An Identity- Based Key Management in MANET with Threshold sharing

R. Rajesh
Research Scholar, School of Information & Technology
Madurai Kamaraj University, Madurai

Abstract

Wireless mobile Ad Hoc Networks (MANETs) are an upcoming technology in the field of mobile computing. These networks express severe security problems due to their distinctive uniqueness such as mobility, dynamic topology and lack of central infrastructure support. To execute this system MANET and to construct it practical, we incorporate the idea of Shamir's secret sharing scheme. This system proposes key management and security concerns in mobile ad hoc networks. We present the key management scheme as a combination of Identity-Based, Unique Transmission's time Factor and Threshold Cryptography for ad hoc networks. It is a Certificateless solution which eliminates the need for public key distribution and certificates in public key management schemes. We also suggest a distributed key management approach by using the recently developed ideas of certificate less public key cryptography which is combined with Identity Based and threshold secret sharing schemes. Without any assumption of prefixed trust relationship between nodes, the ad hoc network works in a self-organizing way to provide the key generation and key management services using threshold secret sharing schemes, which effectively solves the problem of single point of failure.

Keywords: *MANETs, key management and security, Unique Transmission's time Factor and Threshold Cryptography for ad hoc networks.*

I. INTRODUCTION

A MANET is a supreme auspicious and rapidly increasing technology which is established on a self-organized and promptly organized network. Mobile Ad Hoc Networks (MANETS) are wireless mobile nodes that supportively form a network without organization. In a MANET, each mobile node acts as a router. The chief benefit of MANET is that it can function in separation or in synchronization with wired substructure. Each node, which performs like a mobile router, has complete control over the data that pass through it. Several of these are malevolent nodes, which enter the network during creation stage while others may make indigenously by cooperating are maining generous node. These mischievous nodes can express out both passive and active attacks against the network.

In inactive attacks, a malicious node only overhears upon packet substances without troublesome the network operation, while active attacks can formulate, change or drop packets. Since of these attacks, security is essential to guard against attacks where cryptography plays a dynamic role. For the reason that, ad hoc networks are highly susceptible to numerous security dangers owing to its crucial characteristics, such as open medium, deficiency of fixed essential structure, energetically varying topology and inhibited source, traditional key management methods based on public key infrastructure is not directly pertinent to ad hoc networks. One of the main tasks in MANET is to recognize secure routing information. Mobile ad hoc networks eradicate the essential for any organization support by trusting on the mobile wireless nodes themselves to jointly accomplish all networking functions, such as route detection update or data transactions. The features of ad hoc networks make them vulnerable to various attacks. The wireless relations are essentially susceptible and complex by unbalanced connectivity between the nodes owing to the mutual wireless channel. Recurrent connectivity problems are also produced by node flexibility where nodes are permitted to dispense the network, resultant in a volatile and dynamic network topology. These essential susceptibilities make it easier for attackers to negotiate the networking infrastructure in the nonexistence of robust security mechanisms. When an aggressor prospers to entree information of another node illegitimately, the target node is called the negotiated node. Once node has been negotiated, bogus routing table can be disseminated through the network and penetrating and acute information through these negotiated nodes can be easily confined. Wireless devices are vulnerable to active and passive attacks. Fortified routing information used to allocate data from one node to another node is challenging task to withstand. Many results are projected to solve these attacks comprising trust management and cryptography methods. Cryptography methods have played important roles for providing security. Key management is one of the important methods of cryptography that is set of methods which maintains the creation, interchange, storing, use and spare of keys among authorized entities. Identity-Based Cryptography, is a method that public key produced based on user's identity. Prospect of accomplishing many attacks that comes

from impression of legal users can be eliminated by this proposed system

II. CRYPTOGRAPHY

Cryptography is an important and prevailing tool for security amenities, specifically verification, privacy, integrity and non-repudiation. Key management is an elementary part of any confident communication. Key management agrees with key creation, stowage, dissemination, informing, and reversal and certificate facilities, in agreement with security strategies. Deficiency of safe key management makes a network susceptible to attack. Key management structures typically concentrate on educating security and enhancing the key storage. The restricted resources and flexibility of nodes are blockage of MANET security. An operative key management system can crack this problem. In mobile ad hoc network, a group can accelerate message delivery and preclude bandwidth remaining commendably. Group privacy is one of the concerns in group key management used in promising secure multicast group communication where restricted transmission is used. Cluster privacy needs that only legal group users could decrypt the multicast data even if the data is transmission to the complete network

A. Certificateless Public Key Cryptography

In a public key cryptography system, there are two isolated keys evolved: the public key and the private key. The notion of identity-based (ID-based) cryptography was announced by Shamir to crack the main disadvantage of public key cryptography by eliminating the requirement of the credentials. In this system, the uniqueness of users are used as their public keys and therefore there is no need to have this public keys certified. The secret key is resultant from the user's identity organized with the trustworthy authority, called the Private Key Generator secret key. However, this makes the system unfeasible meanwhile the PKG will know all the secret keys that the consumers have and consequently, the PKG can continuously make fun of any users. The idea of Certificateless cryptography is to gather the strength of both the public key cryptography and ID-based cryptography and to avoid the drawbacks that these two systems have. In this system, there is a trusted authority called the Key Generation Centre that will need to generate a partial secret key for the users, given the users' identity. Nonetheless, each user also needs to generate his/her own partial secret key and based on these two pieces of information (partial secret keys), the user can generate the public key that needs to be published.

B. Threshold Secret Sharing

Threshold secret sharing permits a secret to be united among a collection of users in such a manner that no single user can realize the secret from his portion alone. To create the secret, one wants to syndicate a sufficient number of stocks. (*k; n*) threshold secret sharing signifies that the secret is dispersed to *n* shareholders, and any *k* or more users can renovate the secret from their segments, but *k ¡* 1 or fewer users cannot get any information about the secret. Now, *k* is the inception constraint such that 1 · *k* · *n*. To allocate a secret *S* among *n* users, a trusted authority selects a large prime *q*, and arbitrarily picks a polynomial

$$f(x)= S+ a_1x+....+a_{k-1}x^{k-1} (mod\ q)$$

The trusted authority work out each user's share by *Si* = *f*(*i*) and securely sends the share *Si* to user *i*. Then any *k* users can renovate the secret by computing

$$S = \sum_{i=1}^{k} S_i L_i\ (mod\ q)$$

$$L_i = \prod_{j=1, j\neq i}^{k} -j/(i-j)(mod\ q)$$

In the Threshold secret sharing schemes, the secret is secured by dispensing it among numerous users. Though, certain adequately long time an aggressor could negotiate*k* users and attain their segments, thereby permitting him to restructure the secret. To protect against such attackers, positive secret sharing schemes use share energizing, which permits users to calculate new shares from old ones in relationship without revealing the shared secret to any user. The new segments establish a new (*k; n*) sharing of the secret. After stimulating, users eliminate the old shares and only keep the new ones. Since the new shares are self-determining of the old ones, the opponent cannot associate old shares with new shares to improve the secret. Therefore, the aggressor is defied to compromise *k* users between intermittent refreshing.

III. EXISTING SYSTEMS

A. Partially distributed authority scheme

Partially distributed authority scheme was firstly proposed by Zhou and Hass. In their system it is supposed that there is an Offline Trust Third Party (OTTP) erecting and allocating keys for all the nodes. Initially, this OTTP produces a couple of master public/ secret keys. The master public key (mpk) is recognized by every node in the network, while the master secret key (msk) is divided into *n* parts, where

each part is presented by *Si*(*i* = 0, 1, 2...*n*). Then OTTP picks *n* arbitrary nodes, randomly distributed with msk parts. These *n* nodes collectively form the Distributed Certificate Authority (DCA). The OTTP then creates certificates for all of the nodes and allocates them separately. In this arrangement, those certificates are completely stored in each DCA node as well. This provides confirmation from possible threads of unlawful nodes. Any illegal node does not have legal certificate, thus will not get key shares from DCA nodes.

B. Fully distributed authority scheme

A fully distributed authority scheme is an alteration of partially distributed certificate authority system. This method also creates use of the (*n, t*) threshold secret sharing scheme. The modification between Luo et al.'s model and Zhou model depend on on the following: In Zhou model, DCA nodes are casually selected from all the nodes while Luo et al's model uses all of the nodes in the MANET to form the DCA. The *msk* is united among all the nodes and for this reason, this scheme is called 'fully distributed'.

C. ID-Based distribution scheme

One of the Identity-based authority systems was suggested by Boneh and Franklin, which is an improved result to Zhou and Hass' scheme. It interchanged the DCA with a threshold private key generator. Primarily, users in the network will mutually form the PKG. This PKG will produce a couple of *mpk/msk*, and the *msk* is divided and shared among all the initial nodes. It is not specified in how this PKG is shaped nor how the *msk* is dispersed. Later the beginning, the user's uniqueness is used as the user's public key, while each PKG node will generate a part of this user's private key, which is based on the user's identity.

IV. PROPOSED SYSTEM

Our key management method does not rely on any supposition of underlying key management subsystem. Specifically, there is no reliable authority to produce and allocate the public/private keys and there is no prebuilt trust relationship between nodes in the network. All the keys used are produced and sustained in a self-organizing way inside the network. We take up that each mobile node conveys an IP address or an identity, which is distinctive and unaffected during its generation in the ad hoc network. The IP address or identity can be acquired through some lively address distribution and auto arrangement, only if the address is nominated without any struggle with other nodes in the network. We also take up that each mobile node has a method to determine its one-hop community and to get the distinctiveness of other nodes in the network.

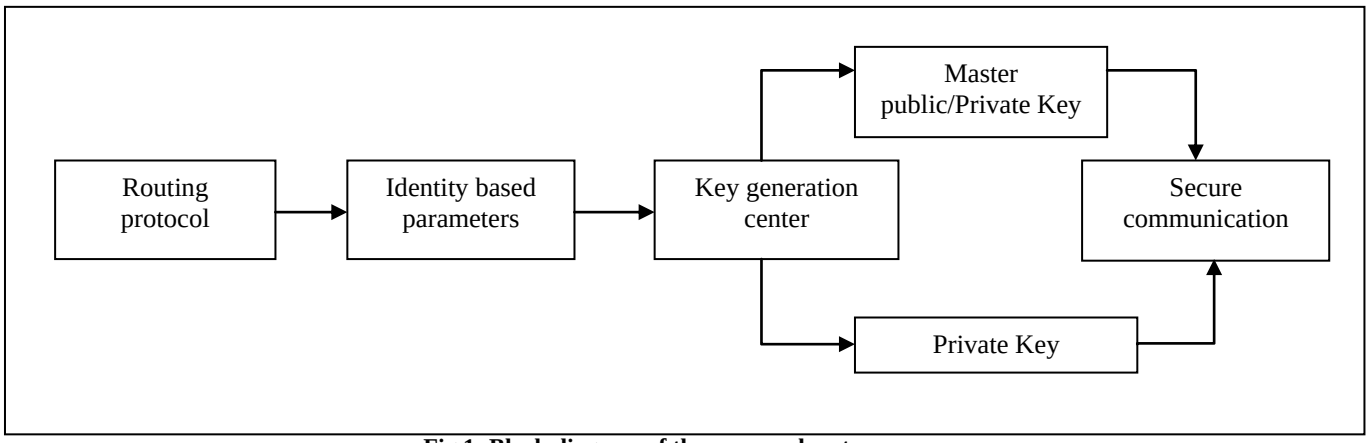

Fig.1: Block diagram of the proposed system

The proposed algorithm for the proposed method is defined as follows:

Step 1: Start
Step 2: Read unique identity
Step 3: Read data
Step 4: Setup stage ⟶ Master public/Private Key
Step 5: Extract stage ⟶ Generate public/private key
Step 6: Encrypt Stage ⟶ Encrypt message

i. Compute master public key and public key ($M_{pk,}$ Pub_k, $f(Pub_k)$,$m \epsilon M$)
ii. Compute master public key and public $M_{sk,}$ $Priv_{k,}$ $g(Priv_k)$, $c \epsilon C$
iii. $Priv_{K,} \longrightarrow C$

1. No: Discard packet
2. Yes: Decrypt packet

Step 7: Decrypt Phase ⟶ Decrypt message
Step 8: End

The chief idea of this algorithm is relating distinctive and small parameter comprises identity ti and uID in Identity-Based Cryptography method for swelling the presentation of legitimacy of entity. This features

leads to decrease imitating, packet reducing and routing attacks.

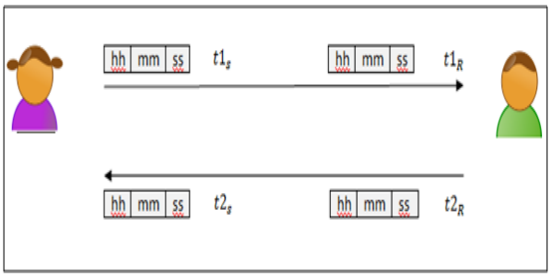

Fig.2: Key Management

As Fig. 1 determines, User A sends the request at the unique time $t1$, and User B receives this request at the time $t1$, this time might not be unique since many nodes in same distance can received this packet at the same time. On the other hand time $t2R$ is unique for User B.

One of the essential concerns, this method point out is that during confirmation process and communication there is not any reliable third party. Then, in respect with Group heads are supposed as PKGs, we relate threshold for key management in the network. Consequently single point of the catastrophe is eradicated. It means if a mobile node within the network is negotiated, the verification still achieved by other nodes. In accumulation a few packets are essential to realize the mutual confirmation routing in MANET. IBC-t proposed a strong user identification and authentication which indicates to decrease the chance of these attacks by totaling a small and distinctive factor which generates Public/Private keys in a sensible time and does not lead to traffic or over head through the network.

V. PERFORMANCE ANALYSIS

In this proposed system, communication overhead is deliberated by three methods ARAN, SRP and ISMANET. ARAN presents a preliminary authorization process, through two segments, the initial stage, a necessary end to end verification, and the second stage, an elective providing of shortest path. In this system each node directs an application of certification employed by a trusted certificate server before entering into the network. SRP suggested a technique with the declaration that any of two nodes have a security suggestion. In this method there is lack of authentication process for intermediate nodes between the source node and the destination node. In IBS method, node computes security restrictions and then mark this communication summary before sending packet, receiver node compares security parameters and checks the signature.

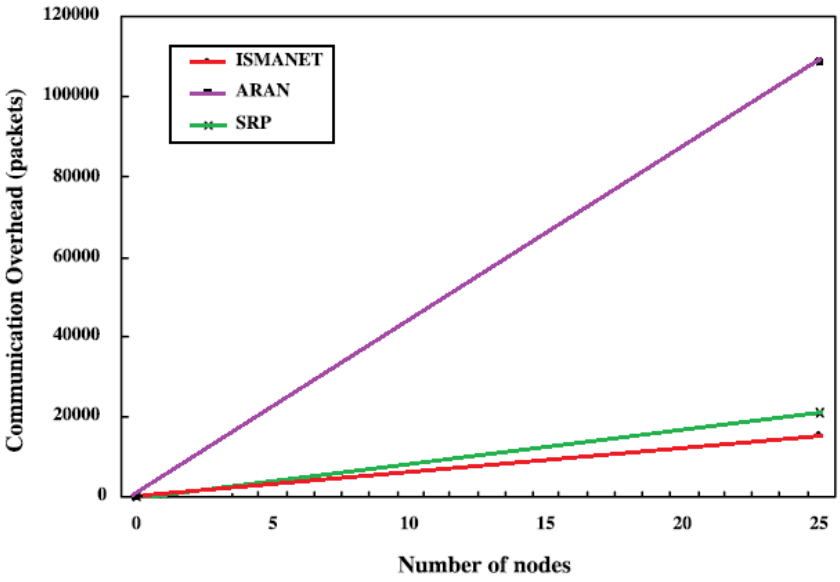

Fig.3: Performance Analysis of Nodes in Different Methods

It provides the strong authentication makes the privacy and reliability in the network. Numerous active and passive attacks are occurred owing to absence of the strong authentication. Aggressor inhibits illegitimately through the communication and then can reject the node actions simply if there is a pathetic identification and verification process. Robust authentication will decrease imitation attacks. Imitation attack is an austere risk to the security of mobile ad hoc network. Provision of strong authentication prepares the confidentiality and integrity in the network.

VI. CONCLUSION

Mobile Ad hoc networks are new exemplar in networking technologies. Key management is one of the best essential technologies for security of ad

hoc networks. The idea of this proposed method is a original method of spreading over ID-Based public/private key which not only assurances high-level verification of mobile nodes but also enables efficient key produces which indicates to flexibility against node negotiating. Most prevailing security methods for mobile ad hoc networks are created on applying public key certificates. The conclusion of this research improves legitimacy and concealment through the network by plummeting the computational time and increasing the authentication of mobile nodes.

REFERENCES

[1] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer, A secure routing protocol for ad hoc networks, In Proceedings of 10th IEEE International Conference on Network Protocols, Paris, France, pp. 78{87, 2002.

[2] W. Mohammad and R. S. Kumar, "A survey of attacks happened at different layers of mobile Ad-Hoc network & some available detection techniques," presented at the International Conference on Computer Communication and Networks, 2011.

[3] P. Papadimitratos and Z.J. Haas. Secure routing for mobile ad hoc networks. In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27{31, 2002.

[4] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," IEEE Trans. Dependable Secur. Comput, vol. 3, no. 4, pp. 386–399, 2006.

[5] Y. Ren, J. Wang, Y. Zhang, and L. Fang, "Identity-based key issuing protocol for ad hoc networks," in Proc. International Conference onComputational Intelligence and Security, 2007, pp. 917–921.

[6] L. Zhou and Z.J. Haas. Securing ad hoc networks. IEEE Network, Vol. 13, No. 6, pp. 24{30, 1999.

[7] P. B. Nyong and L. Wonjun, "ISMANET: a secure routing protocol using identity-based signcryption scheme for mobile Ad-Hoc networks," IEICE Trans. Commun, 2005.

[8] S.S.Al-RiyamiK.G.Paterson. Certificateless public key cryptography. page 452C473. C.S. Laih(ed.) Advances in Cryptology C Asiacrypt 2003,Lecture Notes in Computer Science, 2003.

[9] C. Jin-Hee, "A Survey on trust management on mobile Ad hoc networks," Communications Surveys & Tutorials, pp. 562-583, 2011.

[10] L. Wenjia and A. Joshi "Security issues in mobile Ad Hoc networks," 2006.

[11] J.Van Der Merwe D. Dawoud S. McDonald. Asurvey on peer-to-peer key management for mobilead hoc network. pages Article 1 (April 2007), 45

[12] S. Khan, "Passive security threats and consequences in IEEE 802.11 wireless mesh networks," International Journal of Digital ContentTechnology and its Applications, pp. 4-8, Dec 2008.

[13] 4. J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for mobile ad hoc networks. In Proceedings of 2001 International Conference on Network Protocols, Riverside, USA, pp. 251{260, 2001.

[14] S. Namita, "Secure communication using elliptic curve cryptosystem ad hoc network," University of Ottawa, 2008.

[15] C. Yu, Y. Mu, and S. Willy, "An identity-based broadcast encryption scheme for mobile ad hoc networks," Journal of Telecommunication and Information Technology, vol. 1, pp. 24-29, 2006.

[16] R.L.RivestA.ShamirL.Adleman. Certificatelesspublic key cryptography. pages 120–126. Communications of the ACM 21, 1978. pages. ACM Comput. Surv. 39, 1, 2007

[17] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In Proceedings of 26th IEEE Symposium on Foundations of Computer Science, Portland, OR, USA, pp. 151{160, 1985.

[18] 16. P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In Proceedings of 28th IEEE Symposium on Foundations of Computer Science, Los Angeles, CA, USA, pp. 427{437, 1987.