Secure and Authorized Approach for Routing In MANET Using Group Signature

[1]Phani Raja.I
[1]Assistant Professor, Department of Computer Science Engineering,
[1]Guru Nanak Institute of Technology,Ibrahimpatnam, Ranga Reddy, Telangana, India

ABSTRACT: *- Anonymous communications are essential for plentyof the programs of cellular ad hoc networks (MANETs) deployedin adversary environments. There are several routing protocolsare to be had for comfy facts switch from one node to another but nonetheless they venerablefrom verity of assaults. Many techniques are to be had for relaxed routing recordsbut still security isn't always completely satisfied. A try has been made to enhance thesafety at some stage in transmission in MANETs with minimum overhead. RSA public keyencryption providessecure routing of data and can defend against attacks like blackhole, grey hole.*

KEYWORDS*: - Anonymous Routing, Mobile Ad hoc Networks.*

I. INTRODUCTION

.In MANETs, the necessities of anonymouscommunications may be done by way of the mixture ofunindentifiability and unlinkability. Already there are such a lot of anonymous routing protocols proposed. Ourfundamental goal is the form of topology based totally on-demandanonymous routing protocols, which are widespread forMANETs in adversarial environments. The generallyused on-demand ad hoc routing protocols are AODV[2] and DSR . Secure Ad-hoc On-call for DistanceVector Routing Protocol (SAODV) [4] is enhancingversion of AODV routing protocol. SAODV make useof uneven cryptography with the help of institutionsignatures.

Secure Efficient Ad-hoc Distance VectorRouting (SEAD) [3] protocolis a proactiveroutingprotocol which continues fresh lists ofdestinations and their routes through periodicallydispensing routing tables during the network.This protocol makes use of hash chain technique forchecking the authenticity of the data packet. This hashchainvalue is used for transmitting a routing replace. Both SAODV and SEAD can't satisfythe requirement of anonymous communications. Now,we focus at the MANETs in adverse environments,where the general public and institution key may be to start withdeployed inside the mobile nodes. We advocate anauthenticated anonymous at ease routing (AASR) totriumph over the above troubles.Toauthenticate the RREQ packet at each hop is necessarywhich is achieved by group signature.

The threats which can be particular to MANETS and are as follows: Worm-hole assault, Greyhole assault, Sinkhole assault, and Sybil attack [5-7].Black-hole attack is a kind of lively assault that exploitsthe RREP function of AODV. These assaults involve somemodification of the records flow or the advent of a fakestream [5]. A malicious node sends RREP messageswithout checking its routing table for a fresh path to avacation spot. A RREP message from a malicious node isthe primary to arrive at a source node. Hence, a supply nodeupdates its routing desk for the brand new direction to the precise vacation spot node and discards every other RREP messages from different neighboring nodes or maybe from thereal vacation spot node. Once a source node saves a direction,it starts offevolved sending buffered records packets to a maliciousnode hoping they'll be forwarded to a vacation spot node.Nevertheless, a malicious node (acting a black-hole attack) drops all information packets as opposed to forwardingthem on. A special observe of the various attacks can beseen in [9, 5]. So a ways we realize that black-hole attack is a DoS attack that disrupts the services of routing layer by means ofexploiting the course discovery technique of AODV inMANETS.

II. RELATED WORK

R. Song, L. Korba, and G. Yee, in "AnonDSR: efficientnameless supply routing for mobile ad hoc networks" [7], provided a mechanism in which the anonymous route establishment is predicated upon the quantity of hops among thesource and the destination, time could be expanded as numberof hops will increase, but it lets in the destination nodes to understandall of the intermediate node IDs.

Y. Zhang, W. Lou, and Y. G. Fang, in "MASK:AnonymousOn-Demand Routing in Mobile Ad Hoc Networks" [8],proposed an algorithm to offer anonymity which dependson a completely unique type of open key cryptosystem, the pairing-primarily basedcryptosystem, to accomplish unknown correspondence inMANET but it fails on the vacation spot nodes because

thevacation spot node ID is found in every RREQ message inundeniable text.

L. Yang, M. Jakobsson, and S. Wetzel, in "Discountanonymous on call for routing for mobile ad hoc networks"[9], proposed the equal machine of ANODR at a decrease cost. Ithas the benefit of carrying out drastically lowercomputation and correspondence complexities at the cost ofexpense of a moderate lessening of safety insurances. Routerequests in Discount-ANODR and in ANODR are parallel howeverthe trouble is that intermediate nodes only recognize thedestination of the request and the identification of the precedingintermediate node but now not the source node.

J. Paik, B. Kim, and D. Lee, in "A3RP: Anonymous andAuthenticated Ad hoc Routing Protocol" [10], offerssafety to statistics packets by group signature however the A3RP usedsecure hash feature to calculate the anonymous direction the usage ofthe real IDs of the destination node but it isn't scalable asencrypted onion mechanism.

III. PROPOSED SYSTEM

This sectioncomprises the particulars about the proposed system. And also represents thehardware and software requirements for the proposed system.

Group signature schemes allow any associate of a pool of signers to sign files on behalf of the group. In standard, a group supervisor controls the institution membership and problems institution signing keys to institution individuals. The group signing keys allow a group member to signal documents on behalf of the group. In specific, a group signature scheme presents anonymity and unlinkability to the signer, i.e.anybody can verify that the signature is legitimate on behalf of a collection, but no person besides for the organization supervisor can determine the signing member.

Mobile ad hoc networks (MANETs) is a group ofmobile nodes allocation a wireless channel with none centralized control.All mobile nodes make a contribution in communications and permitted to attach andgo away the network any time, due to this functionality the safety of networkhave become key mission in MANET. Especially in terms of locked routinginformation. Many routing protocols are proposed for routing whichvulnerable of assaults.Group Signature scheme is used for Authentication purpose. Group signaturecontain entire network T as a group and each node in a group have publickey and personal key pair. The organization public key represented by way of G_{A+}, that'sequal for all nodes in a collection and the institution personal key represented by using G_{A-} which is distinctive for each nodes in a group.

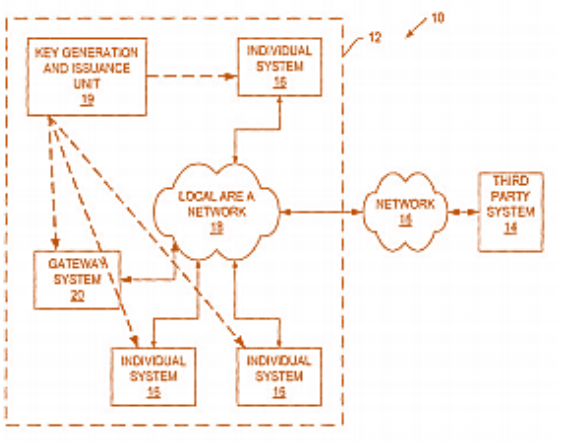

Fig 1: Group Signatures [8]

Asymmetric encryption uses a pair of keys (one public and one private). Anything encrypted with one of the keys, can only be decrypted with the other. The public key can also be used for sender authentication in certain scenarios.

First Generation Algorithms: There are two noteworthy first generation algorithms for generating asymmetric key pairs.

- RSA Algorithm
- Diffie Hellman Algorithm

The main problems with both algorithms are:
They are both much slower than equivalent symmetric algorithms. They both require much larger keys than equivalent symmetric algorithms to ensure security.

Next Generation Algorithms: Elliptic Curve Cryptography (ECC) algorithms may provide much more efficient and secure key pairs as can be seen in the NSA publication.

The computational steps for key generation are

1. Generate two different primes number p and q
   - The p, q are the integer must be chosen at random manner, and must besimilar in magnitude but different in length by a few digits to makefactoring harder.
2. Calculate the modulus $n = p \times q$
   - Here, n is used for the modulus for both the public and private keys.Its length is usually expressed in bits which known as a the key length.
3. Calculate the totient $\varphi(n) = (p - 1) \times (q - 1)$

Where φ is Euler's totient function. This value is kept private.

4. Select for public exponent an integer e such that $1 < e < \varphi(n)$and $\gcd(\varphi(n), e) = 1$
   - Here, e and φ(n) are coprime.

5. Calculate for the private exponent a value for d such that d = e-1 mod φ(n)
   - Where, d is the modular multiplicative inverse of e (modulo φ(n)).
6. Public Key = [e, n]
7. Private Key = [d, n]

Encryption: For encryption purpose, Suppose node A want to send data packet "m" to nodeB, then node A encrypt the data packet through public key which is sharedbetween all nodes of group.

$C = m^e \pmod n$

Decryption: Node B receive data packet in encrypted form and B decrypt received packetusing its private key which is unique one. Node B can recover original data byapplying decryption.

$C^d = (m^e)d = (\text{mod } n)$

Pseudo code

Begin
Source nodes want to transmit the data packet to specific destination
Route Discovery established
Route become discover
For each node in group have pair of public and private keys
Source node sending data packet using public key encryption
Every intermediate node authenticate hop by hop for route
If malicious node available
Detection malicious node
RSA to deliver secure data transmission acquire
Data_packet reached at destination
Destination node decrypt data_packet using private key
End

The algorithm of proposed work is as follows

1) Network Initialization
2) Using RSA Asymmetriccryptography Public Key andPrivate Key Generated
3) In Group Every Node have samePublic key and Unique PrivateKey
4) Source node use Public Key forEncryption of data
5) If MaliciousNode inNetwork, yes then the Detection of MaliciousNode, Providing Secure Pathusing RSA
6) If Malicious Node in Network, noData Packet Reached atDestination
7) Destination Decrypt data packetusing Private Key
8) End

Table.1 Simulation Parameters

Simulation Used	NS-2.32
Number of Nodes	50,60,70,80,90,100
Dimension of Simulation Area	1000 * 1000
Routing protocol	(DSR,RSA)
Simulation Time	100sec
Antenna Type	Omni Antenna
MAC Protocol	IEEE 802.11
Queue	DropTailPriQueue
Channel Type	Wireless Channel
Packet Size	152 byte

The following parameters are of interest when evaluating theefficiency of a particular group signature scheme:

1. The size (number of bits) of the group public key Y.
2. The size (number of bits) of an actual group signature ona message.
3. The efficiency of the Setup, Sign, Verify, and Openprotocols.

IV. SIMULATION RESULTS

For research vicinity of wireless networking, network status quo in actual time with theactual records is just too tough. For trying out, appropriate simulator has to be select to getpreferred output. The simulator helps to the community developers to pick out whether or notthe network is capable to paintings in the real time or not. Below are the diverse tools thatcan be used as community simulators.Network Simulator Version 2, widely known as NS2, is only an event drivensimulation tool that has revealed useful in learning the dynamic nature ofcommunication networks. Simulation of wired as well as wireless networkfunctions and protocols are like routing algorithms, UDP, TCP can be doneusing NS2.

Implementation of the proposed system is done using RSA asymmetric public keycryptography used for generation of public and private keys and can defend againstblack hole attack

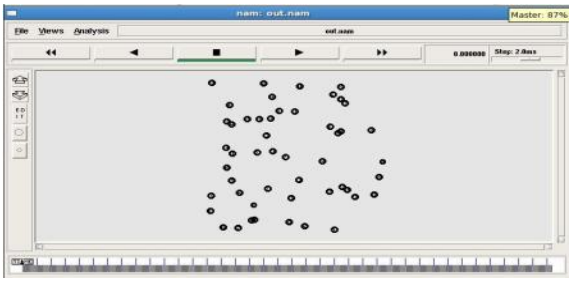

Fig. 2 Network Initialization in proposed system

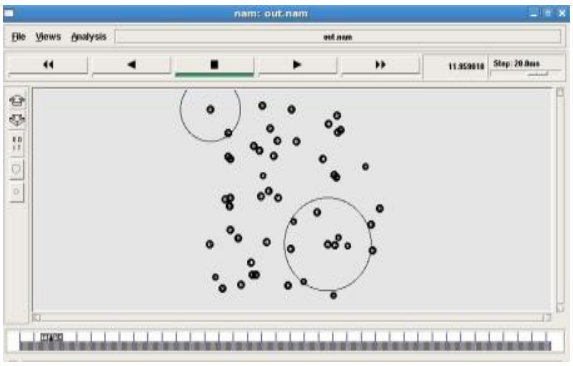

Fig. 3. Route Setup in proposed system

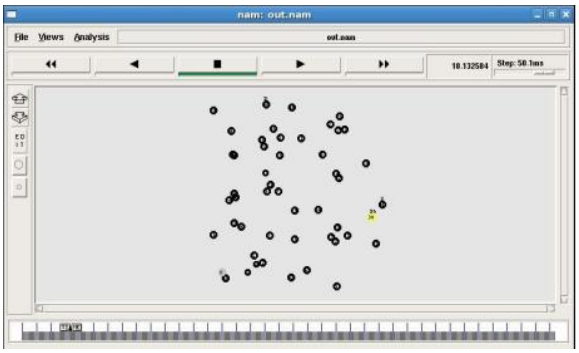

Fig. 4. Detection of black hole attack

V. CONCLUSION

In this paper, we have offered diverse components of group signature like evaluate properties, keys, programs, and challenges. The group signature scheme prevents the active attacker withoutintroducing the node identification. The nodes in the network cannot always be depended on. Security of routing statistics is afundamental subject. Main intention to offer securely facts transfer the use of authenticationmethod. Group Signature technique used for authentication to provide comfortable path.RSA uneven encryption set of rules is used for provide secure path at some stage in routingpackets, and guard in opposition to assaults like black entire, grey hollow.

REFERENCES

[1] Devesh Kumar Pal et al, "Survey on Security Issues in Mobile Ad HocNetworks", IJCSIT (2014)

[2] Sheng Liu, Yang, Weixing Wang, "Research ofAODV Routing Protocol for AdHoc Networks", 2013AASR, Conference on Parallel and DistributedComputing and Systems.

[3] Prasuna V. G, Dr. S. Madhusudhana Verma,"SEAD-FHC: Secure Efficient Distance Vector Routingwith Fixed Hash Chain length", Global Journal ofComputer Science and Technology Volume 11 Issue 20Version 1.0 December 2011

[4] C. Sreedhar, Dr. S. Madhusudhana Verma, Dr. N.Kasiviswanath, "Performance Analysis of SecureRouting Protocols in Mobile Ad-Hoc Networks", International Journal of Computer Science andTechnology.

[5] M. Imani, M. E. Rajabi, M. Taheri and M. Naderi, "Vulnerabilities in Network Layer at Wireless Mesh Network(WMNs)," Proceeding from ICENT'10: 2010 International Conference on Educational and Network Technology, Qinhuangdao, 25-27 June 2010, pp. 487-492.doi:10.1109/ICENT.2010.5532257

[6] F. Nait-Abdesselam, B. Bensaou and T. Taleb, "Detectingand Avoiding Wormhole Attacks in Wireless Ad-HocNetworks," IEEE Communication Magazine, Vol. 46, No.4, 2008, pp. 127-133. doi:10.1109/MCOM.2008.4481351

[7] V. Zhang, J. Zheng and H. Hu, "Security in WirelessMesh Networks," Auerbach Publications Taylor & Francis Group, London, 2009

[8]Http://www.freepatentsonline.com/7093133.html (Lastusedon 9/4/2013)

[9] S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad-Hoc Networks under Black Hole Attacks," Proceeding from SECON'07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.

[10] Hwan-Seok Yang, Seung-Jae Yoo "Authentication Techniques for Improvingthe Reliability of the Nodes in the MANET", IEEE (2014)

[11] S.S.Zalte, Prof.(Dr.) Vijay R.Ghorpade, "Secure Token for Secure Routing ofPacket in MANET", IJCSIT(2014)

[12] Miss Morli Pandya, Associate Prof. Ashish Kr. Shrivastava, "Review onsecurity issues of AODV routing protocol for MANETs", IOSR Journal ofComputer Engineering (2013)