researchers to bend their attention towards it [11]. Specifically, in ad hoc networks authentication means to provide corroboration of the peer identity in an association, using digital signature. The well-known PKI (Public Key Infrastructure) is unsuitable for ad hoc networks as

Aasia Samreen is with Department of Computer Science, University of Karachi, Pakistan. (Email: asiasamreen@yahoo.com)

Seema Ansari is with Karachi Institute of Economics and Technology, Pakistan. (Email: sansari@pafkiet.edu.pk)

978-1-4244-4609-4/09/$25.00 ©2009 IEEE

compared to wired networks, as it involves complex computations to grant or verify a certificate, which is issued by a certificate authority. Consequently, IBE (ID-Based Encryption) systems were introduced where public key reflects the id of a user for example user name, email address or any arbitrary number that makes verification simple and eliminates the need of a CA. Various schemes [1,4,5,6,8,10,11] are proposed to implement ID-based cryptosystems. To cope with key exposure problem [5] has proposed threshold cryptography based scheme in which at least *k* out of *n* helpers are required to update temporary private key. As these schemes follow the paradigm "key insulation" that uses the concept of division of time span into discrete intervals so that temporary private key is refreshed at every period T_i and can be applicable for the corresponding period only. To reduce computational cost and to provide easy authentication for multi-domain ad hoc networks Fagen Li et al [17], proposed a multi-PKG's environment with the provided public verification and resistance against forging attack. A threshold signature scheme uses secret sharing, which was first introduced by Shamir's [9] in 1979. V. Shoup [15] gives the idea of threshold signature scheme providing unforgeability and robustness in random oracle model with the assumption that the RSA problem is hard. The scheme works as, the dealer generates public key and private key along with verification keys. The combiner takes PK (Public key), VK (Verification key) and SK_i (private key share) as the input and runs verification algorithm for SK_i and if the validity of Sk_i is proved, it runs then combining algorithm that takes *k* valid signature shares and outputs a valid signature on message m. To emphasize on the role of RSA in construction of secure ID-based systems [3,4,15] describe the functionality and correctness along with robust solution of threshold RSA based schemes to compute threshold signatures. An enhanced version of Shoup's scheme is proposed by Rosario et al [14]. The scheme claims for efficient and non-interactive communication in MANETs considering the requirement of dynamic admission and departure of nodes in a network or in the existing ad hoc group and designed an enhanced RSA (modified version of Shoup' scheme) based threshold signature. Certificateless or the ID-based authentication schemes arise the issue of robust digital signature formulation and related problems such as anonymity of a user, multi-signature for multi-agent system, key escrow and key exposure. All [8,10,11] have provided the solutions to these problems.

III. PRELIMINARIES

This section of the paper discusses the issues regarding authentication such as threshold signature schemes, threshold secret sharing and RSA public key cryptography.

A. Threshold digital signature.

Threshold signatures are part of a general approach known as *Threshold Cryptography* that specifically focuses on providing efficient and practical solutions for specific signature schemes. To unfold the depth of threshold signature we first define some basic techniques.

Threshold Cryptography: Threshold cryptography presents the idea of the distribution of the secret key in such a way that a secret key is stored in a shared form among several parties to make forging more difficult than a single-owner storage for secret key [14]; as only a coalition of cooperative parties can jointly recover the key. Threshold cryptography based schemes mainly follow the two steps *sharing* and *computation*. In sharing a trusted dealer distributes the shares sk_i of private key *SK* among *n* parties and then erase the key from its memory. In computation step any *t* parties or more can perform some operation jointly to compute *SK* whereas, no coalition of *(t-1)* or fewer parties can perform the same operation.

Secret Sharing: Secret sharing was introduced by Shamir's [9], which plays a role of backbone for almost all threshold schemes. This scheme is based on polynomial interpolation to divide a secret *S* into *n* pieces, following the steps given below:

- A TD (Trusted Dealer) chooses a large prime *q* and a random polynomial over Z_q of degree *k-1* such that *f(0)=S*. (Where q > S and q > n)
- TD computes $ss_i = f(i) \bmod q$, where ss_i is the secret share for user *Ui* which is then transmitted to *Ui*.
- Any *k* users reconstruct the secret by computing

$$f(z) = \sum_{i=1}^{k} ss_i l_i(z) \bmod q$$

Where $l_i(z) = \prod_{j=1, j\neq i}^{k} \frac{z-j}{i-j} \bmod q$, is the Lagrange coefficient. Thus, finally secret *S* can be computed as

$$S = f(0) = \sum_{i=1}^{k} ss_i l_i(0) \bmod q \qquad \therefore f(0) = S$$

This shows that *S* can be computed only if at least *k* shares (ss_i) are combined. Some other versions of secret sharing are as follows:

JJS (joint Secret Sharing): It is an extension to SSS that removes the need of a trusted dealer, rather it gives the idea of sharing the polynomial *f(z)* over *Zq* in such a way that each user U_i selects $f_i(z) \varepsilon Zq$, computes shares for other users and finally with the help of received shares, receiver can compute his own share.

JZSS (Joint Zero Secret Sharing): This scheme is often known as *proactive secret sharing*, in which for different intervals of time individual shares are refreshed without affecting the group secret defining another polynomial *g(x)* Such that *h(0)=f(0)+g(0)=S* .

VSS (Verifiable Secret Sharing): This scheme provides a mean to verify the correctness of the received share at reconstruction time of secret *S*. Verifiable secret sharing is often used to check dealer or participants cheating while generating and distributing the sub-secrets.

A threshold digital signature is generated on a message *m* by *t* players using (*t*,*n*) threshold scheme where *t* is predefined threshold value.

To clarify the concept we have given some definitions

Definition: A *digital signature* σ is a bit pattern following an authentication mechanism, attached with a message and can be recognized and verified by a receiver or a third party.

Definition: To divide secret *S* among *n* players such that *S* is easily reconstructable from any *k* shares but complete knowledge of even *k-1* shares do not reveal any information about secret, is known as *threshold secret sharing*

Definition: A *threshold signature* on message *m* is produced by $t<n$ parties with the condition that each one generates a partial signature (using its private key share; sk_i) and then all are combined to compute a valid signature.

Definition: A threshold signature scheme (Thr-key-gen,Thr-sig,ver) comprises of secret key sharing phase, threshold signature computation phase and verification of signature on message *m* by *t* parties out of *n* parties.

B. RSA algorithm.

The most important aspect of the RSA algorithm is the pair of keys, which have a particular mathematical form in which the modulus *n* is obtained as the product $n = pq$ of two prime numbers *p* and *q*. If $\varphi(n) = (p - 1)(q - 1)$ then for a given *n,* the public key component *e* can be chosen such that $e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$. The secret component *d* corresponding to *n* and *e* is obtained by calculating the inverse of *e* as*:* $d = e-1 \bmod \varphi(n)$

RSA signature: A signature on message m generated with the help of RSA, can be computed as follows:

- Node A generates e_A,d_A and n_A then sends public key (e_A,n_A) to Node B.
- A sends message *m* along with signature σ to B after signing the message following given two steps
  Calculation of hash: $h=H(m)$
  Sign the message: $\sigma=h^{dA} \bmod n_A$
- To verify signature B calculates
  I. $h=H(m)$
  II. $h`= \sigma^{eA} \bmod n_A$
- if $h=h`$ then B accepts signature as the valid signature.

To make the implementation of RSA algorithm secure, at minimum all the related data should be erased after using it as if an adversary reads from memory it can disclose the secret.

IV. PROPOSED SCHEME

To overcome the problem of single point failure we have proposed a distributed master key pair [11] scheme combined with the threshold RAS cryptosystems.

A. Communication model

We are assuming that there are two types of participants, system participants VMN's (Virtual Monitoring Node) and

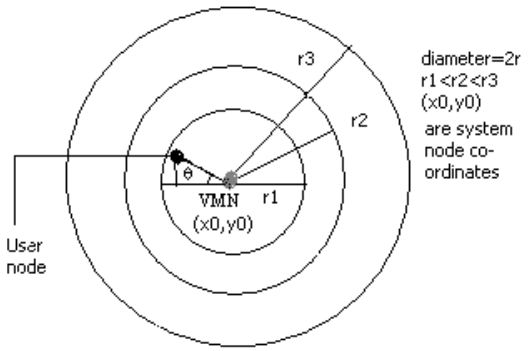

Figure 1: Adjustable range to support mobility.

user participants or UN (User Node) or simply user U_i. A VMN is further categorized as WVMN (Working Virtual Monitoring Node) and SVMN (Silent Virtual Monitoring Node). WVMN is the functioning system node that performs a role of central head for the ad hoc groups. If we divide the whole distributed environment into groups or sub domains then there will be N_s system nodes including helper nodes (SVMNs), which are to keep replica of important data and prevent from failure or accidental crash of WVMN.

To provide mobility to nodes a flexible communication range is defined by concentric circles having radius r_1, r_2 and r_3 respectively. As shown in figure 1, if somehow the number of user nodes is less than a threshold (Defined by network administrator) the range is increased to next predefined point from the central point. This assumption is due to the fact that in MANETs parties can join and leave the network at any time. If VMN needs to communicate with node Ui at some distance in θ direction then these two nodes will be able to communicate, if the following inequality holds:

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} < TR$$

Where TR= the maximum transmission range.

Direction and position of node for any radius *r* can also be calculated using polar co-ordinates if either is known.
$X=r \cos \theta$, $Y=r \sin \theta$, and $\theta=\tan^{-1}(y/x)$

B. Initial Setup.

As our scheme is an ID-based scheme for ad hoc groups where each group has a system participant node known as WVMN. Master key pair (PK,SK) is generated in such a way that SK is shared among all user nodes. Each user has an id and to get its private key, *t* out of *n* WMNS collaboratively compute shares and with the help of those shares user private key *sk* is computed. Public key (PK) is denoted by (N, e) where $N = pq$ and p, q are large primes of the form $p = 2p' + 1$, $q = 2q' + 1$, further $m= p'q'$. Where p', q' are also prime numbers. The value *e* must be chosen as a prime larger than any possible identity [14].

C. ID-based key generation

To get a public key for encryption a user Ui selects an identification number (IP address, email address, phone number or any other number that may be integer) and sends to the VMN that performs the following steps.

- Designated VMN checks out the validity of the received identity.
- If validity is confirmed, some public information along with time stamp are appended to that id and the hashed identity is calculated as
  $HID_i=h(ID_i \,||\alpha||T)$
  Where α is common public parameter, T is the time stamp from which an expiry of id can be calculated. HID_i is the hashed id calculated using one way hash function $h()$.
- User Ui's public key $pk=e_i$ is calculated as
  $e_i=f(HID_i)$

Note that the recipient's public key certificate is not required for the sender to encrypt since the key is derived from the receiver's unique identifier. Another aspect is that the public key of user contains some specific information (only known to user), which is kept hidden so there is no chance of stealing the ID

D. Threshold signature generation

In threshold signatures for MANETs we would like any client to be able to make at any time an ad hoc selection of a subset K of user nodes from which client can request a threshold signature with the help of VMN. Given this selection, a regular (t, n)-threshold signature should be sent from the virtual node to the client, where $n = |K|$ and t are the size and threshold parameter chosen by the client. To generate a threshold signature using threshold RSA as proposed by [15] the following steps are required.

Private key sharing: A WVMN computes $d=e^{-1} \bmod m$ to distribute it among users. It further selects t random $a_i \varepsilon Zm$ for $i=1,2,\ldots\ldots t$ and a polynomial $f(z) = a_0+a_1z+a_2z^2+\ldots. + a_tz^t$ where $a_0=d$. Each user Ui gets a share of private key $di=f(i) \bmod m$ with the condition that there are maximum n users in the systems and $\Delta=n!$.

Signature computation: For a message m user $Ui \ \varepsilon \ |t|$ computes signature σ_i for $y=h(m)$ as $\sigma_i = y^{2\Delta.di} \bmod N$ where $h(m)$ is hash of message using one way hash function and 2Δ is taken on the basis of discrete logarithm assumption. R Gennaro et al.[14] identifies that for IDs containing long integer computation of Δ becomes infeasible. He has proposed a modification that instead $\Delta=n!$ for k bit numbers $n=2^k$ is the better choice and commutes signature $\sigma_i = y^{2^{kt}.di} \bmod N$. The computation of $\sigma = y^d \bmod N$ using all partial signatures is completed in two steps first the computation of σ' for all $\sigma_{i1},\ldots. \sigma_{it+1}$ and then σ is computed using σ'.

$$\sigma' = \prod_{j=1}^{t+1} \sigma_{ij}^{\ \Delta s.Ls(0)} \bmod N$$

where $S=\{i_1,\ldots\ldots i_{t+1}\}$, $\Delta S = lcm\left\{ \prod_{j\in S, j\neq i} (i-j) : i \in S \right\}$

and Ls(0) is the Lagrange co-efficient (see section III)

$$\sigma' = \prod_{j=1}^{t+1} (y^{2^{kt}.di})^{\Delta s.Ls(0)} \bmod N$$

$$\sigma' = (y^{\Delta S.2^{kt}})^{\sum_{j=1}^{t+1} Ls(0).dij \bmod m} \bmod N$$

$$\sigma' = y^{\Delta S.2^{kt}.f(0)} = y^{\Delta S.2^{kt}.d} \bmod N$$

now σ can be calculated from σ' using extended Euclidean algorithm defining $ae+b(2^{kt}\Delta S)=1$

$$\sigma = y^a (\sigma')^b \bmod N$$

$$\sigma = (y^{1/e})^{ae}.(y^{1/e})^{b2^{kt}\Delta S} \bmod N$$

$$\sigma = y^{1/e} \bmod N$$

a, b are computed using Extended Euclidean algorithm with the e satisfying the condition $GCD(e, 2^{kt}\Delta S)=1$.

E. Authentication process

In our model the private key SK is shared among all users such that each U_i is having its share sk_i while public key is selected by user and after a necessary verification is assigned to user. When user node U_i wants to communicate with node U_j, it has to contact with at least t nodes out of n. All users when received a request of authentication along with a message m to be sent to U_j, each one generates a partial signature using its share of private key sk_l for $l \ \varepsilon \ |t|$ $\sigma_l = h(m)^{sk_l} \bmod N$ and sends back to U_i or combiner to compute the complete signature on m using partial signature. U_i then sends m with signature σ to U_j who can verify the signature as: $\sigma^e = h(m) \bmod N$ using U_i's public key and decrypts the message with its private key. For a new node that wants to join the ad hoc group the registration process is performed and public key is assigned. Again the group head or the WVMN computes his secret key share $sk_{new}=f(z) \bmod m$ which is then transmitted to U_{new}.

V. PERFORMANCE ANALYSIS

This section presents some required features for such authentication scheme as one we have proposed with the help of adapted threshold RSA signature.

Threshold property: Only a quorum of t or more authorized group members are able to co-operatively generate a valid signature. This property also defines the unforgabilty characteristic for the scheme as if, for instance $t-1$ members are compromised then still the secret message remains secure.

Correctness: This property is related to threshold signature and it reflects the fact that a threshold signature generated by a group on message m must be publicly verifiable, which is quite true for our designed scheme.

Verifiability: Any outsider can learn the identities of the individual signer without any interaction. This shows that the signers are publicly recognized with public information. In our case it becomes easier to identify a malicious user by their individual signature fragment while anonymity for honest user is always there due to hashed identity to keep identities hidden.

No Certification: An ad hoc network is a collection of autonomous nodes having no pre-existing infrastructure that communicate with each other by forming groups dynamically. The property of not relying on the support, from any fixed infrastructure makes it useful for specially a P2P MANET. Therefore, our model consists of various group heads or cluster heads or WVMNs who are responsible to do key management function in a threshold manner. A VMN confirms the validity of a user ID that is converted by applying some security parameters, into user public key. Hence user public key does not require any certificate rather it is a function of a predefined (by user) user id.

Non interactive: Given a message and its share of the secret key, each user node locally computes a "signature fragment" without any interaction with the other users. Then a combining algorithm is run by user node or system node (WVMN) to compute the resultant standard signature.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have proposed an identity based authentication scheme for P2P MANET. This scheme is designed for multi-domain environment where each domain is monitored by a system node (WVMN) along with a helper system node (SVMN), which is for replication and load balancing purposes. We have employed threshold cryptography to distribute private key among user nodes (U_i) to make authentication more secure by posing a condition that at least *t* users out of *n* (n is the total number of users in the group at any specific time period) should generate a complete signature using all the *t* partial signatures. Keys generation and signature computation and verification has been performed using RSA algorithm in threshold manner. Our model is similar to 2-redunt super peer model, which is easily extendible into k-redundant model for large groups.

In the future we are planning to investigate an authentication scheme for P2P MANET where system participating nodes share a master network key and will produce a user private key with their honest co-operation

REFERENCES

[1] L. Chen. An Interpretation of Identity-Based Cryptography. *In A. Aldini and R. Gorrieri (Eds.): FOSAD 2006/2007, LNCS vol 4677, pp. 183–208,Springer, Heidelberg 2007.*

[2] D. D. Vergados and G. Stergio. An Authentication Scheme for Ad-hoc Networks using Threshold Secret Sharing. *Wireless Pers Commun (WPC'07) vol 43 ppt. 1767–1780, Springer* 2007.

[3] G. Yaun-ju. Verifiable threshold signature schemes against conspiracy attack. *In ISSN 1009-3095 journal of Zhejiang University SCIENCE vol 5, pp 50-54, 2004*

[4] E. Yoon and K. Yoo. Improving the ID-Based Key Exchange Protocol in Wireless Mobile Ad Hoc Networks In T. Kunz and S.S. Ravi (Eds.): ADHOC-NOW 2006, LNCS vol 4104, pp. 349–354, Springer Heidelberg 2006

[5] J. Weng, S. Liu, K. Chen, D. Zheng, and W. Qiu. Identity-Based Threshold Key-Insulated Encryption without Random Oracles. *In T. Malkin (Ed.): CT-RSA 2008, LNCS, vol 4964, pp. 203–220. Springer, Heidelberg* 2008

[6] Y. Yu , B. Yang and Y. Sun. ID-Based Threshold Signature and Mediated Signature Schemes. *In Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD-07).*,2007.

[7] M. S. Hwang , S. F. Tzeng, and C. T. Li. A Fully Distributed Proactively Secure Threshold-Multisignature Scheme. In *IEEE Transaction on Parallel and Distributed Systems, VOL. 18, NO. 4, APRIL* 2007

[8] W. Chen and F. Lei. An Efficient Multi-sender Identity Based Threshold Signcryption with Public Verifiability. In *Eighth International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2007.

[9] A. Shamir,.How to Share a Secret. *Communications of the ACM*, Vol. 22, No. 11, pp. 612-613, November 1979.

[10] A. Saxena. Threshold SKI Protocol for ID-based Cryptosystems. *In Third International Symposium on Information Assurance and Security(IAS'07),* 2007.

[11] H. Deng, A. Mukherjee, and D. P. Agrawal. Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks. *In Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04),*2004.

[12] F. Li, J. Shang and D. Li. A Proactive Secure Multi-secret Sharing Threshold Scheme. *In Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel Distributed Computing ,* 2007.

[13] L. Ertau and N. J. Chavan. Elliptic Curve Cryptography based Threshold Cryptography (ECC-TC) Implementation for MANETs *In IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.4, April 2007.*

[14] R. Gennaro, S. Halevi, H. Krawczyk, and T. Rabin. Threshold RSA for Dynamic and Ad-Hoc Groups. *N. Smart (Ed.): EUROCRYPT 2008, LNCS 4965, pp. 88–107, Springer, Heidelberg* 2008.

[15] V. Shoup. Practical threshold signatures. *In: Preneel, B. (ed.) EUROCRYPT 2000.LNCS, vol. 1807, pp. 207–220. Springer, Heidelberg* (2000)

[16] M. Gerla, , C. Lindemann, and A. Rowstron,P2P MANETs – New Research Issues.*In Dagstuhl Seminar Proceedings 05152.Perspectives Workshop: Peer-to-Peer Mobile Ad Hoc Networks - New Research Issues* 2005

[17] F. Li1,, Y. Hu1, and C. Zhang.An Identity-Based Signcryption Scheme for Multi-domain Ad Hoc Networks .*In J. Katz and M. Yung (Eds.): ACNS 2007, LNCS vol 4521, pp. 373–384,Springer Heidelberg* 2007