A Novel Security Approach in MANET with Certificateless Cryptography

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

Abstract

A mobile ad hoc network is an independent collection of mobile devices that communicate with each other over wireless links and work together in a distributed manner. In this network, Security is the most important attention because of its lack of centralized devices. In mobile ad hoc networks, the load and complication for key management is intensely dependent on limitation of the node's accessible resources and the dynamic nature of network topology. In this proposed system, we suggest a key management method by using the ideas of certificateless public key cryptography. It is applied here not only to remove the necessity for certificates, as well as to maintain the desirable assets of identity-based key management methods without the inherent key escrow problem. Typically, keys are produced by a certificate authority that is given whole power and is tacitly trusted. In this effort, we adopt this system's advantage over MANET. The master secret keys are distributed to all the nodes that are presented within the network. This makes the system self-organized once the network has been initiated. From this key management in MANET, we achieve a maximum security to the system.

Keywords

public-key, Key Management, certificateless cryptography, key escrow problem, security issues.

I. INTRODUCTION

The mobile ad hoc network (MANET) is a network that is simply encompassed of mobiles devices without any pre-established infrastructures. In this network, routing is acritical problem, since different fromother networks, it has no access point for the nodes to connect and communicate. With the growing technology, security turns out to be a significant issue. Due to tremendous application development in this network, the requirement for MANET security has improved considerably increases from the past years. Key management methods may either need an online trusted server or not. The infrastructure less nature of MANETs prohibits the use of server-based protocols. Hence, focus on server less methodology from here on. There are two spontaneous symmetric-key solutions, other one is satisfactory. The first one is to preload all the nodes with a global symmetric key, which is vulnerable to any point of compromise: if any single node is compromised, the security of the entire network is breached. Because ad hoc networks are highly vulnerable to various security threats due to its inherent characteristics, such as open medium, absence of fixed central structure, dynamically changing topology and constrained resource, traditional key management methods based on public key infrastructure (PKI) is not openly related to ad hoc networks. Planning an efficient key management solution must fulfill resulting characteristics such as Insubstantial of the nodes, Distributed network, Volatile in nature, Fault-Tolerant and it essentially determines the network conveniently. Key management service is an essential security concern since it is the vital assumption of many other security services. For example, many secure routing protocols, undertake that a pair of private and public keys and a certificate engaged by a trusted third party have been allocated to nodes. Recent investigation works in key management are generally based on traditional PKI and identity-based public key cryptography (ID-PKC). These methodologies based on customary PKI use a partially distributed or a completely distributed certificate authority (CA) to issue and succeed public key certificates. Nevertheless, the resource-constrained ad hoc networks might be incapable to give the rather difficult certificate management, comprising revocation, storage and distribution, and the computational costs of certificate verification. ID-PKC discard the public key certificates by permitting the user's public key to be any binary string, for instance an email address, IP address that can identify the user.

In this work, ID-PKC has a benefit in the part of the key management associated with the customized PKI. Though, it needs a trusted private key generator (PKG) which creates the private keys of the units using their public keys and a master secret key. Consequently, the requirement on the PKG who know all users' private keys unavoidably causes the key escrow problem to the ID-PKC systems. For instance, it can decrypt any cipher text in an identity-based public key encryption scheme. Similarly unpredictable, it could be fake any entity's signatures

in an identity-based signature system. The fore most methodological difference between the two systems is in the binding between the public and private keys and the worth of validating those keys. Typically, this is accomplished through the habit of using a certificate in the PKI system. Moreover, in an ID-PKC mechanism, the binding between the private key and the trustworthiness data is accomplished by a Trusted Authority (TA) at the point of demand, while the binding between the public key and that data can be done by anyone at any point.

In a certificate less cryptography, a Key Generation Center (KGC) is tangled in distributing user partial key to user whose uniqueness is supposed to be distinctive in the system. The user also autonomously produces an extra user public/secret key pair. In the Cryptographic processes, they can then be implemented effectively only when both the user partial key and the user secret key are identified. Knowing only one of them should not be able to take off the user that is, working any cryptographic operations as the user. The attacks that are deliberated in certificate less cryptography are key replacement attack and malicious KGC attack. The first attack is that a third party attempts to imitate a user after negotiating the user secret key and/or exchanging the user public key with some value selected by the third party. The KGC, who recognizes the partial key of a user, is mischievous and attempts to impersonate the user. Nevertheless, the KGC does not identify the user secret key or being able to interchange the user public key.

II. OVERVIEW

The notion of CL-PKC is proposed by Al-Riyami and Peterson with the unique inspiration of eradicating the inherent key escrow problem of ID-PKC. Later then, many more encryption and signature schemes were proposed by many researchers. In this method, the KGC supplies a user with a partial secret key which the KGC calculates from the user's identity and a master key, and then the user syndicates its fractional secret key and the public limitations with some secret facts to produce its definite secret key and public key separately. Like this, a user's secret key is not available to the KGC. If we need aspects of certificate less public key cryptography, we must indulge in an algorithm that augments the system in a step by step manner. Here we just concentrated on what is certificate less key cryptography not how it works. So the impression is sufficient to recognize the structures of the certificate less key cryptography. In brief, the structure consists of setup partial private key, set secret value, set public key, set private key, encrypt and decrypt.

In PKI, the management of certificates and its associated keys is the crucial problem in running the process. To avoid such difficulties, identifier – based cryptography was proposed and it actually overcomes this problems. This system is originally designed in which the key itself is generated from some publicly identifiable information, such as a person's e-mail address. Recently, it has been recognized that an identity need not be the only determinant of a client's public key. In this system, the TA is straightly in control for the creation of the private key hence there is intrinsic escrow ability in the system. This aims analteration in the role of the reliable third party within the system. In a PKI, the CA is disturbed with authenticating the authenticity of the information present in the certificate; however, in an ID-PKC the TA is directly in charge for producing and allocating all setting material within the system.

III. PROPOSED SYSTEM

Key management is a basic portion of any protected communication. Most secure communication protocols depend on the significant secure, strong, and effectual key management system. Key is a part of input information for cryptography processes. Mainly, if the key is disposed, the encrypted information would be disclosed. The secrecy of the symmetric key and private key must be assured locally. The Key Encryption Key approach could be used at local hosts. Key integrity and ownership should be protected from advanced key attacks. Digital signature, message digest and hashed message authentication code are techniques used for the data authentication or integrity purpose. Likewise, public key is secured by public-key certificate, in which a reliable entity called certification authority in PKI assures the binding of the public key with vendor’s identity. In structures, where requiring trusted third party, public-key certificate is promised by noble nodes, in a distributed manner, such as good secrecy. Noticeably, certificate cannot demonstrate whether an entity is good or bad, but the verified of ownership of key. Evidently, in mobile ad hoc networks, structure of key management which built on a entirely centralized mode is not possible not only because of the struggle to sustain such a universally trusted entity but also the central entity could become a hot spot of aggressive, thus network undergoes from the security blockage. In the meantime, an entirely dispersed model may not be satisfactory as a result of no well-trusted security anchor accessible in the whole system. One possible result is to allocate the central belief to multiple or entire network units based on secret sharing scheme.

In key management system, the crucial difference between the Public key infrastructures and Identity based public key cryptography is to be elaborated by

means of how they manage keys within the network. Hence, by this effort, we categorized the following into three main concerns: generation of public keys, generation of private keys and revocation of keys. In generating the keys, the main concentration is on the key generation techniques. They are who, when, where and how the keys are generated.

A) Generation of public keys

The generation of public keys is already we proposed a lot in previous paper. Some of the important factors are mentioned for recalling the process.

1) Encryption: For ID-PKC, the user creating the cipher text can produce the encryption key pair without consuming to know the identity of the client who will decrypt the message. For PKI, the user would require to discern the public key that was associated to the private key to be used to decrypt the message previously – generally the decryption key assured to the recipient's identity.

2) Signature verification: For ID-PKC, the authentication key is produced from the signer's identity. This can be agreed either by the signer, who then attributes the certification key to the signed message, or by the verifier who estimates it at the time of verification. In a PKI, the certification key is generated at the same time as the signing key and the certificate enclosing the verification key often accompanies the signature.

B) Generation of Private keys

The generation of private keys by the TA in the ID-PKC increases issues of escrow and/or privacy environment the management of private keys. This force is of advantage to an encryption scheme in a business atmosphere where the company keeps the data, but is problem in an implementation for digital signatures which might want to suggest non-repudiation.

1) Decryption: For ID-PKC the private key desires to be delivered to the decrypting party by the TA. Whether this key will be new for this certain session/message rest on the client producing the cipher text used a long term or short term public key. For PKI, the public encryption key used is generally the client's long term key destined to their certificate, while a short term key could also be used. If a long term key is used, there seems to be little difference between the two schemes.

2) Signature creation: For ID-PKC, the private key is created by the TA and agreed to the client. Since signature schemes should distinctively recognize the creator of the signature, the inherent key escrow in ID-PKC makes it a less attractive choice. For PKI, the key is either generated by the CA or the client. This ability to choose who generates the private key offers PKI an advantage in terms of flexibility over ID-PKC.

C) Revocation of keys

Revocation is one of the main complications faced by implementers of PKIs. Whereas ID-PKC does not have a key intrinsically, the concern of how to accomplish the identity/identifier related to a specific public key has until now expected very slight consideration. This problem is similar to the difficulty of certificate management in a PKI. In this sector, we will maintain that revocation could possibly become as large dispute for ID-PKC as it presently is for PKI. The main concerns of revocation of keys are described as follows as

1) In key management, the most practical concern is that retaining track of the characteristics that are developed within the system. As a significance of the tough relationship between keys and uniqueness in ID-PKC, denying a public key demands the revocation of the associated identifier. This problem is becomes severe if the identifier is one which could be problematic to modify the secret identities.

2) But these are exactly the identifiers that are certainly expected by the entity struggling to independently generate a valid key for an intended recipient. This suggests that less predictable identifiers would need to be employed.

3) Because of the inherent binding between identifier and key in ID-PKC, there is a potential drawback in terms of re-certification. At a recent PKI workshop, we saw a demonstration for a product which separated the storage of private key and certificate. The private key was stored on a smart card, while the certificate was stored on the hard drive. This allowed the organization to change the certificate content through re-certification without needing to go through the more expensive procedure of issuing the clients with a new private key. A precise imitation would be incredible to achieve in an ID-PKC system.

4) When condemning the concern of revocation, integrating the date with the user's identity to provide the identifier for the key. The argument delivered is that the re-issuance of keys on a per time basis precludes the need for a revocation mechanism. This mechanism increases some complications. If we force all genuine users to invite fresh keys every day, then it services the TA to be on-line for a greater quantity of the time and may

significantly increase the TA workload.

IV. RIGHTS MANAGEMENT

Rights management is the principal concern in the surroundings of key management in the Certificate less Public Key Cryptography. It is the period in which it integrates the whole thing that the control of a key and their related certificate/identifier approves the client to confirm. In this proposed system, Rights management is segregated into two main topics such as Generation and authentication of rights.

A) Generation of Rights

In the key management system, the rights of the keys can be employed by two systems. One method is by using signatures and the other method is by using encryption.

In signing methodology, the PKI, the signing key is generally assured to an identity. Depending on the system policy, the right to sign is either implicit in the verifier knowing who the signing party is, or it is explicit through a binding to an authorization mechanism. In an ID-based scheme, it would appear that the same principles apply. The popular choice for a signature creation key is likely to be some variant of the signing party's identity. In Encryption mechanism, traditionally PKIs have been primarily associated with authentication rather than authorization. In most commercial PKI systems, the identity certificate is used to authenticate the client to a separate authorization infrastructure. One of the proposed benefits of using ID-PKC is that the public encryption key can be generated by the party encrypting the data in advance of the corresponding private key having been generated.

B) Authentication of Rights

The rights that are used in the key management have been intimately verified and it could dignify the authorization process before entering into the process. The main intention of the system is to recognize how the worth by which these rights are verified affects the design of the system. To complete this process, the discussion about the key could be at the standard level and progress thing by investigated of the following three factors for signatures and encryption.

In PKI, In the case of signature verification, anyone who can use the public key associated with the signature key can verify the signature. The certification ensues when the user authenticating the signature carries out the signature confirmation. Within the network, this could possibly be far detached from the time that the signature was created. As a consequence of the nature of a traditional public key and its associated certificate, the verification could be conducted at a logically or physically remote site to the signature. This is considered one of the great strengths of public key cryptography. In ID-PKC, anyone with access to the public key corresponding to the private key can verify the signature. The timing of the verification is likely to be similar to a PKI. The verification of the right to sign will happen when the signature is checked by the relying party. Once again, there is the potential for the signature to be verified somewhere that is logically and physically remote from the signing party.

The key feature of the certificate less public key cryptography is that it completely eliminates the need for certificates. The technical means by which it does so is actually rather closely related to that used in a user A's private key is composed in two stages. In the first stage, a characteristics oriented partial private key is expected over a trustworthy and reliable channel from a confidential authority. In the next stage, the user produces his private key by combining the partial private key with some secret known only to the user. The user also publishes a public key which matches the private key. However, this public key need not be supported by a certificate. Most probably, CL-PKC won't require certificates to create trust in public keys, as an alternative, trust is created in an inherent way. This would look to make CL-PKC model for systems where escrow is intolerable, but where the full weight of PKI is indefensible.

V. CL-PKE in MANET

In MANET, the process of key management and CL-PKE are integrated to work in a decisive manner. Then accept that the starting of the network, there is a Key Generator Center (KGC) which produces partial secret keys for all the users. We also represent n to be the number of original nodes and t to be the design of security level of the threshold system. Those n nodes cooperatively form a Distributed Key Generator Center(DKGC).
In a mobile ad hoc network have k nodes in the early stage. The network has a public/private key pair, called master key (*MK, SK*) which is used to generate key generation service to all the nodes in the network. The master key pair is produced in such a method that the master public key *PK* is well known to all the nodes in the network, and the master private key *SK* is collective by all the nodes in a (*k; n*) threshold fashion. Previously employing any network service, each node has to achieve its partial private key equivalent to its identity and allocate its public key throughout the network. This partial private key can be calculated by attaining k shares of its key from the original nodes in the

network. Moreover, authentic nodes need only interaction any knodes so as toacquire their own partial private keys, thus making the protocol resistant to momentary loss of connectivity with other nodes in the network.

The most convenient solution has the following features: (i) it does not require a reliable authority to choose and to allocate the master private key to nodes. (ii) It is not essential for public key certificates, validated network bandwidth and computational power of nodes. (iii) The practice of CL-PKC create the solution eradicate the key escrow problem of the ID-PKC key management methods

VI. GENERATION OF MASTER KEY

The approach is not require the assist of the trusted authority to calculate a master private key, distinct it into multiple portions and then allocates the segments to users. As an alternative, the master key pair is work out collaboratively by the first network nodes.

- Select the nodes randomly and also secret key which they are in polynomial over the degree
- Compute the node which is broadcast within the network
- All nodes sent particular values securely to a specified node.
- The node verifies the accuracy by checking the status of the node
- The master private key share of node is combined by the sub shares from all the nodes, and each of them contributes one piece of that information.
- The master private key is computed as

$$MK = \sum_{i=1}^{n} x_{\mathrm{i}}$$

- The master public key can be computed as

$$PK = \sum_{i=1}^{n} S_{\mathrm{i}}\, L_{\mathrm{i}} P$$

A) *Distributed partial private key Generation*

In this structure, all the network nodes should share the master private key, thus each of them can be the KGC service node. Every node k of KGC service nodes produces a secret portion of the partial private key DA and sends to A. To make guaranteed, the created shares are steadily spread, each of the KGC service nodes sends encrypted share to the node A using A's public key PA. The process of generation of a share of the partial private key DA can be represented by

$$DA_{\mathrm{i}} = S_{\mathrm{i}} H_1(IDA)$$

WhereS_{i}(i = 1,…,k) is the share of the master private key of the KGC node,
H_1- a hash function used by the certificate less encryption scheme,
DA_{i}-the generated partial private key share for the node A.

VII. MASTER PRIVATE KEY SHARE CREATION

If suppose a new node links to the network, it will share its uniqueness, public key, and certain other essential corporeal proof to k neighbor nodes and requests the master public key and his share of the master private key. Each node in the association confirms the authority of the identity of the new node. If the authentication prospers, the private key can be produced for the new node. Note that the partial segments may be shuttled before being sent to the joining node to protect the secrecy of the coalition nodes' secret shares. Subsequently, attaining the share of the master private key, the new joining node is available to provide KGC service to other joining nodes. New node obtains its new share by adding the partial shares as

$$Mp = \sum_{j=1}^{k} Mp, j$$

To look after against attackers that might negotiate k or more nodes. If there is adequate time, a positive secret sharing scheme is used to permit nodes of an area to calculate new shares from old ones in collaboration without revealing the master private key of the region. Mainly notice that, it is redundant to necessitate all the nodes complicated in the master private key share refreshing process. In that case, the task can be completed by only knodes, meanwhile we assume that, between any successive secret shares apprises, the number of opponents who hold secret shares instigated from the same secret key is less than k. Since the new shares are liberated of the old ones, the adversary cannot combine old shares with new shares to recover the master private key. Thus, the opponent is challenged to negotiate k nodes in the same region between periodic refreshing.

XIII. SIMULATION AND DISCUSSION

In this MANET, the output of the system is verified by using simulation. From the simulation, the node in the network generally focuses on the continuous movement and the network is not stable in nature. The Simulation is take place in MATLAB. This simulation runs over following scenarios:

- Establishing a Network suitable for the framework f.
- Encrypting the data which is to be cipher text is ready for the input process.
- According to the proposed system, Public key is randomly selected through the polynomial Hf(x) = (βf,1 x + βf,2 x2 ... + βf,Pk-1) and the private key is altered as stated by the changes in the node position as

$$Mp = \sum_{j=1}^{k} Mp, j$$

- Finally, by using formulas to generate key and gradually strength of the key share enhanced on the basis of group moving.

Table.1: Tabulation for analyzing Route discovery time

Time(ms)	Existing system	Proposed system
5	0.15	0.102
10	0.28	0.168
15	0.42	0.176
20	0.273	0.24
25	0.25	0.19
30	0.212	0.103
35	0.196	0.08
40	0.185	0.112

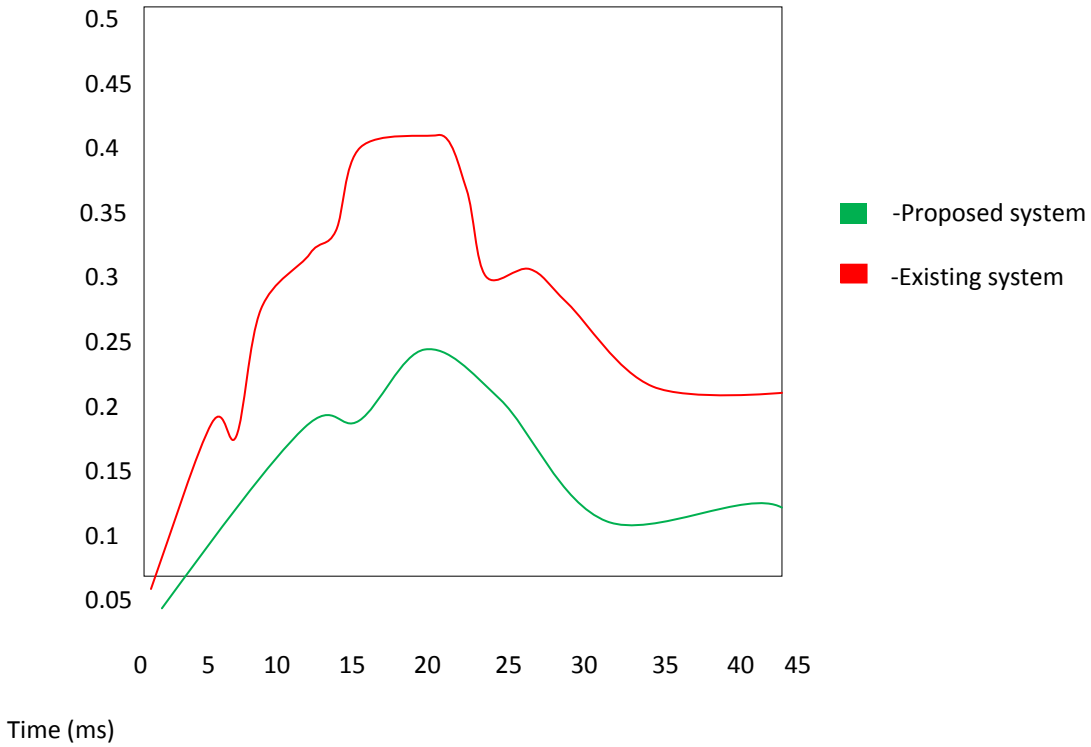


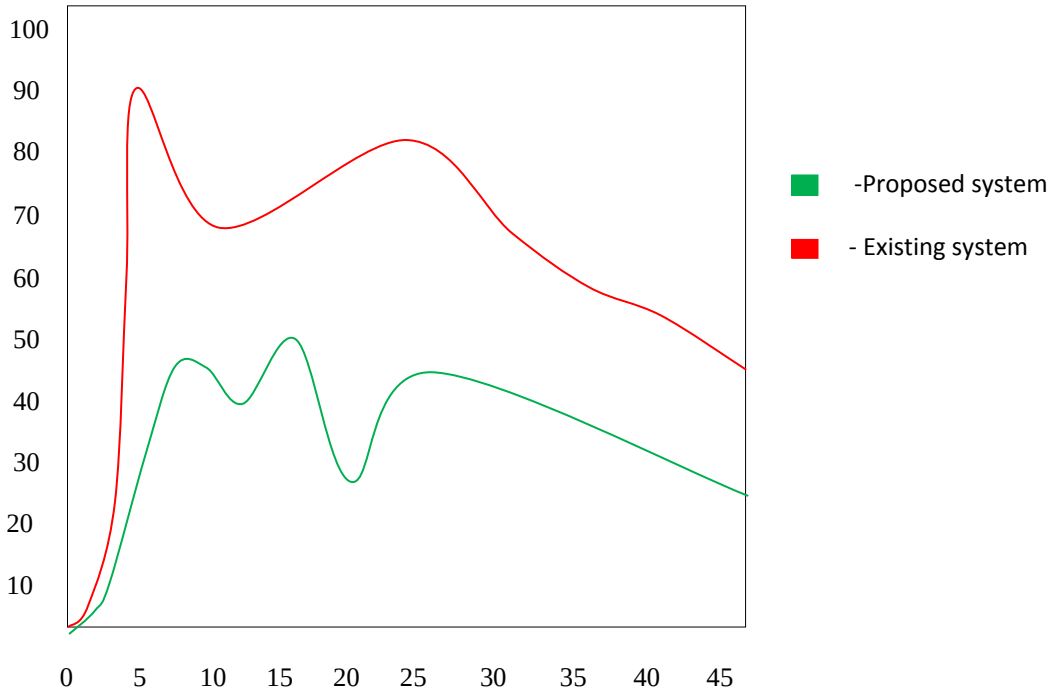
Fig.1: Average Route Discovery Time

Time(ms)	Existing system	Proposed system
0	0	0
5	90	27
10	68	43
15	70	50
20	80	25
25	76	45
30	65	41

35	59	38
40	53	32
45	48	26

¥ **Table.2: Tabulation for Total Packets Dropped in MANET**

Average traffic in AODV MANET



IX. CONCLUSION

Mobile Ad hoc Network is an innovative field in networking technologies. Key management is one of the principal methodologies for security of ad hoc networks. This paper suggests a novel approach for key management and Rights management using certificate less public key cryptography. Certificate less public key cryptography is instigated here not only to eradicate the requirement of certificates, but also to maintain the necessary properties of identity-based key management methods without the inherent key escrow problem. In this work, we have successfully issued public/secret keys for users without providing certificates. In simulation, the total number of packets dropped is decreased when compared to existing systems and also average traffic is decreased. This proposed scheme also confirms that system can work on self-organized networks after the instigation. It also provides a futuristic approach in the field of key management in MANET.

REFERENCES

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

[2] D.BonehM.Franklin. Identity-based encryption from weil pairing. pages 586–615. SIAM J. Computing 32(3), 2001.

[3] 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.

[4] 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.

[5] 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.

[6] S.Tapaswi1, Virendra Singh Kushwah, "Securing Nodes in MANETs Using Node Based Key Management Scheme," International Conference on Advances in Computer Engineering, IEEE, 978-0-7695-4058, Dec., 2010.

[7] Rakesh Chandra Gangwar and Anil K. Sarje," Secure and Efficient Dynamic Group Key Agreement Proto-col for an Ad Hoc Network," IEEE, 1-4244-0731,june 1, 2006.

[8] MengboHou and QiuliangXu," An Efficient and Secure One-Round Authenticated Key Agreement Protocol without Pairings," IEEE, 978-1-61284-774, Nov., 2011.

[9] Hongji Wang, Gang Yao, Qingshan Jiang, "An Identity-Based Group Key Agreement Protocol from Pairing" Third International Conference on Availability, Reliability and Security, IEEE, 0-7695-3102, Aug. 4, 2008.
[10] Zhenfei Zhang, Willy Susilo, and RaadRaad, "Mobile Ad-hoc Network Key Management with Certificateless Cryptography", IEEE,978-1-4244-4242, Aug. 3, 2008.
[11] Eduardo Da Silva, Aldri L. Dos Santos, and Luiz Car-los P. Albini, "Identity-based Key Management in Mobile Ad hoc Networks: Techniques and Applications," IEEE Wireless Communications, 1536-1284, Aug. 2008.
[12] Amit K Awasthi and Sunder Lal, "ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings," arXiv:cs/0504097V1[cs.CR],Apr. 23, 2005.
[13] YANG Ya-tao, ZENG Ping, FANG Yong, CHI YaPing," A Feasible Key Management Scheme in Adhoc Network , " Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, IEEE, 0-7695-2909,July 7, 2007.
[14] M.Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. In Proc. EUROCRYPT 2004, pages 268–286.
[15] B.C. Hu, D. S. Wong, Z. Zhang, and X. Deng, "Key replacement attack against a generic construction of certificateless signature", In Information Security and Privacy: 11th Australasian Conference, ACISP 2006, pages 235–246, Springer-Verlag, 2006. LNCS 4058.
[16] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, and Younggoo Kwon, "AC-PKI: Anonymous and Certificateless Public-Key Infrastructure for Mo-bile Ad Hoc Networks," IEEE 0-7803-8939, May 5, 2005.