ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

An Innovative Cryptographical Scheme for Mobile Ad-Hoc Network Security using Certificate less Public key Cryptography

Surbhi Tahanguria*[1], Deepak Kumar Xaxa[2]
*[1,2] MATS school of Engg. & Tech. Raipur, India
surbhitahanguria8@gmail.com

Abstract

A Mobile ad hoc Network (MANET) is a self-governing network comprised of free roaming nodes which communicate wireless by radio transmission. As MANET edge closer toward wide-spread deployment, security issues have become a central concern and are increasingly important. Various security mechanisms have been proposed, widely used, and proven to be effective in wired networks, but no single mechanism provides all the services required in a MANET. Due to certain characteristics of MANETs, some security mechanisms are not applicable to this environment. These certain characteristics of ad hoc networks include: lack of a network infrastructure and online administration, the dynamics of the network topology and node membership, the potential attacks from inside the network. In this paper we have proposed an innovative and secured, ACS (address based cryptography scheme) as a combination of Ad hoc node address and public/Private key cryptography. ACS is a certificate less public key cryptography solution which empowers efficient network-wide secure key update via a single broadcast message. It also provides general information about how to choose the secret key sharing parameters used with public key cryptography to meet desirable levels of security and authentication. Thus, it eliminates the need for certificate-based authenticated public-key distribution essential in conventional public-key management scheme.

Keywords: RSA, MANET, ACS, Diffie-Hellman.

Introduction

Wireless communication is the key to network availability anywhere and at any time. Today's wireless communication systems usually depend on pre-established communication infrastructure. Ad hoc implies that the network is formed in a spontaneous manner to meet an immediate demand and specific goal. Ad hoc networks have the ability to form "on the fly" and dynamically handle the joining or leaving of nodes in the network. Mobile nodes are autonomous units that are capable of roaming independently [2]. A mobile ad-hoc network (also known as MANET) is a self-organized wireless network of mobile nodes without any fixed infrastructure. Nodes roam through the network, causing its topology to change rapidly and unpredictably over time. New nodes can join the network, whereas at the same time other nodes leave it or just fail to connect (temporarily) because they move to a region that is not in the cover range of the network. Typical mobile ad hoc wireless nodes are Laptops, PDAs, Pocket PCs, Cellular Phones, Internet Mobile Phones, Palmtops or any other mobile wireless devices. MANET is a unstructured dynamic network comprises of mobile nodes that can join or walk out any time in the network. So, MANET is likely to be vulnerable to the malicious activities of intruders. Some of these problems may be solved or mitigated with the use of cryptographic protocols. Cryptography is then used to provide a general design framework. Cryptography techniques used in MANETs can be classified into two categories, namely, Symmetric Key based and Asymmetric Key based.

- In symmetric key based schemes, if an attacker compromises the symmetric key of a group of users, then all encrypted messages for that group will be exposed.
- Asymmetric key based schemes can provide more functionalities than symmetric ones, e.g., key distribution is much easier, authentication and non-repudiation are available, and compromise of a private key of a user does not reveal messages encrypted for other users in the group. However, they are generally computationally expensive.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

The major limitation of these schemes is that most of them rely on a trusted third party, thus not fulfilling the self-organization requirement of an ad hoc network.

Literature Survey

Various researches have been carried out in this area to increase the security of MANET.

B. Clifford Neuman [17] uses a series of encrypted message to prove a verifier that a client is running on behalf of a particular user.

Wei Liu, Yanchao Zhang [18] presents ID based cryptography and key management thus eliminating the certificate based authentication public key distribution.

A. Rex Macedo Arokiaraj [19] state that high level authentication is provided by the combination of adhoc node adess and public key cryptography.

Ashwani Garg and Vikas Beniwal [20] present some available routing protocols and most common attack patterns against ad hoc network. They also state that no protocols are fully secured from attacks hence must choose a combination of techniques.

Athulya M S and Sheeba V S [21] provide the combined approaches for key generation, key exchange, data encryption and routing protocol for securing MANET.

After surveying different techniques we define the Merits and Demerits of techniques in the table:

Techniques	Main Idea & Contribution(s)	Merits	Demerits
RSA based cryptography	Uses a variable size encryption block and a variable size key. The key pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules	1. increased security and convenience 2. Private keys never need to transmitted or revealed to anyone. 3. Can provide a method for digital signatures. 4. Best suited for an open multi-user environment.	1. much slower than other symmetric cryptosystems 2. may be vulnerable to impersonation, 3. The length of plain text that can be encrypted is limited to the size of n=p*q.
SHARED KEY Cryptography	The Diffie-Hellman key agreement protocol uses the secret information on the one end and the public information on the other end for communication between source and destination nodes.	1. The security fact ors with respect to the fact that solving the discrete logarithm is very challenging, and that the shared key (i.e. the secret) is never itself transmitted over the channel.	1. There is no identity of the parties involved in the exchange. 2. It is easily susceptible to man-in-the-middle attacks. 3. Computationally intensive. -cannot be used to encrypt messages. -lack of authentication.
Identity-Based Cryptography	Allows public keys to be derived from entities known identity information, thus eliminating the need for public key distribution and certificates.	1. No preparation is required on the part of the recipient to receive an encrypted message. 2. No need to managing a public key infrastructure. 3. decryption- and signature can take place on the server. 4. Improved user-friendliness 5. Less public information about your enterprise need be revealed.	1. inherent key escrow property 2.lacks key revocation 3.high level of assurance required in the PKG.
Address Based Cryptography	ACS broadcasts encrypted message containing its own private key which increases security threats for MANET.	1. Each node's public key and private key is composed of a node address element and a network-wide common element. 2. Common key elements enable very efficient network-wide	1.The private and public key generation does not ensure uniform key distribution,

		public/private key updates via a single broadcast message. 3. efficient key agreement, public-key encryption, authentication based on such public/private and secret key distribution similarly to ACS broadcasts encrypted message containing its own private key which increases security threats for MANET	

Problem Identification

MANET is a group of mobile, wireless device which communicate between them without the assistance of any infrastructure. As the mobile ad hoc network edges closer toward widespread deployment, security issue have become more concern and important. So introducing the security methods provided to MANET, to securely transmit the data. Since both data and ad- hoc network are complex to handle, some simple and efficient methods are require. Crypto graphical scheme is efficient to handle this issues. As we surveyed RSA algorithm much slower than other symmetric cryptosystems and that may be vulnerable to impersonation.

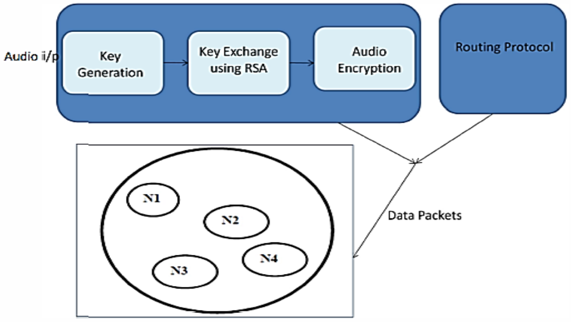

Fig.-1 Existing Network Model

ACS uses the node address with certificateless cryptography to give the end to end authentication. Route invention in ACS is based on route invention packet from source node and route reply packet from destination node. The route packets are encrypted based on ACS.

Proposed Methodology

We are proposing ACS (address based cryptography) scheme as a combination of Ad hoc node address and public key cryptography. ACS is a certificateless public key cryptography solution. Thus, it eliminates the need for certificate-based authenticated public-key distribution essential in conventional public-key management scheme.

In ACS, each node's public key and private key is composed of a node address element and a network-wide common element. Common key elements enable very efficient network-wide public/private key updates via a single broadcast message. It also discuss efficient key agreement, public-key encryption, authentication based on such public/private and secret key distribution.

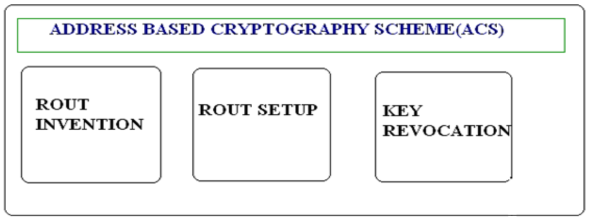

Fig. - 2 ACS

In ACS only authorized nodes participate at each hop between source and the destination. Assume key generation is known by all authorized nodes.

Route Invention in ACS

A simple ad hoc network, when the first authorized node enters in the network is treated as a node N1 and consecutive authorized nodes are namely N2, N3, and N4 and so on based on its entry time in the network. Then node N1 to N4 updates No. of nodes available in the network. Whenever a node N1 desires to undertake secure communication with another node N4, the source node N1 generates its encrypted broadcast message (RDP) and send to the network and waits for a reply message from node N4. N1 broadcast: E[RDP, ADN4 , [EnTN1, CuTN1 ,ExTN1]] PrKN1 - (1) The broadcast message includes a packet type identifier ("RDP"), the node destination address ADN4 and the combination of EnTN1, CuTN1, ExTN1 with node N1 private key PrKN1. N3 broadcast: E[RDP, ADN4 , {[EnTN1,CuTN1, ExTN1]] PrKN1] PrKN3 – (2) The receiving node encrypts the contents of the message, appends its own encryption scheme, and forward broadcasts the message to each of its neighbours.

P1= N1 broadcast: E [RDP, ADN4 , [EnTN1, CuTN1 ,ExTN1]] PrKN1 - (1)

P2= N3 broadcast: E [RDP, ADN4 , {[EnTN1,CuTN1, ExTN1]] PrKN1] PrKN3 – (2)

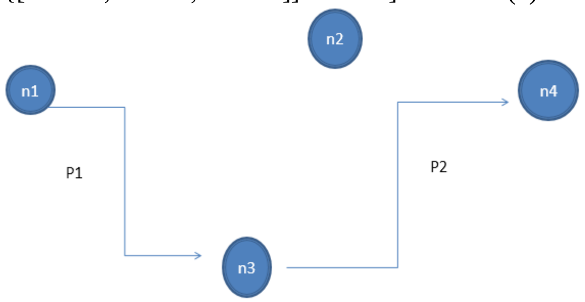

Fig.-3 Route Invention in ACS

Route Invention in ACS

The reverse steps to find the path From N4 to N1. First the REP message has sent to neighbour N3. That is the node address N4 is encrypted by private key of N4 (3). Then the REP message reaches to node N1 to find the actual path. N4 N3: E [REP, ADN1,] PrKN4 N3 N1: E [REP, ADN1] [PrKN4] PrKN3. After receiving the RDP, the destination unicasts a reply (REP) packet back along the reverse path to the source. In between node verify its encrypted information and pass the REP message to its next node in a reverse direction. Each node checks the encrypted information of the previous count C as the REP is returned to the source.

N4 N3: E [REP, ADN1,] PrKN4 - (3)

N3 N1: E [REP, ADN1]]PrKN4] PrKN3 - (4)

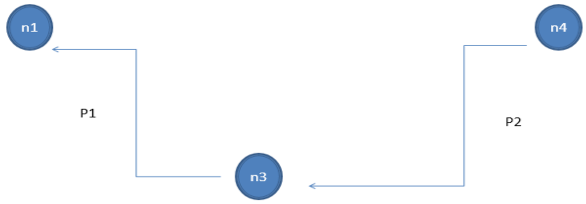

Fig.-4 Route Invention in ACS

Key Revocation

The system generates key pair is denoted by as {PuK, PrK} A encryption by the PrK can be verified by the well-known system public key PuK. Besides the system key pair, each entity N also maintains a personal RSA private and public key pair {PuKN, PrKN}. This pair of personal keys is used in end to end security to realize cipher key exchange, message privacy, message integrity and nonrepudiation. For encryption and Decryption following formula used:-

For encryption:-

Ch=(Str[i]+key[i]+ch1)%256

For decryption:-

Ch=(256+str[0]-key[0]-ch1)%256

Conclusion

Mobile ad hoc networks are an emerging research area with powerful applications. Security problem in wireless ad hoc network is not trivial to solve. Their natural characteristics make them vulnerable to passive and active attacks, in which misbehaving nodes can eavesdrop or delete packets, modify packet contents, or impersonate other nodes. In this paper, ACS labelled a solution to security provision in MANETs. ACS provides general information about how to choose the secret key sharing parameters used with public key cryptography to meet desirable levels of security and authentication. Thus, it eliminates the need for certificate-based authenticated public-key distribution essential in conventional public-key management scheme.

References

[1] *C.K. Tok: Ad Hoc Mobile Wireless Networks: Protocols and Systems, Pearson Education, pp. 28-30 (2002).*

[2] *X. Cheng, X. Huang and D.Z Du: Ad Hoc Wireless Networking, Kluwer Academic Publishers, pp. 319-364(2006)*

[3] *Shashi Mertra Seth, Rajan Mishra, "Comparative Analysis" of Encryption Algorithoms For Comunication", IJCST VOL.2, Issue 2, June 2011.*

[4] *H.M. Kader and M.M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms," Performance Evaluation, pp. 58-64, 2009*

[5] *keith Palmgren, "Diffie-Hellma n Key Exchange", February 2005, http://www.securitydocs.com /library/2978*

[6] *Y. Desmedt and Y. Frankel, "Threshold cryptosystems", in Advances in Cryptology - Crypto '89, Proceedings, Lecture Notes in Computer Science 435, G. Brassard, Ed., Santa Barbara: Springer - Verlag,1990, pp. 307 - 315.*

[7] *Dynamic group Diffi - hellman key exchange under standard assumption, Emmanual Bresson, LNSC 2332, page321 .*

[8] *A. Shamir, Identity-based Cryptosystems and Signature Schemes, Proceedings of CRYPTO '84, LNCS 196, pages 47-53, Springer-Verlag, 1984.*

[9] *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.*

[10] *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. 309–17.*

[11] *R.Rivest, A. Shamir, L.Adleman. "A method for obtaining digital signatures and public-key cryptosystems"z. Communications of the ACM, Feb 1978.*

[12] *B. DeCleene, L. Dondeti, S. Griffin, T. Hardjono, D. Kiwior, J. Kurose, D. Towsley, S. Vasudevan, and C. Zhang. "Secure Group Communications for Wireless Networks", in proc. IEEE MILCOM01, ct. 2001*

[13] *L. Zhou, Z.J. Haas, Securing ad hoc networks, IEEE Network 13 (6) (1999) 24–30.*

[14] *A. Khalili, J. Katz, W.A. Arbaugh, Toward secure key distribution in truly ad-hoc networks, in: Proceedings of SAINT Workshops'03, vol. 22, 2003, pp. 342–346.*

[15] *Macedo Arokiaraj, A. R., and A. Shanmugam. "ACS: An efficient address based cryptography scheme for Mobile ad hoc networks security." Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on. IEEE, 2008.*

[16] *Anoop MS, "Public key Cryptography (Applications Algorithm and Mathematical Explanations)"*

[17] *B. Clifford Neuman, Theodore Ts'o, Kerberos: "An Auth.entication Service for Computer Networks", IEEE Communications Magazine, September 1994, pp. 33-38.*

[18] *Wei Liu, Yanchao Zhang, Wenjing Lou and Yuguang Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys", IEEE Transactions on Dependable and Secure Computing, Vol. 3, No. 4, pp. 386–399, 2006.*

[19] *A. Rex Macedo Arokiaraj, A. Shanmugam, ACS: "An Efficient Address based Cryptography Scheme for Mobile Ad Hoc Networks Security", May 2008, pp. 52-56.*

[20] *Ashwani Garg and Vikas Beniwal "A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks" Volume 2, Issue 9, September 2012.*

[21] *Athulya M S and Sheeba V S, "Security in Mobile Ad-Hoc Networks", July 2012, Coimbatore, India.*