ADVANCED SECURITY FOR MANETS USING THRESHOLD CRYPTOGRAPHY

H. Ateeq Ahmed[1], C. Mohammed Gulzar[2], S. Imran Pasha[3]

[1]*Asst. Professor, Department of CSE, Dr. KVSRIT, AP, India*
[2]*Assoc. Professor, Department of CSE, Dr. KVSRIT, AP, India*
[3]*Asst. Professor, Department of CSE, Dr. KVSRIT, AP, India*

Abstract

The development of technologies such as Mobile and Adhoc networks have made the distributed environments widely accepted as they allows large scale support for resource sharing infrastructure. One of the challenging issues for such environments is secure authentication. We considered the role of threshold cryptography to provide advanced security for the MANETs, revealing the authorization process using threshold digital signature, proxy signature and multi-signature in ID-based and CA-based structures. In this paper after taking a review of various proposed schemes, problems and attacks for MANETs and their solutions, In order to make any system secure, the security services such as authentication, confidentiality, integrity, availability and non repudiation must be satisfied. However, in case of distributed environment, separate and advanced security techniques have to be implemented. As mentioned earlier, one the major challenge that needs to be addressed is security of authentication. We conclude some issues and determine some challenges that can take place in future.

Keywords: *Threshold signature, Proxy signature, Advanced threshold cryptography, Threshold multi-signature.*

----------***----------

1. INTRODUCTION

The recent study has shown the importance of distributed cryptography in securing MANET's (Mobile and Ad Hoc Networks) due to open nature of such systems. With the growing fame of ad hoc networks their scalability, dynamic and accommodating nature, distributed operations to perform a task using distributed resources in a decentralized manner, Bandwidth constraints and lack of infrastructure presents many dangers regarding security for interactive or non interactive communication. Amongst them the most important difficulty is how to authorize a user to use the resources and whom to be authorized? This paper investigates and surveys some of authentication schemes from the area of Threshold Cryptography to find out the solution for the problem.

Threshold cryptography is the ability of chopping a secret for security purposes It offers improved security while authenticating a user than non- threshold cryptographic schemes for the following reasons.
1) Distribution of key: The group secret key is distributed among all members using a *(t, n)* threshold scheme, so that any subset of at least t current members can produce a valid signature.
2) The single CA (Certificate authority) will be vulnerable as if the single CA is compromised then the entire network security will be crashed. Threshold cryptography provides the idea of distribution of CA's functions.
3) Threshold multi-signature schemes providing secure authentication, satisfy the following properties [4,6,7]

- Correctness: The group-oriented signature is verifiable
- Unforgeability: Only a quorum of t or more than t authorized members can generate a valid signature.
- Traceability: Any member who participating in signing process can be identified publicly, hence individual signature cannot harm the system by any adversary attack.
- No authentication: No subset of t users can sign on behalf of any other t users.
-Prevention against malicious attacks: Threshold cryptography provides a strong binding between secret sharing and generating so that the threshold signature scheme cannot be breakable even if the system is under attack.

This paper presents the process of authentication for various situations, related problems and issues, future challenges and currently used approaches, found in the literature in the light of Advanced threshold cryptography.

The paper is organized as follows: in section 2 the process of authentication using Threshold cryptography is described, in section 3 issues and problems have been discussed, section 4 describes our solution to the addressed problems and section 5 discusses some important security problems. Finally, the section 6 gives the conclusion.

2. AUTHENTICATION USING KEY SHARING

Particularly, in ad hoc networks authentication means to provide validation of the peer identity in an association, using digital signature. A common principle of security engineering is that one should not rely on a single line of defense, so researchers propose the sharing of secrets. In secret sharing, the secret is first shared among the parties who later reconstruct it while in Threshold Cryptography the secret is assumed as a shared input to a cryptographic

computation, it is never reconstructed rather computed providing security against forging and exposure of private keys etc. For secure authentication the digital signature is computed in a distributed way based on the shares of secret key, therefore taking idea of secret sharing from Shamir's secret sharing scheme [1] the idea of Threshold signature was developed and applied to MANETs following the procedure in the below given definition.

Definition: A threshold signature scheme (Thresh-Key-Gen, Thresh-Sig, Ver) is t-secure (with parameters (T,k), if no t-adversary A that runs in time T can produce a signature on any message M without the participation of at least one honest party, except with probability

Thresh-Key-Gen: is a key generation protocol carried out by a designated dealer to generate a pair (Pk, Sk) of primary and private keys.

Thresh-Sig: is the distributed signature protocol. The output of the protocol is a signature Sig on message M.

Ver: is the verification algorithm on input M, Sig, and Pk, checks if Sig is a valid signature of M under Pk.

2.1 Overview of Secret Sharing

The idea of secret sharing is to divide a secret S into pieces, distribute them into users who pool the shares to reconstruct secret S when required. A well-known scheme is Shamir's secret sharing scheme, which is based on polynomial interpolation. A dealer shares a secret among n users in the following way:

Trusted dealer chooses a large prim q and at random a polynomial $f(z)$ over Zq of degree t such that $f(0)= S$. The dealer computes each user's share SS_i such that $SS_i = f(i) \bmod q$ then secretly transmits SS_i to each user. After receiving shares, any group of t members can recover the secret with the help of their shares using LaGrange Interpolation formula:

$$f(z) = \sum_{i=1}^{t} SS_i \, l_i(z) \bmod q$$

Where,

$$l_i(z) = \prod_{j=1, j\neq i}^{t} \frac{z-j}{i-j} \bmod q$$

Since $f(0)=S$, the shared secret can be computed as:

$$s = f(0) = \sum_{i=1} SS_i \, l_i(0) \bmod q$$

Thus t shares give no information about S while t+1 shares completely define S, via polynomial interpolation. An extension to Shamir's secret sharing scheme is known as Joint Secret Sharing Scheme it uses no dealer rather group members collectively choose shares, in that case the polynomial is itself shared such that f(z)= f1(z) + . . . +fn(z) where fi(z) is the polynomial of user Ui over Zq . It is assumed that all n users are agreed on q, the joint secret is computed following the steps given below.

- User U_i chooses at random a polynomial $fi(z) \in Zq$ of degree $t-1$ such that $fi(0)=S_i$.
  Let $fi(z) = f_{i0}+f_{i1}z+\ldots+f_{it-1}z^{t-1}$ $(mod\ q)$, where $f_{i0}=S_i$
- U_i computes U_j's share $SS^i_j = fi(j)$ then sends it to U_j through a secure channel
- User U_j computes her share SS_j of the secret after summing all the received shares ;

$$SS_j = \sum_{i=1}^{t} SS_j^i$$

Secret Sharing is also used for proactive secret sharing to change the individual secret shares(after a limited time) of the user U_i without changing the group secret. If the polynomial is $f(z)$ such that $f(0)=S$ and there is another polynomial $g(z)$ such that $g(0)=0$, then by adding them we can get the same secret as: $h(0)=S=f(0) + g(0)$. Against the malicious intention of users another technique of secret sharing is designed known as *Verifiable Secret Sharing.* VSS generates share for each user U_i, then these shares are sent to each user with an element know as w*itness* for verification purpose.

2.2 Overview of Threshold Signature

Informally, a digital signature is used for authentication, as it must verify the author and the Date and time of signature. It is an informative tag produced by a party A which is then appended to a message such that any other party can verify the tag as a valid signature by A, and another party C cannot produce a tag for a different message that can be verified as a valid signature from A. Threshold cryptography uses various different forms of digital signature we will give a brief description of such signatures.

Threshold Digital Signature: This is a (t, n) distributed signature scheme. There are n members each one is having a sub part of secret key and for the given message m at least t+1 or more honest members are required to generate a valid signature on m.

ID-based Threshold signature: A user submits his identity information ID to KGC. KGC selects Zp and computes the user's public key as QID = H2(ID), and returns SID = sQID to the user as his private key. Each user Ui sends back partial signature to DC (Designated combiner), after signing the message. DC Combines the partial signatures and constructs a valid threshold signature.

Threshold proxy Signature: In a (t,n) threshold proxy signature scheme, the original signer can delegate his/her own signing capability to a group of n proxy signers such that t or more of them can generate proxy signatures cooperatively, but t-1 or less of them cannot do the same thing in a way that the following requirements are satisfied
1) *Unforgeability*: No third party who is not designated can create a valid proxy signature.
2) *Verifiability*: A recipient can verify the received proxy signature.

Threshold Multi-signature: Threshold-multi-signature schemes combine the properties of threshold group-oriented signature schemes and multi-signature schemes to yield a signature scheme that allows a threshold t or more group members to collaboratively sign an arbitrary message providing that every signer can be identified.

3. SOME IDENTIFIED PROBLEMS

This paper discusses the issues regarding threshold signature schemes such as threshold multi-signatures partial signatures, proxy signature and takes a comprehensive look at the problems that occur during the process of authentication or after the authentication.

3.1 Communication over MANET with the Problems of Lack of Infrastructure and Central Authority

A Mobile Ad hoc Network (MANET) provides cooperatively sharing of resources infrastructure. These networks, due to their lack of physical infrastructures or centralized authorities, pose a number of security challenges to an authentication protocol designer [1,3]. A centralized solution employing servers can easily be compromised, leaving the nodes exposed to threats by malicious peers [2].

3.2 End-to-End Authenticity for Ad Hoc Networks Using Threshold Cryptography

As these networks are operated on highly unsecured wireless medium, secure authentication scheme is the major requirement for communication [2]. For such networks where mobility of nodes and extension are the basic requirements, the problems related to authentication using Threshold cryptography like public key management and private key share acquisition and computation are also big challenges regarding security.

3.3 Exposure of a Secret Key, and Key Management

The most dangerous attack on Cryptosystems in insecure, especially identity based encryption environment (like mobile systems) is Key-Exposure [5]. Secret key issuing process for ID based systems suffers from key escrowing and also requires a secure channel to issue the private key. Another problem related to keys management is that any t users may impersonate other t users' signatures without taking any responsibility.

3.4 Problems with Setting up a Proactive Secure Multi-secret Sharing Threshold System

Malicious users can harm the system even using Threshold signature scheme. A natural method to prevent from them is to periodically refresh the secrets; however, this is not always possible. Suppose that someone wants to protect a data file by encrypting it under an initial key and then periodically updates that key, he should decrypt the file with the old key and encrypt it with the new key every time when the key changes, such method doesn't protect the integrity of the file at all, and it also exposes the secrecy to adversary when the file is being decrypted.

3.5 Proxy Signature on Behalf of an Original Signer

In a proxy signature an original signer delegates a user called proxy signer to sign message on behalf of the original signer in the case of his absence or large amount of work. The proxy signature generated by proxy signers for a message on behalf of an original signer can be misused as, an adversary can forge an illegal proxy signature for any message seemed to be generated by proxy signers on behalf of this adversary himself. The actual signer can attack on the system using its own-made proxy signature, therefore a flawless scheme is required limited resources do not allow any extra burden for MANETs that is why Threshold cryptographic solutions may not be suitable for most commercial ad hoc networks environments, as it involves additional computationally intensive modular exponentiations as compared to the asymmetric-key cryptographic protocols [3]. So an authentication scheme must also be very precise and easier to implement with reasonable storage capacity.

4. OUR SOLUTION

There are various methodologies adopted which are given below.

4.1 Solution to One Point Failure & Nodes Authenticity

The use of a single CA (certificate authority) will be the vulnerable point in an Ad-hoc network , therefore the idea of distribution of CA is used that is *K* out of *N* nodes are required to take the action. Parameters *N* and *K* can be selected in such a way that the number of CA nodes in the network is adequate to provide robust certification services. Therefore gives a distributed self-organized CA, which does not rely on any central or external authority. To make threshold signature scheme more secure against malicious acts, [1] proposed the verifiable IP-address binding with public key. Each square region has a specific number of nodes=N. Author claims that this IP-bound threshold signature scheme not only provides a user simultaneous message authentication but also implicit public-key authenticity. The best authentication scheme is one with threshold cryptography and distributed CA capabilities [2].
The scheme proposed by [2] defines a rectangular topology, as given in figure 1, which assumes uniform distribution of the nodes in the smaller square region. Suppose that the coordinates of two mobile nodes are (x1, y1) and (x2, y2) respectively. These two nodes will be able to communicate, if the following inequality holds:

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

where RN= the maximum transmission range.

4.2 Key Disclosure and Key Management Solution

There are two schemes for key management PKI (Public Key Infrastructure) which is CA-based and another is ID-based introduced by Shamir in 1984. ID-based systems can be a good alternative for CA-based systems from the viewpoint of efficiency and convenience. It uses the identity of user as public key and computes the private key as the function of public key; moreover user's credibility and trust management can omit the need of a secure channel. . CA-based key distribution schemes have some drawbacks such as certificate validity and verification. Proposes id-based scheme for keys management using elliptic curve groups and bilinear maps, scheme works as a KGC register the new user and maintain a data base for necessary details.

User can select any t+1 out of n KPAs (Key Privacy Authorities) to obtain all partial keys to compute private key. IBTKIE (Identity-based Threshold Key Insulation Encryption) is another time based key management scheme proposed by [5].in this scheme for a certain time duration at least *k* out of *n* helpers are needed to update the user's temporary private keys. Combining at least *k*ID key update information shares with one temporary private key corresponding to another period *t'*, user ID can derive the temporary private key for the current period *t*. Distributed key when used for jointly such as for conferences can be constructed as mentioned above.

4.3 Solution to Proactive Multi-Secret Sharing Threshold Schemes

For threshold multisecret sharing two schemes are in use CA-based and ID-based as proposed by. CA-based scheme requires a secure channel to issue certificate while identity based needs a lot of computational work. Using the concepts of bilinear pairing, distributed key generation and joint Pedersen verifiable secret sharing scheme [8] proposed the solution related to problems of security in open networks. A proactive secure scheme based on discrete logarithm DKMI (Distributed Key Management Infrastructure) is introduced in [7] that consider secret distribution, updating and redistribution using DKRU that solves the problem of the faulty share holders by identifying them in first round.

4.4 Solution to Proxy Signature Problem

For a valid Proxy signature, two or more proxy signers out of n can cooperatively produce it presents the security analysis of an ID based solution for forgery attack and shows that the scheme has some flaws however after correcting a new solution can be designed gives another solution based on KC-scheme making use of RSA and Lagrange interpolation to generate the proxy signature. A verification is performed for valid proxy signer to make scheme more secure and robust. Another solution is proposed in [6] to overcome the problem for an attack by original signer. The scheme works as the original signer say P0 chooses shares for each member in the proxy signer group and send them via a secure channel, P0 then selects time duration and divides it into short periods and generates secret shares with some useful information like public key valid delegation period etc, for these periods. Upon receiving these shares, proxy signers compute individual proxy signature send them back to designated clerk who after verification compute the signature and then a verification is performed using parameter ASID which shows the actual signer id. For the scheme if attackers try to forge or calculate the private information from public information it's not possible due to provided computation security using discrete logarithm.

Table -1: Key sizes in bits for equivalent levels

Symmetric	ECC	RSA
80	163	1024
128	283	3072
192	409	7680

5. SECURITY PROBLEMS

For MANETs, there are several security related issues. The security solution for MANETs is to provide security services such as Confidentiality, Integrity, Availability, and Non-Repudiation. We describe and discuss about these major security issues taking cryptographic techniques under consideration.

Authentication: To identify a node or user in ad hoc network, secure authentication is required. The basic objective is to save honest users from being cheated and to prevent impersonation. Digital signature is the technique which is used for the purpose effectively. A signature is shared among users and regenerated when needed, is the basic idea behind threshold signature schemes. But sometimes a user grants the signing authority to another user as we have observed in proxy signature which is a threat for other users. Another potential threat is, if a group of malicious user attacks collusively such as n users impersonate the other n user's signature could harm the smoothness of system until it shall be resolved. For this purpose CA and ID-based schemes based on threshold cryptographic primitives have been designed. Either CA assigns a key or ID to user which is used to generate the share of signature known as partial signature. Partial signatures and threshold signatures are generated as the function of ID and verified. These partial signatures then are combined to form threshold multi-signatures. New techniques are being developed to reduce the danger of Key escrowing and with reduced computation especially for MANETs.

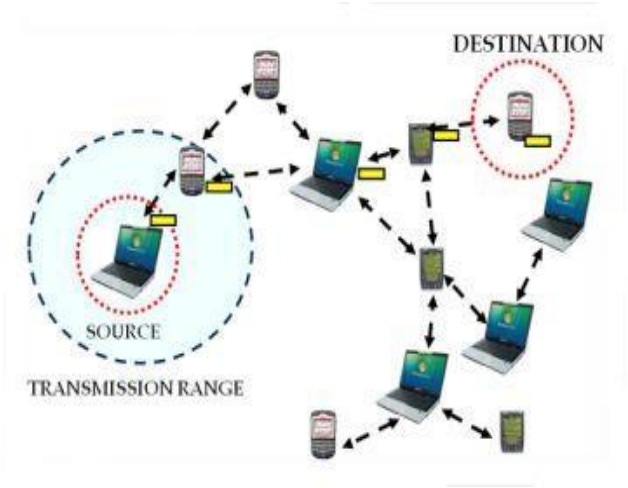

Fig -1: Secure Authentication

Confidentiality: Another important security feature is confidentiality which means the contents of secret message should not be disclosed to any other user but the one to whom secret information has been sent. MANETs are open networks and therefore, communication over such networks requires a verifiable identity as remote users may not know each other. This verification process detects the sender which helps to find out that if the message is forged or the signature has been stolen or the authorized user is behaving unkindly. All these problems are considered when security of MANET is concerned. Threshold digital signatures provide a way to build confidentiality as only a legal user can only open the message.

Non-Repudiation: The major goal achieved by implementing non-repudiation is to ensure that if a user sends a message with the signature then that user cannot deny having sent the message.

Availably: The objective of availability is to keep the network service or resources obtainable to the authorized users. It permits the survivability of the network despite malicious incidents such as DoS (Denial of Service) attack. When a dishonest node launches a DoS attack or tries to disturb the communication between nodes generating some erroneous messages, an intrusion detection process is taken place. In such process a periodically monitoring of the current activities of all participating nodes is done.

Integrity: It shows that received message is not modified or corrupted. When data or secret information is sent through the wireless medium, there is a possibility that an intruder picks up message and resend with incorrect information. Integrity can be achieved through digital signature or hash function algorithms.

6. CONCLUSION

After reviewing a range of techniques to authenticate an individual signer or a group of signers, we conclude that Advanced Threshold cryptography is providing security to MANETs in term of public key management, partial signature aggregation and entity management structure for dynamically adjustable groups. In spite of difficulties in implementation, there are techniques such as weighted RSA technique and use of Elliptic Curve based Threshold cryptography to overcome the problem. Trust building among nodes without a central authority is the future challenge in the field of threshold cryptography.

In the future we plan to investigate reputation and trust based threshold signature scheme for dynamic and ad-hoc groups to obtain a more secure authentication scheme for Point to Point MANETs.

ACKNOWLEDGEMENTS

We wish to thanks the previous authors for providing a nice concept in the area of security. This paper presents a significantly improved construction and a complete rewrite and evaluation of our implementation that can significantly improves the overall concept of security for MANETs by using threshold cryptography.

REFERENCES

[1]. G. D. Crescenzo, R. Ge and G. R. Arce. “Improved Topology Assumptions for Threshold Cryptography in Mobile Ad Hoc Networks”. In ACM SASN, 2005.
[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]. M. A. Azer ,S. M. El-Kassas and M. S. El-Soudani . “Threshold Cryptography and Authentication in Ad Hoc Networks “. In Second International Conference on Systems and Networks Communications (ICSNC’07), 2007.
[4]. S. Iftene and M. Grindei. “Weighted Threshold RSA Based on the Chinese Remainder Theorem”. In Ninth International Symposium on Symbolic and Numeric Algorithms for Scientific Computing-2008
[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. 2013-220. Springer, Heidelberg 2008.
[6]. M. S. Hwang , S. F. Tzeng, and C. T. Li.”A New Non-repudiable Threshold Proxy Signature with Valid Scheme Delegation Period”. Gervasi and M. Gavrilova (Eds.): ICCSA 2007, LNCS vol 4707, Part III, pp. 273-284, Springer, Heidelberg.
[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]. F. Li, Q. Xue and Z. Cao.”Cryptanalysis of Kuo and Chen’s Threshold Proxy Signature Scheme Based on the RSA”. In International Conference on Information Technology (ITNG'07).2007.

BIOGRAPHIES

H. Ateeq Ahmed received M.Tech from Samskruti College of Engineering & Technology, JNTUH, Hyderabad. Currently he is working as an Asst. Professor in the Department of CSE at Dr. K.V. Subba Reddy Institute of Technology, Kurnool, A.P. He has more than 5 years of teaching experience. His area of interest includes Computer networks and network security.

C. Mohammed Gulzar received his M.Tech degree in CSE from VTU, Belgaum, in 2008. Currently he is working as an Associate Professor in Dr. K.V. Subba Reddy institute of Technology, Kurnool, AP, India. He has Eleven years of experience in teaching. His area of interest includes adhoc and wireless sensor networks.

S. Imran Pasha received M.Tech from Samskruti College of Engineering & Technology, JNTUH, Hyderabad. Currently he is working as an Asst. Professor in the Department of CSE at Dr. KV. Subba Reddy Institute of Technology, Kurnool, A.P. He has more than 5 years of teaching experience. His area of interest includes Image Processing, Adhoc Networks and Data Mining.