An Efficient Secure Routing Scheme For MANET

Ms. Dipika R. Kolipatel [1],Mr. Krunal J. Panchal [2]
[2]Assistant Professor
[1, 2] L.J. Institute of Engineering and Technology

Abstract- *Mobile Ad hoc NETwork (MANET) is a collection of self-organizing mobile nodes without any help of centralized administration or established infrastructure. In nature it is dynamic & it discovers the way routes dynamically to reach the destination. Before establishing communication route is not known, so securing a dynamic way route is difficult task in MANET. Routing protocols developed for MANET helps node to communicate with each other. Different Secure routing protocols were developed to detect and prevent from specific type of attacks or malicious behavior of the nodes in network. In this research work an efficient secure routing scheme for MANET which establish secure and optimal path will be proposed. Proposed scheme permits only trustworthy node to come to be part of routing using delegation based scheme and transmit data securely towards destination using asymmetric cryptographic algorithm RSA. Efficiency of network is increased by optimal path searching using optimization algorithm (PSO).*

Keywords- MANET, Security attacks, secure routing, Delegation based scheme,PSO

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a constantly self-designing, infrastructure-less network of mobile devices associated without wires. Ad Hoc is Latin & means “for this purpose” Each device in a MANET is free to move autonomously in any direction and will change its links to other devices frequently. [1]The mobile Ad hoc networks are differ from internet in two major ways. In the first way the hosts in this network are resource restriction. Nodes have restricted energy, computing power & memory. In the second way the nodes of the network are mobile & the topology changes rapidly. These two features pose great challenges to the investigators working in the area.

Example of MANET applications include law enforcement operations, automated military applications, Disaster reliefapplications, interactive lectures or conferences, Intelligent buildings, logistics etc. In ad-hoc network, finding a path between two hosts using routing protocol is a very enormous- task due totheir highly dynamic topology, absence of centralized administration. Designing of routing protocol in ad-hoc network depends various factors like mobility, bandwidth, resource constraint, hidden and exposed terminal problems etc. Thus, routing protocol is structured for purposes such as fully distributed, adaptive frequent and stable topology, loop free and minimum number of collisions. To meet the recent and rapidly increasing demand in decentralized environments like mobile ad hoc networks (MANETS) the need for a secure routing protocol becomes inevitable so that the attacks such as malicious routing misdirection, black hole, gray hole, denial of service etc.can be averted. [2]

II. RELATED WORK

Raj Kamal Kapur, Sunil Kumar Khatriet al. [3] have proposedSecure Data Transfer in MANET Using Symmetric and Asymmetric Cryptography.In this work they haveproposed a technique which provides secure transmission of data. The technique involves encryption of data using symmetric cryptographic technique, and also generating the digital signature of the data using the asymmetric cryptographic technique from the Hash of the data. The encrypted data is transmitted through the network to the destination where the received data and digital signature of the data are validated using symmetric and asymmetric cryptography. The data on validation is accepted thus ensuring secure data transmission. The proposed technique provides confidentiality, integrity, authenticity and non-repudiation to the data. It protects the data transmitted over the network from snooping, modification, replay and fabrication attack at the application layer**.**

Remya S, Lakshmi K.S et al. [4] have proposed Secured Hierarchical Anonymous Routing Protocol (SHARP) based on cluster routing. SHARP offers anonymity to source, destination, and routes. Anonymous routing protocols are used by MANETs that hi de s the identity of nodes as well as routes from outside observers. In MANETs anonymity means identity and location anonymity of data sources and destinations as well as route anonymity

Jarupula Rajeshwar,Gugulotu Narsimhaet al.[5] proposed Secure way routing protocol for mobile ad hoc network, which secure the routing mechanism from both the internal and the external attacks. Most of the existing secure routing protocols target to evade specific type of attacks or malicious behaviour of the nodes or networks. This paper propose a novel secure way routing protocol for securing the dynamic way routes in MANET. It provides a unique session key for each route to secure the data communication. Moreover, it authenticates the data packets using asymmetric cryptography and secures the routing field message using two-way asymmetric cryptography.

Ashish Sharma, Dinesh Bhuriya, UpendraSinghet al.[6] have proposedsecure data Transmission on MANET by Hybrid Cryptography Technique. In this paper they have focus only active attacks in network layer. Ad Hoc On Demand Vector Routing protocol is a reactive routing protocol for ad hoc networks that maintain routes only between nodes which want to communicate by using routing messages. In order to provide security in the mobile ad hocnetwork the hybrid encryption approach using RSAand DSA algorithms is used for implementation. Thathybrid algorithm is incorporated in the AODV routing protocol for securing data during the

Rasika R. Mali, Sudhir T. Bagadeet al.[7] Detection of Misbehaving Node using Secure Acknowledgement in MANET. This paper propose and implement, new IDS named as Secure Acknowledgement (ACK) System. The Secure ACK system is purely an acknowledgement based technique. The type of misbehaviour detected by proposed system is about delay in packet transmission. In this system, for every three consecutive nodes in the route, the third node is required to send back an acknowledgement packet to the first node in the group. Based on the non-receipt of ACK packet within predefine time to the first node in the group, it reports about misbehaviour activity in the network. As soon as the proposed system detects misbehaving node present in the network, it stops the further data transmission. So, the misbehaving node will not be able to damage network thereafter.

Anup Ashok Patil, Shital Maliet al.[8] Hybrid Cryptography Mechanism for Securing Self-Organized Wireless Networks As communication is done through wireless links,these types of networks are more prone to several kinds ofattacks. Authentication and encryption acts as first line ofdefense while an intrusion detection system (IDS) acts as a secondline of defense. One of the intrusion detection system used inMANET is Enhanced Adaptive Acknowledgement (EAACK)which is based on acknowledgement packets for detection ofmalicious activities. This system increases the overhead ofnetwork significantly relative to other system such as watchdog.So, in this paper they adopt the hybrid cryptography to reduce thenetwork overhead and enhance the security of networkssignificantly**.**

Parth Patel, Rajesh Bansode,bhushan Nemadeet al.[9] proposed Performance Evaluation of MANET Network Parameters using AODV Protocol for HEAACK Enhancement. Hybrid Enhanced Adaptive Acknowledgement (HEAACK) which is proposed in this paper to adds cryptography mechanism such as RSA and Triple DES giving a secure network and thus the rate of data manipulation and network overhead decreases. By adding HEAACK incorporates Digital Signatures such as RSA and Triple DES which can detect malicious node in network. HEAACK provides a secure network for data transmission.

S. Rameshet al.[10] proposed An Efficient Secure Routing for Intermittently Connected Mobile Networks.The paper exhibits the efficient secure routing by PPARP which shows a higher level of security in ICMN. Secure communication in the network is made possible by certain authentication series as ICMN is known for its higher delays. A peculiar routing protocol called Privacy Preserving Ant Routing Protocol (PPARP) which is a fusion of ACO with authentication series promises us an expected security.

Sachin D. Ubarhande,Dharmpal D. Doye, Prakash S.Nalwade et al.[11] have proposed a distributed delegation-based scheme, namely, a secure path selection scheme. The proposed scheme identifies and allows only trusted nodes to become part of active path. The SPSS scheme establishes a secure path from source to destination in presence of attackers.

III. OBJECTIVE AND PROBLEM STATEMENT

To find secure path before actual data transmission which does not participate malicious node into routing, transfer data securely from source to destination using cryptography and to make routing efficient using Swarm intelligence based optimization algorithms.

“Development of new routing scheme for MANET is to overcome issues related to security and efficiency in routing process in MANET to transfer data securely from source to destination.

IV. PROPOSED WORK

The proposed system work based on following assumptions:

1. 1.For all communications source node is not malicious.
2. Address of all delegate nodes is already known to legitimate nodes.
3. Delegate nodes update and broadcast trusted nodes list in network.

4. 4.In Initialization phase all legitimate nodes send join request with trust value as 1.

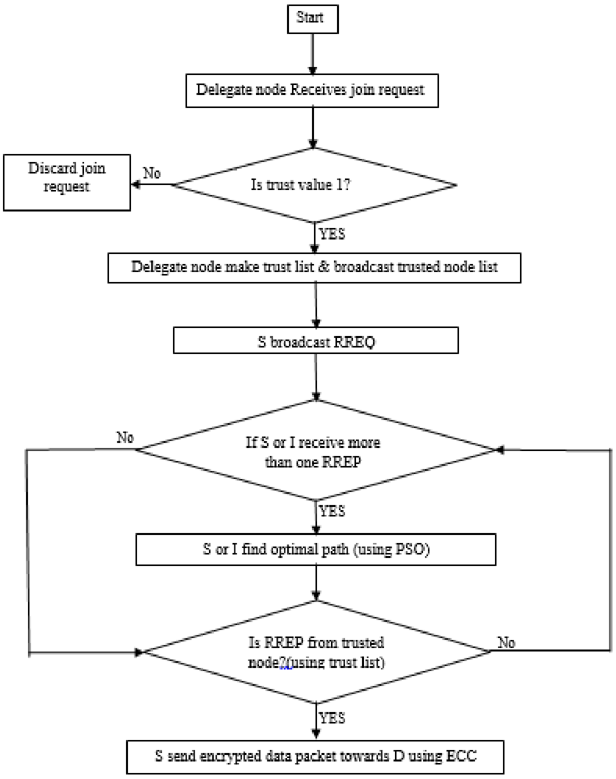

Start
Delegate node Receives join request
Discard join request
No
Is trust value 1?
YES
Delegate node make trust list & broadcast trusted node list
S broadcast RREQ
No
If S or I receive more than one RREP
YES
S or I find optimal path (using PSO)
Is RREP from trusted node?(using trust list)
No
YES
S send encrypted data packet towards D using ECC

Fig.1:Proposed system flow chart

Here,S is Source node, D is Destination node, I - Intermediate node, RREQ - Route Request,RREP - Route Reply

Proposed technique has 3 phases: Initialization, Route discovery, Data transmission

In proposed technique in initialization phase Delegation scheme is used to make trust list of trusted nodes. In route Discovery route is discovered by AODV protocol in which secure nodes are selected using trust list and PSO algorithm find optimal route. Then after in Data transmission phase data is transmitted using ECC algorithm.

Initialization

In initialization phase it assumes that all legitimate nodes send join request with trust value as 1. The join request sending process is run until requesting node does not receive join acknowledgment from delegate node. If trust value of requesting node is matched, delegate node broad cast trusted node list in the network.

Route Discovery

In this phase, each node before processing any request first it check if more than two routes are available, then source select optimal route using PSO. Then source verifies responder node address.

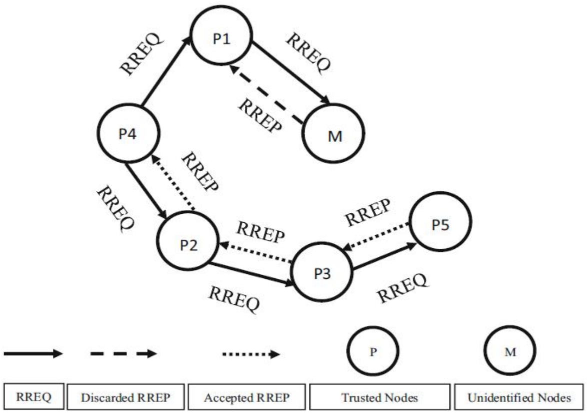


Fig.2 : Working of secure node selection

For Fig.it assumes that delegate nodes broadcast trusted node list as T = {P1, P2, P3, P4, P5}.

If responder node is listed in trusted nodes list. In Fig.2 node P4 is source node and node P5 is destination node. Source node P4 broadcasts RREQ packet to establish path to destination node P5. Neighbor nodes P1 and P2 receive RREQ packet and broadcast it further. Node M receives RREQ packet from node P1. Node M immediately sends RREP packet to node P1 even without having an actual path to destination. But, if node P1 does not get address of node M in trusted nodes list, node P1 discards RREP packet received from node M. The path from source to destination get established via nodes P4, P2, P3 and P5.

Data transmission

As an example nodes P4, P2, P3 and P5 successfully pass the verifying process, source node P4 then sends data encrypted data packets by ECC to destination node through established secure path.

V. PERFORMANCE EVALUATION AND RESULS

To implement a new routing scheme for MANETs using NS-2 it needs to add a new routing protocol. C++ coding is used to implement routing protocol in NS-2, and the simulations describing scenarios are created by Tcl scripts. To do this this work uses NS-2.35 version. In this work the protocol is based on AODV protocol.

Experimental parameters

Measures of performance of proposed system are packet delivery ratio, packet loss rate, throughput and routing overhead against SPSS system.

1. Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as:

PDR= C1÷ C2

Where, C1 is the sum of data packets received by the each destination

and C2 is the sum of data packets generated by the each source

2. Packet Loss Ratio

Packet loss ratio is defined as the ratio of data packets fail to reach at destination.Mathematically, it can be defined as:

PLR = C1÷ C2

Where, C1 is the sum of data packets generated by the each source

and C2 is the sum of data packetsreceived by the each destination

3. Throughput

It is defined as the total number of packets delivered over the total simulation time. Mathematically, it can be defined as:

Throughput= K/1000

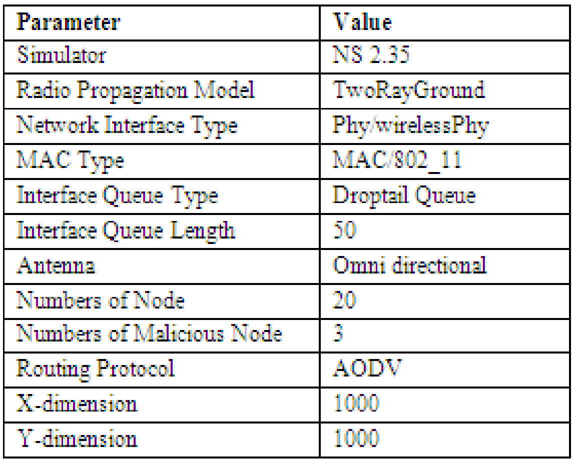
Where, K is Number of packets and 1000 is simulation time.

4. Overhead

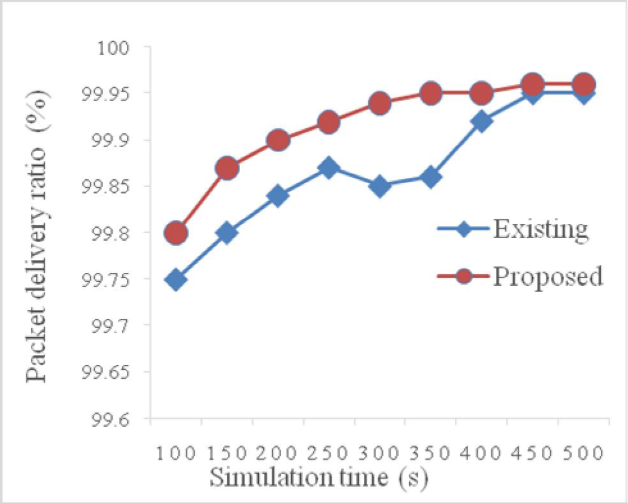
This is described as the ratio of routing, which relates to the packets in bytes to the total routing and data transmission (sent or forwarded packets), in bytes.

RO= (Routing Transmission) / ((Data Transmission) + (Routing Transmission))

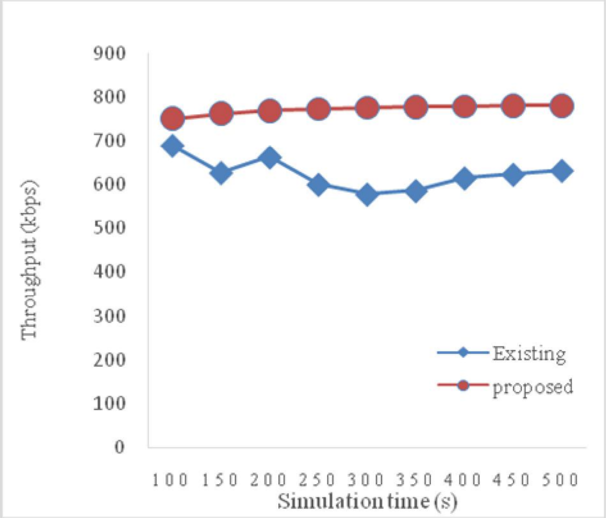
Table 1 :Simulation Parameters



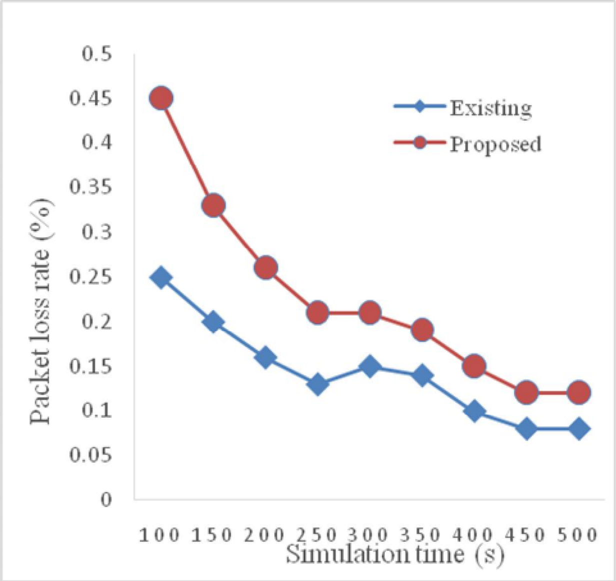
Parameter	Value
Simulator	NS 2.35
Radio Propagation Model	TwoRayGround
Network Interface Type	Phy/wirelessPhy
MAC Type	MAC/802_11
Interface Queue Type	Droptail Queue
Interface Queue Length	50
Antenna	Omni directional
Numbers of Node	20
Numbers of Malicious Node	3
Routing Protocol	AODV
X-dimension	1000
Y-dimension	1000



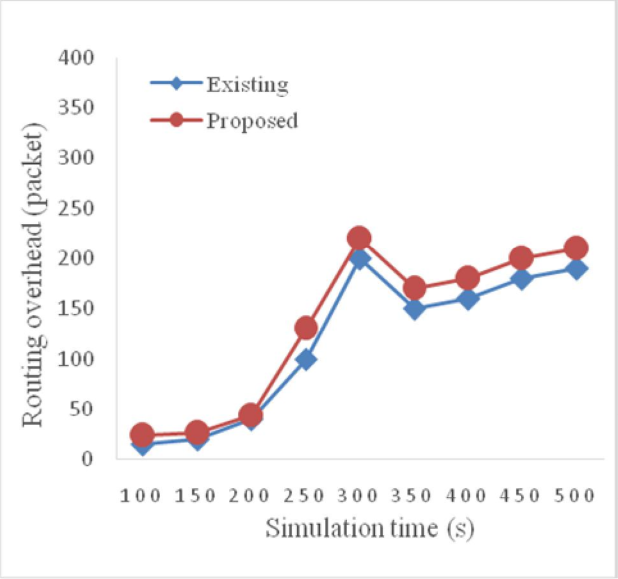
(a)



(b)



(c)



(d)

Fig. 3 : (a)Packet delivery ratio, (b) Throughput, (c) Packet loss rate, (d)routing overhead over the simulation time

VI. CONCLUSION

Due to mobility of nodes MANET is vulnerable to security threats.This paper propose new routing scheme for MANET which overcome issues related to security and efficiency in routing process in MANET and also minimize resource consumption. Delegation scheme with ECC provide security in both route discovery and data transmission phase. The performance of proposed scheme is compared against SPSS system using NS2 simulator for varying simulation time. The simulation results show that proposed scheme improve performance of MANET for packet delivery ratio, packet loss rate, throughput with increasing minimal load.

REFERENCES

[1] Jai Shree Mehta, Shilpa Nupur,Swati Gupta."An Overview of MANET: Concepts, Architecture & Issues",International Journal of Research in Management, Science & Technology (E-ISSN: 2321-3264),Vol. 3, No. 2, April 2015(pp:98-101)

[2] Umang singh “secure routing protocols in mobile adhoc networks-a survey and taxanomy”International journal of review in computing.ISSN: 2076-3328-2011. Vol. 7

[3] Raj Kamal Kapur, Sunil Kumar Khatri, “Secure Data Transfer in MANET Using Symmetric and Asymmetric Cryptography” ,978-1-4673-7231-2/15/$31.00 ©2015 IEEE.

[4] Remya S, Lakshmi K S(2015)." SHARP : Secured Hierarchical Anonymous Routing Protocol for MANETs ". 2015 International Conference on Computer Communication and Informatics (ICCCI), 978-1-4799-6805-3/15/$31.00 @2015 IEEE.

[5] Jarupula Rajeshwar,Gugulotu Narsimha(2015)." Secure way routing protocol for mobile ad hoc network". Wireless network, by SPRINGER, DOI 10.1007/s11276-015-1161-3.

[6] Ashish Sharma Dinesh Bhuriya Upendra Singh “Secure Data Transmission on MANET by Hybrid Cryptography Technique” IEEE International Conference on Computer, Communication and Control (IC4-2015)

[7] Rasika R. Mali, Sudhir T. Bagade, “Detection of Misbehaving Node using Secure Acknowledgement in MANET”, International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune, India. Dec 19-21, 2016, 978-1-5090-1338-8/16/$31.00 ©2016 IEEE, pp.611-616

[8] RaAnup Ashok Patil, Shital Mali, “Hybrid Cryptography Mechanism for Securing Self-Organized Wireless Networks”. 3rd International Conference on Advanced Computing and Communication Systems (ICACCS - 2016), Jan. 22 – 23, 2016, 978-1-4673-9206-8/16/$31.00 ©2016 IEEE

[9] Parth Patel, Rajesh Bansode,bhushan Nemade, “Performance Evaluation of MANET Network Parameters using AODV Protocol for HEAACK Enhancement”, 7th International Conference on Communication, Computing and Virtualization 2016, doi: 10.1016/j.procs.2016.03.11

[10] S.Ramesh(2016)." An Efficient Secure Routing for Intermittently Connected Mobile Networks “Wireless Personal Communication. DOI 10.1007/s11277-016-3885-5

[11] Sachin D. Ubarhande,Dharmpal D. Doye, Prakash S. Nalwade(2017)." A Secur Path Selection Scheme for Mobile Ad Hoc Network. “Wireless Personal Communication, Springer, DOI 10.1007/s11277-017-4597-1