A Survey on Various Identity Based Key Management In Mobile Ad Hoc Networks

[1]Dipali suhagiya ,[2]Asst. prof. Purvi ramanuj
[1]M.E. in Shantilal shah engineering college,[2] assistant professor in SSEC
[1]Information technology,
[1]Shantilal shah Engineering College –Bhavnagar, Gujarat

***Abstract*— Cryptography is one of basis of security solutions for mobile ad hoc networks. Among public key techniques, the identity-based ones are very attractive for mobile environment, mainly due to their simple key management process and reduced memory storage cost. In this paper we give an overview about existing Identity Based Key Management Schemes for MANET. We point out some problems of Identity-based key management schemes in MANETs, which are not addressed and we will explore in the future.**

***IndexTerms*— Mobile Ad Hoc Networks, Identity based cryptography, Key Management**

I. INTRODUCTION

Mobile ad hoc network is a dynamic network which allows communication between the mobile nodes without a central administrator. A MANET consists of mobile platforms (e.g. a router with multiple hosts and wireless communication devices) herein simply referred to as "nodes" which are free to move about arbitrarily. The nodes may be located on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. The nodes are able to join or leave anytime which makes the network topology dynamic in nature. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Interne [7]. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced

II. OVERVIEW OF KEY MANAGEMENT SCHEMES IN MANET

Key management is a technique to support establishment and maintenance of keying relationships between authorized parties [9]. A keying relationship is the state wherein network nodes share keying material for use in cryptographic. Keying material could be private key and public key pair or secret keys.To achieve the high security in MANET different Key Management schemes are used. Using and managing keys for security is a crucial task in MANET due to its energy constrained operations, limited physical security, variable capacity links and dynamic topology. Different cryptographic keys are used for encryption like symmetric key, public key, group key and hybrid key (symmetric+ asymmetric key) [8]. Let us discuss about some of the important Key Management techniques in MANET.

A. Symmetric Key Management in MANET

In symmetric key management same keys are used for encryption the data as well as for decryption the data. In public key cryptography, two keys are used one private key and another public key. Different keys are used for encryption and decryption. The private key is available only for individual and kept by source node and it is used for decryption. The public key is used for encryption and it available to the public. In each communication new pair of public and private key is created. It requires less numbers of keys as compared to symmetric key cryptography.

B. Asymmetric key management in MANET

Asymmetric key uses different keys for encryption the data and decryption the data. Each recipient has a private key that is kept secret and a public key that is published for everyone. The sender looks up or is sent the recipient's public key and uses it to encrypt the message. The recipient uses the private key to decrypt the message and never publishes or transmits the private key to anyone. Thus, the private key is never in transit and remains invulnerable. This system is sometimes referred to as using public keys. This reduces the risk of data loss and increases compliance management when the private keys are properly managed.

C. Group key management scheme in MANET

Group key in cryptography is a single key which is assigned only for one group of mobile nodes in MANET. For establishing a group key, group key is creating and distributing a secret for group members. There are specifically three categories of group key protocol 1. Centralized, in which the controlling and re-keying of group is being done by one entity. 2. Distributed, group members or a mobile node which comes in group are equally responsible for making the group key, distribute the group key and also for re-keying the group. 3. Decentralized, more than one entity is responsible for making, distributing and re-keying the group key.

D. Hybrid Key Management schemes in MANET

Hybrid or composite keys are those key which are made from the combination of two or more than two keys and it may be symmetric or an asymmetric or the combination of symmetric & asymmetric key.

III. IDENTITYBASEDCRYPTOGRAPHY

An identity based cryptography, the public key or secret key pair is generated by a Private Key Generator (PKG) service, and the public key based on the own identity. It is known to everyone. The idea of Identity Based cryptography was first Identity based cryptography (IBC) is a special form of public key cryptography. It is an approach to eliminate the requirement of a CA (Certificate Authority) and PKCs (Public Key Certificates). Some properties of IBC make it especially suitable for MANETs [10]:

- Easier to deploy without any infrastructure requirement. This saves certificate distribution, while bringing pair wise keys without any interaction between nodes.
- Its resources requirements, regarding processing power, storage space, communication bandwidth, are much lower.
- The public key of IBC is self proving and can carry much useful information.

The advantages of IBC are the simple key management process and reduced memory storage cost, compared with traditional methods. Easier to deploy without any infrastructure requirement. This saves certificate distribution, while bringing "free" pair wise keys without any interaction between nodes. Its resources requirement, regarding process power, storage space, communication bandwidth, are much lower.

Secure routing is an important when transferring critical information between source and destination. Without a proper security method, a secured routing information and data transfer will be easily compromised.

The major problem with ID-based schemes is that the private key of all users must be known by the PKG. In MANETs in which the PKG must be distributed by an arbitrary entity, this might be a major problem or issue. Identity based schemes lack anonymity and privacy preservation, as public keys are directly derived from the identity of the nodes.

IV. IDBASEDKEYMANAGEMENT

In an IBC scheme, the sender can use the receiver's identity of public key to encrypt message, and the receiver can decrypt the ciphertext by his own private key obtained from the PKG according to his identity.

The functions that compose a generic IBC are specified the following four randomized algorithms: setup, extract, encrypt, and decrypt [1].

- Setup: First takes security parameters as input and returns a master public key and private key pair for the system. The master private key is known to PKG.
- Extract: it takes master key and an identity of a node as input, and returns the personal private key of the node.
- Encrypt: takes master public key, the private key of the node, public key of the destination node, and the message as input, and returns corresponding ciphertext.
- Decrypt: takes master public key, the private key of the node, and ciphertext as input and returns the decrypted message.

This paper presents the most important schemes for MANETs.

A. Khaili-Katz-Arbaugh

Khaili's scheme is based on Franklin and Bone scheme [2] and recognizes the drawbacks of key management schemes with assumptions of existence of PKI and shared secret among nodes. In this scheme the identity based method is combined with threshold cryptography scheme. This scheme does not address key revocation or key renewing.

B. Deng-Mukherjee-Agrawal

This scheme includes two mechanisms: distributed key generation and identity based authentication [3]. The distributed key generation component provides the master public and private keys and public/private keys in a distributed way. The identity based authentication provides end to end authentication between nodes.

C. Bohio-Miri

A scheme that uses pair wise symmetric keys computed noninteractively by nodes can be found [4]. It assumes that all nodes are properly set up before network formation. This means that all nodes must get public parameters and their private key from the private key group before network formation. This scheme violates the spirit of ID-Based schemes, requirement support structures and online servers.

D. Identity-Based Authentication and Key Exchange:

The identity-based authentication and key exchange (IDAKE) scheme consist of two techniques: a basic MANET-IDAKE and a fully self-organized MANET-IDAKE [5]. Basic MANET-IDAKE consists of two phases: the initialization phase with access to an external PKG (setup, extract, and distribute algorithms) and the running system phase without access to a PKG (compute shared keys, key renewal, and key revocation algorithms).In fully self-organized MANET-IDAKE, all tasks are performed by the network nodes themselves, without any external PKG. The self-organized scheme does not specify how private keys are distributed to the nodes. The MANET-IDAKE scheme has low bandwidth and low memory requirements due to the efficient key management of ID-based schemes. The MANET-IDAKE computational complexity depends on the implementation of the key revocation and renewal algorithms. The basic version of the scheme has a single point of failure, while in the distributed version this problem is eliminated.

E. Identity Based Key Management

Identity based key management (IKM) is a combination of ID-based key management and threshold cryptography [6]. In Identity based key management scheme, the public and private key of each node are composed by a node-specific ID-based element and a network wide common element. The node-specific element ensures that the secrecy of non-compromised node is not jeopardized even in the presence of several compromising nodes. On the other hand, the common element part enables very efficient network-wide public and private key updates via a single broadcast message.

All presented schemes use asymmetric keys, except for the Bohio-Miri scheme, which uses shared symmetric keys for communication.

V. CONCLUSION

We have studied various identity based schemes in mobile ad hoc networks. Among them, identity based cryptography, a special form of public key cryptography; it eliminates the requirement for a certificate authority and public key certificates. The major problem with identity based scheme is that the private key of all users must be known by the private key generator.
In future we may try to develop a method that will provide security against various security threats like authentication, confidentiality as well as data integrity.

.

REFERENCES

[1] A. Khalili, J. Katz, and W.A. Arbaugh, "Towards Secure Key Distribution in Truly Ad-hoc Networks," *Proc. SAINT Workshops, 2003, pp. 342-346.*

[2] D. Boneh and M. Franklin, "Identity based encryption from the weil pairing," *Lecture Notes in Computer Science, vol.2139, pp. 213-229, 2001.*

[3] H. Deng, A. Mukherjee, and D.P. Agrawal, "Threshold and Identity Based Key Management and Authentication for Wireless Ad Hoc Networks," *proc. Int'l Conf. Info. Tech.: Coding and Computing, vol.2, 2004, p. 107.*

[4] M. J. Bohio and A. Miri, "Efficient Identity Based Security Schemes for Ad Hoc Network Routing Protocols," Ad Hoc Networks, vol.2, no.3, 2004, pp.309-317.

[5] K. Hoeper and G. Gong, "Bootstrapping Security in Mobile Ad Hoc Networks Using Identity Based Schemes with Key Revocation*," tech. rep., Center for Applied Cryptographic Research, Univ. of Waterloo*, 2006.

[6] W. Liu, "Securing Mobile Ad Hoc Networks with Certificeteless Public Keys," *IEEE Trans. Dependable Secure Computing*, vol.3, no. 4, 2006, pp.386-399.

[7] A. L.S. Orozeo, J.G. matesanz, L.J. G. Villalba, J. D. M. Diaz, and T. H. Kim, "Security issues in mobile ad hoc networks" *International Journal of distributed Sensor Networks, vol.2012, Dec 2012.*

[8] Merin Francis, M. Sangeetha, Dr. A. Sabari, "A Survey of Key Management Techniques for Secure and Reliable Data Transmission in MANET," IJARCSSE, vol.3, issue 1, 2013, pp. 22-27.

[9] A. J. Menezes, P. C. V. *Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography*, CRC Press, 1996.

[10] S. Honarbakhsh, L. Latif, A. Manaf, B. Emami," Enhancing Security for Mobile Ad Hoc Networks by using Identity Based Cryptography," IJCCE, vol. 3, no. 1, 2014.

[11] E. D. Silva and L. C. P. Albini, "Towards a fully-organized identity based key management system for MANETs," *IEEE 9th conf. on wireless and mobile computing, networking and communications*, 2013.

[12] "Cryptography and Network Security" by William Stallings, fifth edition.