A NOVEL CRYPTOGRAPHICAL SCHEME FOR MOBILE AD-HOC NETWORK SECURITY

Surbhi Tahanguria[1] Deepak Kumar Xaxa[2]
[1,2]Mats School of Engg. & Technology, Raipur

Abstract— Security in Mobile Ad hoc Network (MANET) is very vital issue. Because of dynamic topology and mobility of nodes, MANET's are more vulnerable to security attacks than conventional wired and wireless network. Ad hoc network, infrastructure is not required for establishing communication. 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.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.

Keywords: RSA, MANET, ACS, AODV

I. 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.

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.

II. 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	1. increased security and convenience 2. Private keys never need to	1. much slower than other symmetric cryptosystems 2. may be vulnerable to

	numbers chosen according to special rules	transmitted or revealed to anyone. 3. Can provide a method for digital signatures.	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.	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 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	1.The private and public key generation does not ensure uniform key distribution,

Table. 1: Merits and Demerits of techniques

III. 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.

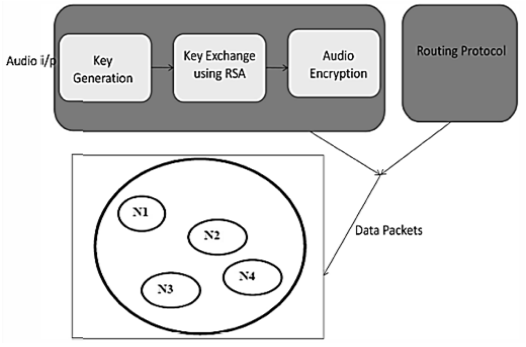

Fig.1: existing network model

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.

IV. 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. The source node prepare the rout discovery packet (RDP) and broadcast it to the MANET with its own address as a secret key. The intermediate neighbouring node receive the packet, decrypt with secret key and verify that the node is matching with the destination node or not. If not matching then the intermediate node will rebroadcast the packet in MANET with its own address as a secret key, and follow the same way till it find the destination. If the receiving node match with destination address given in packet format, then it send the RPLY message to the reverse path. The reverse path will now from destination to source. The rout has been setup now. The source will now sand the data to be securely transmitted by encrypting the message with the secured rout. The destination node decrypt the message with secret key. The scheme proposed in this paper describes the framework to solve the security threats by designing address based cryptography scheme. The proposed scheme ACS gives a new innovation towards more effective and efficient security design for MANETs. STREAM CIPHERING Acquiring security for digital voice, audio and video transmissions has been an important issue during present decade.

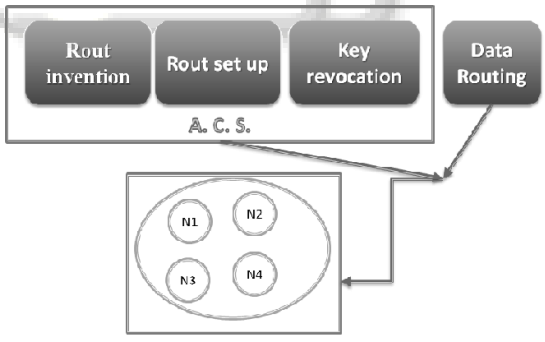

Fig.2: Block Diagram of overall network model

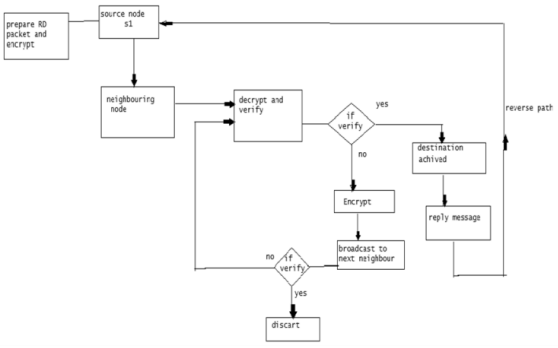

Fig..3: Route Invention and Route Setup Process

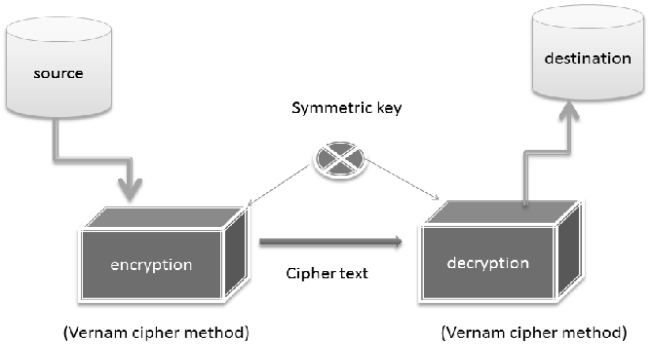

Fig.4: Data transmission with authenticated route

In this paper we have introduced a new combined cryptographic method called TTJSA. Nath et al. have already developed some symmetric key methods. In the present work we have used two methods MSA and NJJSAA which were developed by Nath et al. and have developed a new algorithm, generalized modified Vernam Cipher Method. The above three methods are applied in random order on any given plain text for a number of times to get the ultimate cipher text file. In the present work, authors modified the standard Vernam Cipher Method for all characters (ASCII code 0-255) with randomized keypad, and have also introduced a feedback mechanism. The method has been closely monitored on different known plain text and it was found that this method is almost unbreakable.

A. Vernam cipher

Vernam Cipher Method for all characters (ASCII code 0-255) with randomized keypad, and have also introduced a feedback mechanism. The method has been closely monitored on different known plain text and it was found that this method is almost unbreakable. The present method allows multiple encryption/decryption. The present method is an extremely secure block cipher method and it can be applied to encrypt data in defence system, Banking sector, mobile network etc. The advantage of the present method is that one can apply this method on top of any other standard algorithm such as DES, AES or RSA. The method is suitable to encrypt any type of file.

Algorithm of function encryption(str[],n)

Step 1 : Start encryption() function
Step 2 : set ch1=0
: calculate ch=(str[0]+key[0]+ch1)%256
Step 3 : write ch into output file
Step 4 : set ch1=ch
Step 5 : set i=1
Step 6 : if i≥n then goto Step 13
Step 7 : ch=(str[i]+key[i]+ch1)%256
Step 8 : write ch into the output file
Step 9 : ch1=ch
Step 10 : i=i+1
Step 11 : goto Step 7
Step 12 : Return

End

Algorithm of decryption(str[],n)

Step 1 : Start
Step 2 : ch1=0
Step 3 : ch=(256+str[0]-key[0]-ch1)%256
Step 4 : write ch into the output file
Step 5 : i=1
Step 6 : if i>n then goto Step 12
: ch=(256+str[i]-key[i]-str[i-1])
%256
Step 7 : write ch into the output file
Step 8 : i=i+1
Step 9 : goto Step 6
Step 10 : ch1=str[n-1]
Step 11 : Return
End

V. EXPERIMENTAL EVALUATION

Proposed arrangement has been executed in NS2 version 2.5. To run this scheme minimum hardware configuration is required with no extra specifications. The experiments have been run in Ubuntu.

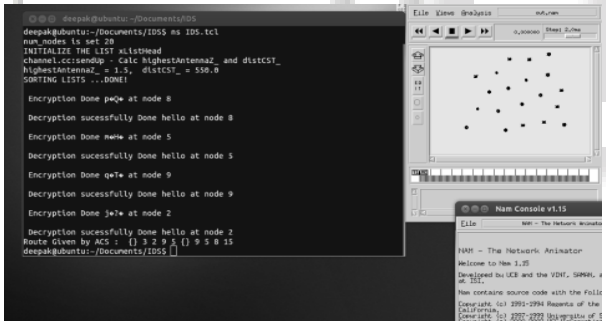

Fig. 5: overall arrangement

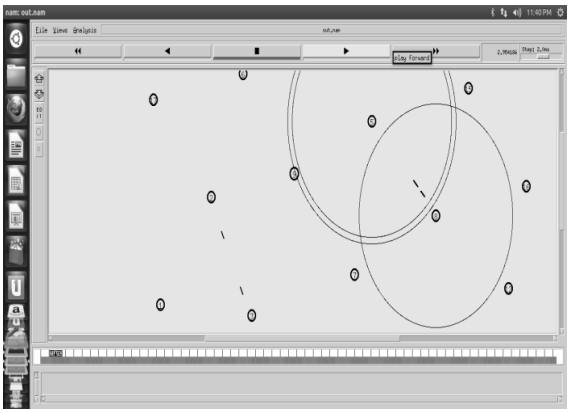

Fig. 6: Route Setup and Invention

In proposed approach we are using ACS as routing setup algorithm, earlier AODV was used. Following show the comparison of AODV and ACS.

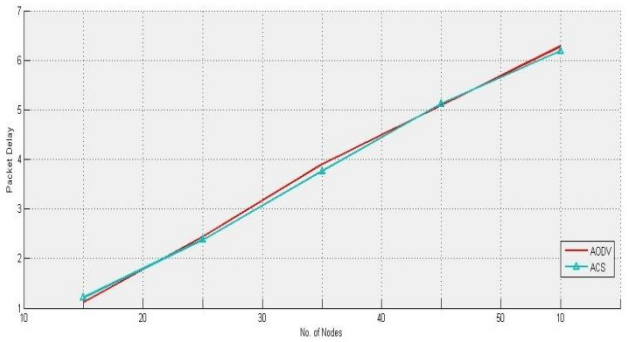

Fig. 7: Comparison of AODV Vs ACS

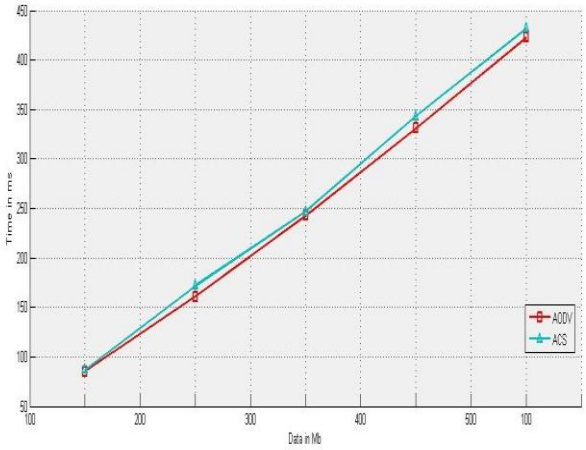

Fig. 8: Comparison of AODV Vs ACS

VI. 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.We have given the theoretical background of different types of Visual Cryptography schemes. Invention of secured rout with ACS scheme. No need of key generation and management. Security is obtaining with encryption and decryption at each node. Rout discovery delay is reduced. Packet delay is reduced.

REFERENCES

[1] Biehl and S. Wetzel. Traceable visual cryptography. In Information and Communications Security, pages 61–71. Springer Berlin / Heidelberg, 1997.
[2] C-C Chang, W-L Tai, and C-C Lin. Hiding a secret colour image in two colour images. The Imaging Science Journal, 53:229{240, May 2005.
[3] Chavan, Pallavi V., and Mohammad Atique. "Design of hierarchical visual cryptography." Engineering

(NUiCONE), 2012 Nirma University International Conference on. IEEE, 2012.
[4] W. Tzeng and C. Hu. A new approach for visual cryptography. Designs, Codes and Cryptography, 27(3):207–227, 2002.
[5] A. Bonnis and A. Santis, "Randomness in secret sharing and visual cryptography schemes," Theory. Computer. Science, 314, pp 351- 374 (2004).
[6] Young-Chang Hou. Visual cryptography for color images. Pattern Recognition, 36:1619{1629, August 2002.
[7] Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in Proc. of IEEE International Conference on Image Processing, Barcelona, Spain,Sept 2003, vol. 1, pp. 521–52.
[8] E. Verheuland H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes."Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.
[9] F. Liu, C.K. Wu, X.J. Lin, "Colour Visual Cryptography Schemes", IET Information Security, vol. 2,No. 4, pp 151-165, 2008.
[10] Chang-Chou Lin andWen-Hsiang Tsai. Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24:349{358, 2003.
[11] Eric R. Verheul, Henk C. A. van Tilborg: Constructions and Properties of k out of n Visual Secret Sharing Schemes. Des. Codes Cryptography 11(2): 179-196 (1997)
[12] Moni Naor and Adi Shamir. Visual cryptography. EUROCRYPT, pages 1{12, 1994.
[13] Nakajima, M. and Yamaguchi, Y., "Extended visual cryptography for natural images" Journal of WSCG. v10 i2. 303-310.
[14] Luiz Velho and Jonas de Miranda Gomes. Digital half toning with space filling curves. Computer Graphics, 25(4):81{90, July 1991.
[15] C.N. Yang e C.S. Laih, "New colored visual secret sharing schemes", DES CODES C, 20(3), 2000, pp. 325-336
[16] NoohulBasheerZainAli,James M Noras," OPTIMAL DATAPATH DESIGN FOR ACRYPTOGRAPHIC PROCESSOR: THE BLOWFISHALGORITHM"in Malaysian Journal of Computer Science, Vol. 14 No. 1, June 2001, pp. 16-27

