IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

An Analytical Study on Key Management in Mobile Ad-Hoc Network

Dr. S. Dhanalakshmi[1], R. Anupriya[2]

Prof& Head, Computer Science and Applications, Viveganandha College of Arts and Sciences for Women (Autonomous) Elayampalayam, Tiruchengode, Namakkal[1]

Research Scholar, Department of Computer Science, Vivekananda College of Arts and Sciences for Women (Autonomous) Elayampalayam, Tiruchengode, Namakkal[2]

Abstract: Mobile Ad hoc Network (MANET) is a collection of wireless infrastructure less network. The topology of the network changes continuously. Due to the dynamic structure of MANETs, they are prone to various types of attacks. The traditional security solutions for MANETs are inadequate, hence security should be maintained at all the levels. Many key management schemes for MANETs are presented to solve various security problems. Usually the cryptography techniques are used for secure communications in wired and wireless networks. Identities (ID)-based cryptography with threshold secret sharing, ECC and Bilinear Pairing computation are popular approaches for the key management design. The task of key management includes keys for generation, distribution and maintenance. Key maintenance includes the procedures for key storage, key update, key revocation. Thus the security is enhanced at various levels which prevent strong malicious attacks. In this paper, we adopt these approaches to construct tree structure and cluster structure ad hoc network and then give out a three-level security communication ad hoc network.

Keywords: MANET, wireless security, Elliptic Curve Cryptography, ID-based key management

I. INTRODUCTION

A mobile ad-hoc network (MANET) is formed on-the-fly and it is also a convenient infrastructure less communication network. So we can construct MANET on demand without support from central servers. MANETs are especially suitable for communications in critical situations such as battlefield, emergency and rescue missions. The asymmetric cryptography is widely used because of its versatileness (authentication, integrity, and confidentiality) and simplicity for key distribution. The symmetric approach has computation efficiency, yet it suffers from potential attacks on key agreement or key distribution. Many encryption and key sharing techniques are implemented in MANETs.. Key management is a basic part of any secure communication. Most cryptosystems rely on some underlying secure, robust, and efficient key management system. Key management deals with key generation, storage, distribution, updating, revocation, and certificate service, in accordance with security policies

II. CHARACTERISTICS OF MOBILE AD HOC NETWORKS

MANETs with variants of the given characteristics. For example, MANET will take on a self-organized nature, and hence the end-users will set up and manage the network themselves. This means that an offline authority may not be available. Another example of varying characteristics emerges from MANETs formed by sensor nodes or laptop computers. Clearly schemes designed for MANETs formed by laptop computers will not have the same limitation on memory, energy (battery), and computational resources as those formed by sensor nodes.

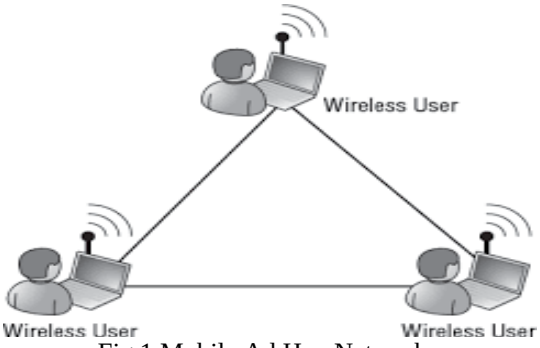

Fig.1 Mobile Ad Hoc Networks

The application may dictate the characteristics of the MANET and the degree to which some characteristics will influence the design of a suitable scheme.

III .OVER VIEW OF KEY MANAGEMENT

Key management is a basic part of any secure communication. Most secure communication protocols rely on the substantial secure, robust, and efficient key management sys-tem. Key management primitive and trust model are described below.

3.1 Key management primitive

- First, 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 (KEK) approach could be used at local hosts.
- Second, key distribution and key agreement over an insecure channel is at high risk and suffers from

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

potential attacks. In the traditional digital envelop approach, a session key is generated at one side and is encrypted by the public-key algorithm, then it is delivered and recovered at other end. In the Diffie-Hellman (DH) scheme, communication parties of both sides exchange some public information and generate a session key on both ends.
Several enhanced DH schemes have been invented to counter the man-in-middle attack. Security has become a hot research topic in mobile ad hoc networks.

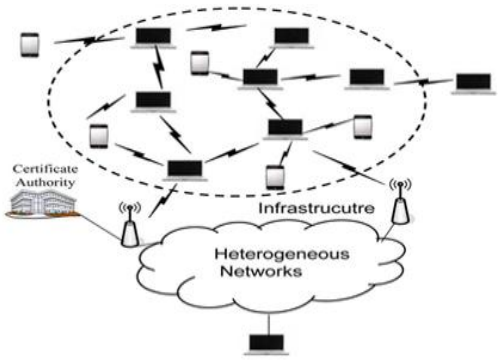

Fig.2 Key Management

Elliptic curve Cryptography, Identity based Cryptography and Shamir (t, n) threshold cryptograph. Nonlinear pair computation is applied to realize secure key management and communication. Shamir (t, n) threshold cryptography is used to build three level security in ad hoc network. This scheme can be applied to dynamic topology and different sizes of ad hoc network. It can get a high security with few traffic and computation.

3.2 Trust models

The services must provide following are: Trust model, Cryptosystems, Key creation, Key storage and Key distribution. The Symmetric Key Cryptography scheme can usually be applied to MANET. These schemes are based on the key deployed in advance which include single key used by all nodes. Each node shares a single key with another single node or multi-nodes.

3.3 Centralized trust model

The centralized trust model, there is a well-trusted entity known as a TTP . ATTP is an entity trusted by all users in the system, and it is often used to provide key management services. Depending on the nature of their involvement, TTPs can be classified into three categories: inline, online, or offline.

An online TTP participates actively but only for management purposes, as the two parties communicate with each other directly. An offline TTP communicates with users prior to the setting up of communication links and remains offline during network operation.

3.4 TTPs in symmetric key management systems

TTPs have been implemented in both symmetric and asymmetric key management systems. Key Distribution

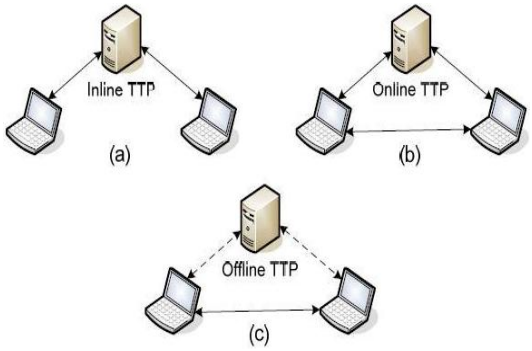

Fig.3 Categories Of Trust Models

Centers (KDC) and Key Translation Centers (KTC) are TTPs in symmetric cryptographic key management systems and the certification authority (CA) is the TTP in public key management systems. KDC and KTC simplify the symmetric key management since each user does not have to share a secret key with every other user. Instead, it only needs to share one key with the TTP.

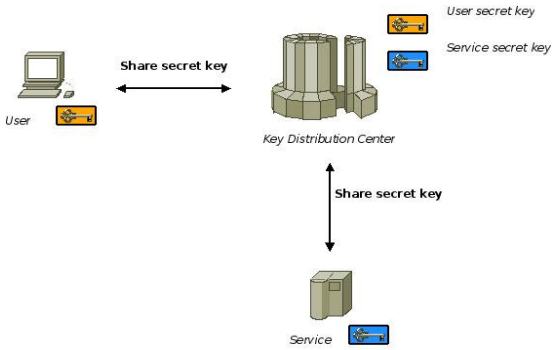

Fig.4 Key Distribution Centers

This reduces the total number of keys that need to be managed from n(n − 1) ton, where n is the total number of users. Figure 4 illustrates the protocols by implementing KDC or KTC.

IV. IDENTITY-BASED KEY MANAGEMENT

4 .1 Node identity-based Public Key and key update

If a node in MANET wants to obtain its own public/private key pair, it should contact at least t neighbor nodes, present its identity and send the requests to t PKGs nodes in order to acquire identity-based public key and private key. All the network nodes share the master private key, and each of these nodes could be the PKG service node. Received the request signal, the t nodes work together to issue the public key / private key pair for the request node.

4.2 Node Join

When a new node joins the cluster, nodes in the cluster only update the cluster master key (public key / private key) in the cluster. But they will keep old / new key. And nodes in other cluster will not update their key.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

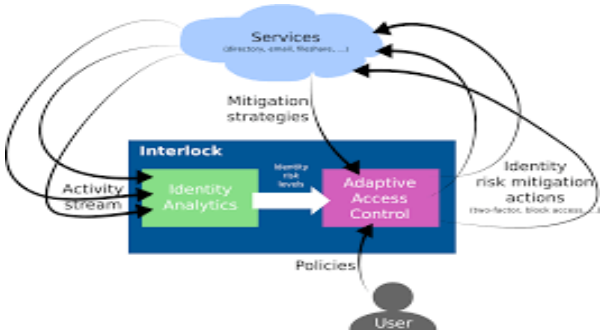

Fig.5 Identity Based Key Management

A node in the cluster communicates with other cluster nodes, it should adopt old key. And it only adopts new key when communicating with the new node of the cluster.

V.ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

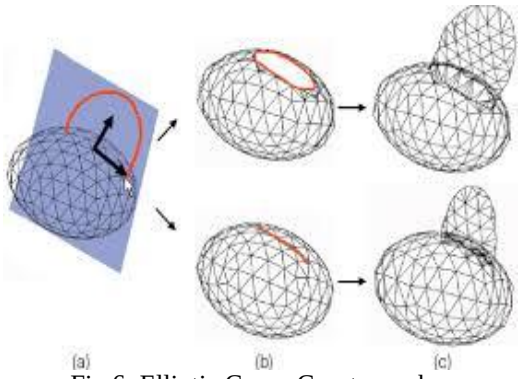

Fig 6: Elliptic Curve Cryptography

ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security.

VI. BILINEAR PAIRING COMPUTATION

Bilinear pairings play an important role in cryptographic protocols. This leads to the development of efficient pairing computations since the implementation of pairing based cryptosystems involves pairing evaluation. Computing the classical Tate and Weil pairings requires log2 r Miller iteration loops where r is the order of the points. If the number of the Miller iteration loops is less than log2 r/φ(k) where k is the embedding degree of elliptic curves, the corresponding pairing is called super-optimal.

VII. CONCLUSION

Security is an important issue for mobile ad hoc networks. For security we mainly consider the following attributes: availability, confidentiality, integrity, authentication, authorization and non-repudiation. It is well known that ECC is appropriate for such nodes due to its smaller keys and its higher security levels. The security is thus enhanced at various levels which prevent strong malicious attacks. In the existing method security is obtained by identity based scheme. Specific types of MANETs, such as sensor networks, the symmetric key management scheme is dominant.

An example of a symmetric approach is the random key pre-distribution insensor networks. In summary, based on different assumptions, many key management protocols have been proposed for MANETs. All key management approaches are subject to various restrictions such as the mobile device's available resources, the network bandwidth, and Manet's dynamic nature. An efficient key management protocol for MANETs is an ongoing hot research area.

REFERENCES

1. Wan An Xiong, Yao Huan Gong, "Secure and Highly Efficient Three Level Key Management Scheme for MANET", proceedings of WSEAS transactions on computers, Volume 10, 2011.
2. HU Rong-lei, LIU Jian-wei, ZHANG Qi-shan. "Cluster-based key management scheme for ad hoc networks". Journal on Communications, china. Vol.29 No.10. October 2008. pp.223-228.
3. D. Wallner, E. Harder, and R. Agee, "Key Management for Multicast: Issues and Architectures", RFC 2627, June 1999.
4. Fiat A and Shamir A, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems" proceedings of the Springer-Veriag, 1999, pp. 306-314.
5. W. Luo, and Y. Fang. A Survey of wireless Security in Mobile Ad Hoc Networks:Challenges and Available Solutions. Kluwer Academic Publishers pp-319-364, 2003.
6. S. Burnett and S. Paine. RSA security's official Guide to Cryptography. RSA press, 2001. momhamod wireless networks. CRC press, 2003.
7. Y. Desmedt and S. Jajodiay Redistribution secret shares to a new access structures and its application. University of Wisconsin-milwaukee, 1997.
8. T. M. Wong, C. Wang, and J. M. Wing. Verifiable Secret Redistribution for Threshold Sharing Schemes. Carnegie Mellon University, 2002.
9. V. Shoup. Practical Threshold Signatures. Eurocrypt 2000.
10. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-Efficient Communication Protocol forWireless Microsensor Networks. Hawaii International Coference on System ScienceMaui, 2000.
11. A.Fiat, A.Shamir: How to Prove Yourself: practical Solutions to Identification and Signature Problems.
12. L.Guilou, J-J. Quisquater: A "Paradoxical" identity based Signature Scheme Resulting From Zero-Knowledge. Advances in Cryptology – Crypto'88, LNCS 0403, Springer (1988) 216-231.