ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Using Identity Based Cryptography (IBC) Increasing Security for Mobile Ad hoc Networks

Ms.Ashwini Choudhari
Student,
Dr.Seema Quadri Institute
of Technology, Aurangabad.

Prof.Santosh Takle
Assistant Professor,
SIES College of Engineering
&Technology, Mumbai.

Prof.Saad Siddiqui
Assistant Professor,
Dr.Seema Quadri Institute
of Technology, Aurangabad.

Abstract:

Security in mobile ad-hoc networks (MANETs) continues to attract attention after years of research. This paper studies key management and security issues in mobile ad hoc networks (MANETs). MANET is a self-configuring network of mobile hosts or routers without any pre-deployed infrastructure, centralized policy and control. Initially, ad hoc routing has focused on the problem of providing efficient mechanisms for finding paths in dynamic networks & without considering security. Because of this, there are a number of attacks that can be used to manipulate the routing in an ad hoc network.

In This Paper We present the key management scheme as a combination of Identity-Based (User's Identification), Unique Transmission's time Factor and Threshold Cryptography for ad hoc networks. It is a certificate less solution which eliminates the need for public key distribution and certificates in public key management scheme. The scheme is also efficient in computation since small unique factor enhance the authentication of entities.

Index Terms:

mobile ad hoc network Identity based cryptography, key management, security.

1. Introduction:

Mobile ad hoc network (MANET) provides communication for mobile devices which moved in any direction and manage arbitrarily. Nodes are self-configuring and communicate together directly or through intermediate nodes.Mobility characteristic of MANET results in dynamic topology which needs frequent changes in routing information.

Nodes in ad hoc network acts as routers which causes network layer to be more vulnerable to security attacks Mobile Ad hoc Network is known as infrastructure less network. Generally, routing protocols are classified into their categories: Proactive, Reactive and Hybrid protocol. In proactive protocol, all the Nodes maintain routing table and routing information are always available.

In reactive Protocol, finding a route is done by route request rather than finding route in advance. Mobility in MANET leads to lack of many security measures, which is used in conventional wireless network with the fixed infrastructure. Security attacks can be deployed in any network layers. Some physical tamper protection and transmission security procedures are capable for lowest layers while for higher layers protection cryptographic methods are applicable.

Security is defined as the reliable transmission of information through an insecure channel while the routing protocol determines the route required to direct packets between the various devices in the mobile ad hoc network.

In regards to some factors such as network environment, number of nodes, information transmission range of each node and so on, secured routing is difficult to provide. Cryptography is a solution which provides most of the security requirements. Basically cryptographic methods are categorized into two groups [1]:Symmetric Key Cryptography:

In this method the key for encrypting and decrypting is the same. The algorithms of encryption and decryption are inversed of each other [1]. Symmetric key cryptography does not support the complete security requirements. Asymmetric Key Cryptography: This method is also called public key cryptography.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

InAsymmetric key Cryptography there are two types of keys; Public Key, and Private Key. Public Key is used for encrypting, and Private Key is used for decrypting. Sender encrypts the plaintext into ciphertext by its public key and the receiver decrypt the cipher text into plaintext by its private key [1]. Based on the characteristics of mobile ad hoc network functionality of Public Key infrastructure has faced many challenges. Identity-based Cryptography is a form of asymmetric cryptography which is appropriate for MANET. In this method, third party server uses a simple and public identifier such as email address, for generating public key [3]. In identity-based cryptosystem, verification of user's validity is achieved by its unique identifier (ID). Private Key generates from a key generation centre (KGC) while the public Key is obtained from user's ID [4]. Index Terms—Identity based cryptography, key management, security, mobile ad hoc network.

2. RELATED WORK:

Most of the master key and private key generation schemes are derived from and are variants of Shamir's method. Zhou et al. have suggested [1], a CA service of PKI can be distributed to multiple nodes in a MANET environment. This idea is also applicable to IBC.In Identity-based cryptography, the PKG is a fundamental node which plays a crucial role for key generation.

Zhou et al. [1] proposed an idea that CA service of PKI is better to distributed to the multiple nodes in mobile ad hoc network.

Deng et al. [2] proposed an Identity-Based key management and authentication for mobile ad hoc network employing IBC and threshold cryptography. This scheme includes distributed key generation and identity authentication. In this method assume that each node is able to discover its one-hop neighbour nodes and can get all the identity of nodes in the network. The key generation component provides the master public/private keys and public/private keys in a distributed way. Zhang et al. [2] proposed a Distributed Private Key Generator (DPKG) to multiple nodes.

Li et al. [3] proposed a scheme based on signcryption that provides a secure transmission by applying key proxy, periodic private keys and multicast group of Private Key Generators.

Key proxy derived from server nodes. Based on the location server nodes create multicast groups. Node send Route Request to server nodes group, when the nod received a Route Reply select a server node with the shortest path as its proxy key. Afterward the routing information to the selected server node is preserved.Fenget al. [4] proposed a method based on divide public key and private key into node specific and phase specific. In this scheme key update parameters is pre-distributed. Before network deployment, cryptographic parameters issue to each node. PKG publishes master keys to DPKG using threshold secret sharing. Each DPKG maintains a secret key and a set of values. Public key and private key is node specific and phase specific which the node specific is the first part of the key and the phase specific is the second partRenet al. [5] proposed a scheme based on DPKG. Inthis method apply mutual authentication in public channel which leads to enhance the need of requirements of secure channel.

Lin et al. [6] proposed a hybrid method including traditional PKI and IBC. In this scheme key management integrate into secure routing protocols. This framework has two-layer hierarchical form. CA in the higher layer is responsible for external cluster domain authentication and the lower layer is responsible for internal cluster domain authentication by applying IBC.Lee et al. [7] proposed a method based on using Key Generator Centre (KGC), which provide the privacy by multiple Key Privacy Authorities (KPAs). In this scheme KPS selects its own master key and compute its public key. The by collaboration among KPAs the system public key is calculated.

3. THE ADVANTAGES OF IBC TO MANET:

One of the best advantages of IBC to MANET is its Easier to deploy without any infrastructure requirement. This saves certificate distribution, while bringing "free" pair wise keys without any interaction between nodes. Its resource requirements, regarding process power, storage space, communication bandwidth, are much lower. The public key of IBC is self-proving and can carry much useful information. Secure routing is an important in case when we transferring data and critical information between source and destination. Without a proper security method, a secured routing information and data transfer will be easily compromised.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

4. SECURITY PROBLEMS IN MANET:

One of the main challenges in MANET is to identify secure routing information. Mobile ad hoc networks eliminate the need for any infrastructure support by relying on the mobile wireless nodes themselves to collectively perform all networking functions, such as route discovery update or data transactions. The characteristics of ad hoc networks make them susceptible to numerous attacks. The wireless links are inherently vulnerable and compounded by irregular connectivity between the nodes due to the shared wireless channel. Frequent connectivity problems are also caused by node mobility where nodes are free to leave the network, resulting in an unpredictable and dynamic network topology.

These inherent vulnerabilities make it easier for attackers to compromise the networking infrastructure in the absence of robust security mechanisms. When an attacker succeeds to access information of another node illegally, the victim node is called the compromised node. Once node has been compromised, fake routing table can be distributed through the network and sensitive and critical information through these compromised nodes can be easily trapped. Wireless devices are vulnerable to active and passive attacks. Secured routing information used to transfer data from one node to another node is difficult task to sustain [16]. Many solutions are proposed to solve these attacks including trust management and cryptography methods [17]. Cryptography mechanisms have played significant roles for providing security. Key management is one of the fundamental methods of cryptography that is set of techniques which support the generation, exchange, storage, Use and replacement of keys (public/private key) among authorized entities. Identity-Based Cryptography (IBC), is a method that public key generated based on user's identity.

5. OVERVIEW OF KEY MANAGEMENT:

Cryptographic methods are one of the significant ways in order to provide security in mobile ad hoc network. Key management in Identity-Based Cryptography includes generation, distribution, protection and revocation of the keys. In the following elaborated some methods of Identity based Key Management in mobile ad hoc network.

6. PROPOSED SYSTEM:

Security of MANET will continuously be under research and development in academia and Industry as advanced technology updates is made. More research on secure MANETs will focus on long term effects instead of most expeditious results. To continually focus on achieving concrete results, some researchers contribute to MANETs security by dealing with real specific problems. Our previous work (Wu & Chen, 2008) is the investigation of attacks and countermeasures in MANETs according to different network layers.

More to drive for results,Kannhavong (Kannhavong, Nakayama, Nemoto, & Kato, 2007) did a survey on routing attacks and countermeasures against those attacks in MANETs after our work. Certainly tobalance the drive for expeditious results and long term effect, our current research is based on the foundational knowledge of security research of MANETs in which we fully investigate the cryptographic primitives by our roughly categorized techniques, and cover a variety of topics ranging from security routing protocol to broadcast communication, group key management, composite key management scheme and single cryptography techniques such as batch verification.

Compared to previous works (Kannhavong, Nakayama, Nemoto, & Kato, 2007; Wu & Chen, 2008), we look for ways to improve the long-term research results of security of MANETs As an adventurous trial, we effectively study applied cryptography to overcome difficult obstacles in understanding complicated security designs in this survey chapter.

The previous rapid advancement of cryptography showed the result of reducing the computational costs of outstanding cryptographic primitive operations in algorithms. In addition, the computation can be accelerated by using dedicated cryptographic hardware with cheaper hardware in the future. To support the above fact, in the IKM scheme's performance evaluation, IKM's computation cost as an IBC scheme is not only compared to RSA operations; however, Zhang (2006) also prompted us that the Barreto approach can expedite the Tate pairing to be up to 10 times faster than previous methods although the implementation is still underway.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

As a practical approach, researchers in the security of MANETs may pay attention to applied cryptography research results in time to fully take advantage of performance gains through improved algorithms in applied cryptography. As always, key management is a fundamental and challenging issue, and with rapid advancement in cryptography research, it brings more topics to the research field. With wireless network security technology advancing more quickly in our daily business life, it is much easier to form a MANET. The cryptographic techniques always play a major role in the design of each stage of the key management. The art of the design can be better evaluated from the conceptual level to the implementation of the simulation study.

The security of design will be dissected more by the research community and the new design will come out quickly and easily reusable as popular "design patterns" using cryptography terminologies. More variations in selection chosen by the designer will still heavily depend on the knowledge and skills level of cryptographic techniques, such as hiding the real identity of a vehicle in the IBV scheme, there are several alternative designs beside the ElGamal type ciphertext.29 The privacy issues and all other non-cryptography based security solutions can also be under the research community work mainly seen from data mining and machine learning area; for example, privacy model and algorithms, attacks using background knowledge and patterns (Aggarwal, & Yu, 2008).

It is not required that we have From a network research perspective, the MANET specific area needs to be looked into when security routing or key management issues are required. Because there are a variety of cases involving MANETs, the network scalability, computer cost, and resource constraints vary and may have to be considered case by case, such as vehicular sensor network, it is more relaxation power and processing constraints than MANETs, and the vehicle has temporary infrastructure access via road-side units as seen in the IBV scheme and public hot-spots. The symmetric cryptography and asymmetric cryptography, and their customized usage according to different network stages, will always be a challenge to cover the wide Range of network layers in MANETs. The current cryptography library and available MANET simulator or self-developed simulation study also will be advanced by the talent of the research community in different areas.

7. PROPOSED ALGORITHM:

The proposed algorithm for IBC-t method is defined as follows:

1) Start
2) Read UID/t
3) Read Data
4) Setup Phase □□Master Public/Private Key
5) Extract Phase □□Generate Public/Private Key
6) Encrypt Phase □□Encrypt message
Mpk , $Pubk$, $f(Pubk)$, $m \epsilon M)$
ii. (Compute Master Private Key & Private Key
Msk , $Privk$, $g(Privk)$, $c \epsilon C)$
iii. ($Privk$
□□$c)$
1. No: Discard Packet
2. Yes: Decrypt Packet
7) Decrypt Phase □□Decrypt Message
8) End

8. DESIGN IBCMETHOD:

The proposed algorithm is described in this section. The main idea of this algorithm is applying unique and small parameter include identity ti and ID in Identity-Based Cryptography method for increasing the performance of authenticity of entity. This attributes leads to reduce impersonating, packet dropping and routing attacks.

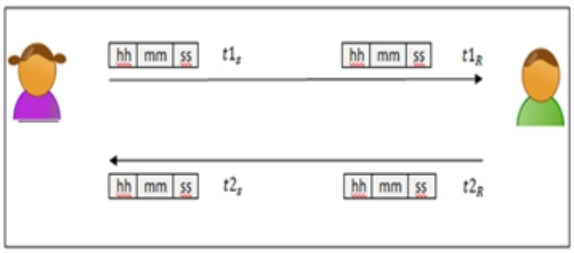

Fig. 1.Transaction for key management.

As Fig. 1 demonstrates, 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.

In this scheme the public key is based on User ID and the unique time, this combination leads to reduce the possibility of impersonation and enhance the authentication process of user in the network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

In this scheme is: $IDtistiPKG$ mod p, finding $tistiPKG$ is hard
Consider these assumption public/private key are as Follow:
Master Public Key = $mPub$
Master Private Key- K (d, n) = $mPriv$
d = 1/emod $(p\text{-}1)$ $(q\text{-}1)$
Public key = ID || tis || $mpub$
T= tis□□□□□□□□□□□□$tiPKG$Private Key= (ID || tis) (1 e mod $(p-1)$ $(q-1)$) mod n
General process of the proposed model is depicted in Fig.2.

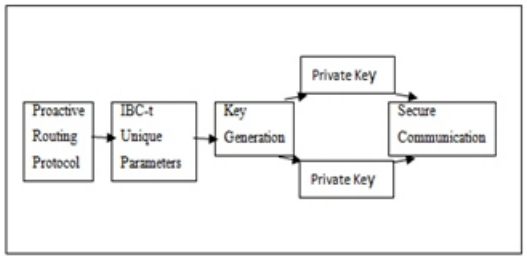

Fig. 2.Model process.

9. SECURITY ANALYSIS:

In regard to the previous methods of IBC - their main ideas, parameters, and weaknesses - this research has more focused on eliminating the relevant vulnerabilities and enhancing the confidentiality and authenticity by proposing IBC-t.

A secure routing communication requires Confidentiality that preserves data secret to unauthorized entity, Integrity that impede data from alteration, Authentication that verifies data from authorized entity, and Non-repudiation that ensures an entity cannot deny their activities through communication.

One of the fundamental issues that this method point out is that during authentication process and communication there is not any trusted third party. Secondly, in regard with Cluster heads are assumed as PKGs, we apply threshold for key management in the network. As a result single point of the failure is eliminated.

It means if a mobile node within the network is compromised, the authentication still performed by other nodes. In addition a few packets are required to achieve the mutual authentication.

Moreover, in order to provide secure communication proper security countermeasures should be performed by applying strong authentication for message transmission. IBC-t proposed a method to authenticate message by using Combination of ID and unique factor „t⍰ (transmission time). There are many attacks in the network which comes from lack of strong authentication such as: Impersonating another node to spoof route message; Advertising a false route metric to misrepresent the topology; Flooding Route Discover excessively as a DoS attack; Modifying a Route Reply message to inject a false route; Generating bogus Route Error to disrupt a working route; probability of these attacks by adding a small and unique factor which generates Public/Private keys in a reasonable time and does not lead to traffic or overhead through the network.

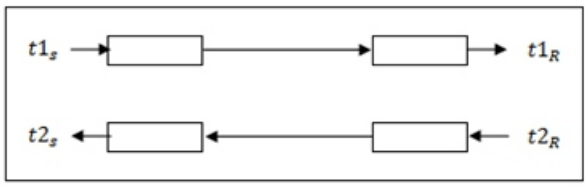

Fig.3. Unique time in packet transaction.

Fig. 3 illustrated the transaction among two nodes, there is a unique time for sender and receiver (t1S for Sender and t2R for Receiver). This unique small factor is combined with the User ID (tiuser|| User ID). The combination of two unique user"s identification leads to enhance the authentication of user and reduce the-possiblity of impersonation. Another important factor in order to applying a suitable method to mobile ad hoc network is considering communication overhead for these methods.

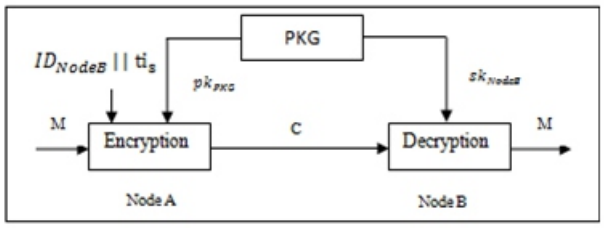

Fig.5. Identity based scheme.

As Fig. 5 shows the combination between ID and ti does not incur a latency in the network. Provide the strong authentication prepares the confidentiality and integrity in the network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Many active and passive attacks are happened because of lack of the strong authentication. Attacker interferes illegally through the communication and then can deny his activities easily if there is a weak identification and authentication process. Strong authentication will reduce impersonation attacks. Impersonation attack is a severe threat to the security of mobile ad hoc network [4]. If there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them similar non-malicious nodes. In this way, the compromised nodes can join the network as the benign nodes and begin to malicious activities, such as propagate fake routing information and gain inappropriate priority to access some confidential information.

10. CONCLUSION:

Key management is one of the primary issues in mobile ad hoc. This research presents IBC-t method key management for MANET. IBC-t is a certificate less solution which allows public and private keys of mobile nodes proceed from combination of their known ID and some other factors while is simple and unique without complex computationally.

The concept of IBC-t method is a novel method of applying ID-Based public/private key which not only guarantees high-level authentication of mobile nodes but also facilitates efficient key generates which leads to resilience against node compromising. Most existing security methods for mobile ad hoc networks are based on applying public key certificates. The finding of this research enhances authenticity and confidentiality through the network by reducing the computational time and enhancing the authentication of mobile nodes.

11. Acknowledgment:

First and foremost I would like to thank my guide Prof.R.A.Auti,,MsNehaKhatri-Valmik,Prof.Saad Siddiqui Prof.SantoshTakle for their guidance and support. I would forever remain grateful for the constant support and guidance extended by guides, in making this paper. The invaluable discussion they had with me, the penetrating question they had put to me and constant motivation, has all led to development of this Paper.

12. References:

1.BruceSchneire,"Applied Cryptography". John Wiely& Son, Inc.1996.

2.ShohrehHonarbakhsh, Liza Binti Abdul Latif, Azizah-bt Abdul Manaf, and BabakEmami "Enhancing Security for Mobile Ad hoc Networks by Using Identity Based Cryptography"International Journal of Computer and Communication Engineering, Vol. 3, No. 1, January 2014.

3. Shushan Zhao, AkshaiAggarwal, Richard Frost, XiaoleBai" A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks".

4. roozmunjal, PinkiTanwar,NitinGoel"Optimized Solutions to Cryptography for Securing MANETs and Analyze Using Reputation System" International Journal of Computer and Communication Engineering, Volume 3, Issue 5, May 2013.

5. Charles E. Perkins "Ad Hoc Networking".

6. 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 onComputer Communication and Networks, 2011.

7. Shushan Zhao Computer Science DepartmentUniversity of Windsor "Application of Identity-Based Cryptography in Mobile Ad Hoc Networks".

8.Jianmin Chen and Jie Wu "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks".