A Survey of Identity Based Key Management in Mobile Ad Hoc Networks

Pragnesh Patel\#, Vaghela Vimalkumar B\* 

Computer Department, L.D. College of Engineering

\#pragnesh.4400@gmail.com

\*vimalvaghela@yahoo.com

Abstract

Today use of Ad Hoc Networks is increased gradually in our day to day life, and there are vulnerabilities in Mobile Ad Hoc Network (MANET) due to their natural characteristics. There are several cryptographic mechanisms for MANET, one of them is Identity Based Cryptosystem and Key Management for security and efficient key management. Identity Based Cryptography is found to make key management simple and reduce memory cost of conventional public key system. In this paper we will study about existing Identity Based Key Management Schemes, their pros and cons and comparing their main features. This study will help users and researchers to build strong and robust key management scheme.

1. INTRODUCTION

As there is rapid increase in development of computers and communication technologies mobile ad hoc networks has gain a lot of attention from researchers and developers. Mobile Ad Hoc Networks are wireless and infrastructure less networks. They are self-organized and self-configuring. In MANET nodes acts as both routers and communication end-points. Mobile Ad Hoc Networks’ wireless and dynamic nature leaves them more vulnerable to different security attacks. It is widely known that Cryptographic mechanism can provide strongest techniques against most of the vulnerabilities. Traditional Cryptographic system can be divided into symmetric and asymmetric ones, based on the way key is used. Symmetric systems are not scalable to apply in MANET because secret keys must be shared either by a secure pre-established channel or before network formation. Traditional asymmetric systems need a trusted third party to issue certificates and ensure that public keys belong to particular identity. So establishing trusted third party is challenging in MANET due to their natural characteristics and lack of trust model.

Key Management is a set of procedures and techniques to establish and maintain keying relationships between authorized entities. Keying relationship is the process by which nodes share their keying materials that includes public/private key pairs, secret keys, initialization parameters, and nonsecret parameters supporting key management in various instances \[1\]. An ideal Key Management must satisfy following requirements:

- Not having a single point failure.
- Compromise of certain nodes doesn’t affect the security of non compromised nodes.
- Being able to revoke keys of compromised nodes and updates keys of non compromised ones.
- Must be efficient in terms of storage, computation and communication.

This paper organized as follows: In section 2 we discuss about Identity Based Cryptosystem. Section 3 describes various Identity Based Key Management Schemes with their prons and cons. Section 4 draws some conclusions.

2. IDENTITY BASED CRYPTOSYSTEM

The concept of Identity Based cryptography(IBC) was suggested by Shamir \[5\]. In this system identity of nodes are used as their public keys like email, IP address, MAC address, etc. Private Key is generated by trusted third party called Private Key Generator (PKG).

The main advantages of IBC are simple key management process and reduce memory cost compared to traditional system. In IBC every node is able to derive public key of other nodes without exchanging any data. They only need to maintain PKG parameters, not public keys of all nodes. In IBC every pair of nodes A and B is able to compute a pairwise pre-shared key without any interaction. This pre-shared key can be used in authenticated encryption scheme and authenticated key exchanging.

The disadvantage of IBC is that private key of all users must known to PKG. It requires safe channel for exchanging private keys with network nodes. An IBC scheme doesn’t preserve the privacy of network node as public key can be directly derived from node identity. Private keys of all users are known by PKG so if PKG is compromised then it will create serious problems. Single point failure can be occurs at PKG.

The important part of Identity Based Cryptosystem is Identity Based Key Management. A proper Identity Based Key Management greatly affects the performance and efficiency of the system. There are several Identity Based Key
Management schemes for MANETs. In the next section we are going to discuss various Identity Based Key Management schemes.

3. IDENTITY BASED KEY MANAGEMENT

Identity Based Cryptography Originated from the need to make key management simple and reduce memory storage cost. Several Identity Based Key Management schemes can be found in literature. This paper presents most important schemes for MANETs, discussing their approaches, strengths and weaknesses.

A. Khalili-Katz-Arbaugh:

This Key Management Scheme is combination of Id-based and threshold techniques. All nodes that initialize the MANET form a distributed PKG set, called the “Threshold PKG”. The Threshold PKG has master private key that is distributed among n nodes using a “t-over-n scheme”. So none of this node is able to reconstruct the master private key based on its own information. The master public key is distributed to all nodes of the network, including those joined later.

An identity of node is used as their public key while their private keys are computed by nodes of threshold PKG. According to threshold scheme to receive its private key a node has to present its identity to at least t nodes of threshold PKG, and each one will send part of private key back. On receiving t correct parts, node computes its own private key.

The use of threshold PKG eliminates the single point failure. An attacker has to comprise at least t nodes to discover private key of any user. Honest nodes only need to contact t nodes in order to obtain their own private keys, making the scheme resilient to temporary loss of connectivity.

This scheme assumes that identities are stored in hardware and cannot be altered. So an attacker who alters its own identity or create false identity can be threatening to it. This scheme doesn’t have any revocation and key renewing.

B. Deng-Mukherjee-Agrawal:

This key management scheme has two components: Distributed Key Generation and Identity Based Authentication.

The key generation component provides the master key of network and public/private key pair of each node in network. The Identity based authentication provides end to end authentication and confidentiality. If authentication process succeeds, these node exchange session key that will be used for further communication. Public/private key pair is computed and distributed in same fashion as Khalili-Katz-Arbaugh scheme. A node has to contact at least t PKG nodes. Presenting its identity and requesting private key generation service. Each PKG node generates a secret part of the private key and send it to the requesting node. On receiving t parts of the private key a node can build its own private key and join the network.

To securely transmitting the generated part of private key, the requesting node must generate and present temporary public key when sending the request. Each PKG node sends the generated part of private key encrypted using that temporary public key.

Like the Khalili-Katz-Arbaugh scheme this scheme also suffers from creation of false identity and alerts its own identity. This scheme doesn’t address key revocation and key renewing.

C. Identity Based Authentication And Key Exchange

This scheme consists of two techniques: a basic MANET-IDAKE (Identity based authentication and key exchange) and a fully self-organized MANET-IDAKE. Both techniques uses symmetric cryptography and pairing based keys. These techniques can be specified by following six algorithms: Setup, Extract, Distribute, Compute shared keys, Key renewal, Key Revocation.

The setup algorithm provides public and private key of PKG and announces the public key of PKG to the network. The extract algorithm provides the private key of network nodes and declares that their public key is their identity. The distribute algorithm distributes private keys to all network nodes. The compute shared key algorithm is required when node A wants to communicate with node B, computing symmetric pairing based key that will be used for communication. The key renewal algorithm is applied when key of node expires or revoked. The key revocation algorithm defines the rule to revoke keys of compromised nodes, combining neighbourhood watch with accusation scheme. All these algorithm works in same fashion for both techniques.

Basic IDAKE has two phases: the initialization phase with access to an external PKG that includes setup, extract and distribute algorithms. Second phase is running system phase without access to PKG that includes compute shared keys, key renewal and key revocation phases. In this technique external PKG must initialize all devices before they join the network.

In fully self organized MANET-IDAKE all tasks are performed by network node themselves without any external PKG. The work of external PKG is assigned to network nodes according to t-over-n threshold scheme. But self organized scheme doesn’t specify how private keys are distributed to the nodes.

The MANET-IDAKE has low bandwidth and low memory requirement due to the efficient Id Based scheme.
The basic MANET-IDAKE has single point failure. In fully self organized MANET-IDAKE this problem is eliminated.

D. Identity Based Key Management (IKM)

Identity Based Key Management is a combination of Id Based Key Management and threshold cryptography. In IKM public and private of each node composed of two elements: node specific id based element and network wide common element. The node specific element ensures that secrecy of non-compromised node is not revealed due to the presence of several compromising nodes. Network wide common element enables very efficient network wide public and private key update via a single broadcasted message.

IKM contains three phases: Key Predistribution, Key Revocation and Key Update. Key predistribution starts during network initialization in which a PKG determines sets of system parameters and preloads every node with required key materials. After that PKG distributes its functionality to t distributed PKGs, called D-PKGs. Private master key is distributed based on t-over-n threshold scheme. This technique will enable secure and robust key revocation and key renewal. Key revocation must be explicit in order to minimize the damages from compromised nodes. During the network operation if any node suspects that other node is malicious or has been compromised, it sends signed message to D-PKG. A node is considered malicious when number of accusations against it reaches to some threshold value called revocation threshold. In IKM nodes must update their public/private keys in periodic intervals or number of revoked node reaches a predefined value.

Table 1 summarizes the main characteristic of the above presented Id Based Key Management schemes.

<table>
<thead>
<tr>
<th>Threshold</th>
<th>PKG</th>
<th>Key Renewal</th>
<th>Key</th>
<th>Basic-IDAKE</th>
<th>Distributed-IDAKE</th>
<th>IKM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Internal</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Internal</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

4. Conclusion

We have already studied some existing Id based key management schemes. These key management schemes have a simple management process and reduce memory storage cost compared to other traditional methods. Some of the Id based key management schemes doesn’t provides the key revocation and renewal techniques. The computational complexity of Id based key management scheme depends on the implementation of key revocation and renewal algorithm. In future we may try to make key revocation algorithm efficient future we may try to make key revocation algorithm efficient to improve performance of existing key management schemes.

REFERENCES


