Mobility Aware Secure Routing in MANET

Nilam S. Parmar[1] Manjusha Deshmukh[2]
[1,2]University of Mumbai

Abstract— In Mobile Ad-hoc Networks if forwarding nodes have high mobility, there are more chances to make local topology inaccuracy. If the node involved in the forwarding path moves frequently then there is the situation of link failure which leads to packet loss. Hence it is required to select the nodes with low mobility which means selection of node as forwarder based on its mobility. Mobility based forwarding node selection scheme improves the routing performance. Source node predicts the distance of each neighbor from itself at particular time (t) using the current location of neighbor and speed of the neighbor. After certain time (t+T) it predicts the distance again using the current location of neighbor. In both situations if the node comes under neighbor status then it is highly stable neighbor. To apply this routing scheme, distance between destination and highly stable neighbors are calculated. The neighbor which is having the minimum distance is selected as forwarder.
If there is tie between the nodes then the node which is having high willingness value become forwarder node. This willingness value can be calculated using power, coverage and reliability of the node. The higher values there are more chances to become forwarder node. The message confidentiality and integrity has also being implemented using RSA asymmetric key encryption algorithm. The node authentication is also implemented using Aggregate Signature algorithm. The simulation result shows how it can reduce broadcasting redundancy and improves the packet delivery ratio.

Key words: MANET, ATSR, MTSR, OLSR, AODV, ZRP, NS-2

I. INTRODUCTION

The Mobility, Willingness and Trust based routing scheme is based on pro-active scheme which is inspired from OLSR, in which minimum number of nodes can form the fully connected network and only these nodes route the packet in the network. With addition to this our scheme uses most stable nodes as forwarder node in the network. Source node calculates the distance of each node in a network from itself at particular time (t) using the current location of neighbour and speed of neighbour. After some period at (t+T) time it again calculates the distance using the current location of neighbour and speed of neighbour. In both situations if the node comes under neighbour status i.e. within its communication range then it is highly stable neighbour. So while applying this routing scheme in a network first we are selecting highly stable neighbours and then calculate the distance between these nodes and destination node. The nodes which are having minimum distance towards the destination is selected as forwarder node and it can forward packets to destination node. If there is tie between the nodes then the node which is having high willingness value become forwarder node. The power, coverage and reliability of the node can be used to calculate willingness value. The higher values there are more chances to become forwarder node. The confidentiality of the message and integrity of the message can be achieved by using RSA asymmetric key encryption algorithm. The node authentication is also achieved using Aggregate Signature scheme. The network is simulated by using ns-2 (Network Simulator version 2) and it increases packet delivery ratio as compare to the existing system. The end to end delay is somewhat more than the existing system because it provides more security. The admin count ratio i.e. number of admin nodes in between source and destination is varying in both systems.

II. RELATED WORK

In this topic we mention the related past works in which various routing protocols have been used to route the packets efficiently and securely in network using various approaches.

Sreeleja N. Unnithanand and Vijitha S.[1] proposed a new modified firm scheme which makes a accurate stability between immovability of link, neighbour node, path and total number of mobile nodes which increases the network lifetime. The main goal of the projected work is to decrease the ratio of packet loss and provide high network lifespan by using the firmness model. The projected model consists of three stages like identification of stability of neighbour node, path, link prediction of total network lifespan. The proposed algorithm obtains better output in terms of number of packets sent per unit of time i.e. PDR ratio, network lifespan, delay between packet sending, overhead and energy consumption of a node. But when the distance between two nodes becomes larger than the transmission range nodes will be disconnected.

M. Raiendiran and S.K. Srivatsa [2] when designed a routing scheme of multicast which was based on mesh networks that helped in finding constant multicast route from source to destination. In their scheme only those nodes were responsible for flooding the JOIN-QUERY messages which could fulfil the delay requirements. The M/M/1 queuing systems is followed by contributing nodes. The extreme value for queuing and controversy postponement are kept in queuing systems. These values are the- proportion of extreme size of queue and the check time of a node. Controversy postponement and queuing system are used to recover the firmness of link. The nodes which had. high stability of link connectivity were used to find stable routes. The various parameters like: link received power, link quality and distance between neighbouring nodes were used to calculate link stability. The performance of this routing protocol can be checked with the help of large number of mobile nodes. And it is observed that this protocol yields improved output and minimum overheads.

Suman halder [3] designed a Mobility Aware Ad-hoc On Demand Distance Vector routing protocol which was based on AODV protocol. The issue of maximum motion can be handled very efficiently by this MA-AODV protocol. The more firm path from source to destination was established by performing periodic quantification of nodes

mobility. The regular link breakages can be associated with the unsteady paths that holds high movable nodes could be avoided by using this protocol. Topological changes were reduced by this protocol. The overhead of broadcasting messages had been reduced by this protocol. While sending huge amount of data from source to destination it is more desirable to maintain continuous connection between them.

Rajashekhar C[4] developed a routing scheme which is called as multiple path multicast routing and it was based on information priority. This scheme used reliable neighbor node selection mechanism. To find non-pruned neighbors, those neighbor nodes are nominated that fulfill firm threshold of consistency couple of factor. They are used to create multicast routes which have a multiple path of allocated level of priority. The control packets of request and reply are used along with information of routing and neighbor's database. To transfer data of different level of priority to number of destination different routes are used. By using node power model and mobility model neighbor node selection can be done. This scheme also provided strong path maintenance mechanism for handling situations of node and link failure.

Arnab Banerjee, Dipayan Bose, Aniruddha Bhattacharya, Himadri Nath Saha, Dr. Debika Bhattacharyya [5] proposed a new routing scheme in MANET which is based on proactive routing. Here Admin nodes are calculated based on their willingness and trust and only these nodes will route the traffic in the network. Willingness value is calculated based on power, coverage and reliability of the node. But mobility of the node was not taken into consideration in this paper.

III. PROPOSED SYSTEM

A. Calculating Mobility of a Node:

For calculating mobility of a node following algorithm is used.

1) Step 1 : First each node calculates the distance to all other nodes in a network using Euclidian distance formula.
   $D(x,y)=\sqrt{(x1-x2)^2 + (y1-y2)^2}$ (1.1)
   Where (x1,y1) is previous location of node and (x2,y2) is current location of node.
2) Step 2 : Check which are the neighbors of every node in a network by checking its communication range. The nodes which comes under the communication range are the neighbors of a node.
3) Step 3 : After some time again calculate the distance from every node to all other nodes in a network.
4) Step4: Again if same node comes under the communication range then they are the most stable nodes or neighbors of a node which can be selected as an admin nodes.

B. Calculation of Willingness Value:

For calculating willingness of a node the values of power, coverage and reliability of node are considered.

1) Step1 : Initially we are assigning power 300 joules to every node
2) Step 2 : For calculating coverage of a node we are checking which nodes comes under the communication range (i.e. 200 m). The count of such nodes is the coverage of a node.
3) Step 3 : By using random function we are generating value for reliability in range of 0-10.
4) Step 4 : To calculate the value of willingness following formula can be used.

Willingness = 0.50 * P + 0.30 * C +0.20 * R (1.2)

where
P: The power present at the node
C: Communication range
R: Consistency of the node

C. Encryption Using RSA Asymmetric Key Algorithm:

RSA is an encryption technique which uses public key for encrypting the sensitive information which user wants to send through uncertain network like internet. This algorithm contains the following steps:

In this a pair of public and private key is created by every user.

1) Choose any two prime numbers arbitrarily suppose p and q.
2) Calculate the value of N where N=(p*q) Here ø(N)=(p-1)(q-1) (1.3)
3) Encryption key e should be selected randomly. where 1<e<ø(N), gcd(e,ø(N))=1
4) Calculate the decryption key d by solving the given equation
   e*d=1 mod ø(N) and 0≤d≤N (1.4)
5) Announce the public encryption key of every node : KU={e,N}
6) Private decryption key i.e. KR={d,p,q} should remained with the node itself.

D. Aggregate Signature Algorithm:

The digital signature scheme which supports aggregation is known as "Aggregate signature scheme". In these scheme n different users makes n number of signatures on n number of different messages. A single short signature is formed by combining all these signatures. This single short signature will confirm that n number of users have truly sign the n actual messages, i.e. i^{th} user has signed message Mi for i=1,2,3,…..,n. The size of certificate chains is reduced by combining all signatures from chains in a single chain.

An aggregate signature scheme consists of following steps.

1) Start

Take input 1^k , where k €Z is the security constraint and results some publicly known system constraints.

2) Retrieve

Takes input which should be a user identity ID and a secret msk, and results a private key

$S_{ID} \leftarrow$ Extract (msk,m) (1.5)

3) Sign

Take input a private key S_{ID} which is associated to a particular ID and a portion of message m€{0,1} and results into a signature.

$\sigma \leftarrow$ Sign(S_{ID},m) (1.6)

4) Verify

Take input an identity ID, a message m€{0,1}and result is Accurate if Verify (m, ID, σ) =1 (1.7)
or incorrect otherwise.

5) Aggregate

Take input a list of signatures $\{ \sigma_i \}^n_{i=1}$ on $\{ m_i\}^n_{i=1}$ for $\{ID_i\}^n_{i=1}$ and results an aggregate signature

$\sigma \leftarrow$ Agg ($\sigma 1, \ldots . \sigma$ n) (1.8)

6) AVerify

Take input a list of identities (ID_i, …., ID_n) , messages (m_1,….,m_n) and an aggregate signature σ and results correct if

AVerify (m_1,…,m_n, $ID_{1,\ldots,}ID_n$) = 1 (1.9)

Or incorrect otherwise.

IV. SIMULATION

A. *Simulation Environment:*

Simulation is done with NS2,35, it is installed on an intel core i3 / Personal Computer (PC) with Microsoft Windows 8.1 operating system. The PC has 4GB of RAM. The parameters used for simulation in NS2.35 which are configured as follows :

Parameter	Value
Communication range	250 meters
Bandwidth	2 Mbps
IFQ Type Queue/ DropTail / PriQueue	50 packets
Simulation time	50 seconds
Traffic type	constant bit rate
Pause time	0 seconds (continuous mobility)
Topology size	600m x 600m
Number of nodes	20,40,60,80,100
Maximum speed	2 and 20 m/s

Table 1: Simulation Parameters

B. *Scenario of Proposed System:*

NS2 simulator is used for simulation. In the NS2 simulator Node object is already available. Each node will be given their Unique Node ID and position. Now a network is created with configurable number of 40 nodes. Each node is placed on the region. As shown in figure 7.1 it creates the simulation setup of a only scenario consisting of 40 wireless nodes placed in the network area and simulation time was takes 50 seconds. The second part is for node configuration. Here we use wireless channel with OLSR routing protocol. Note that for MAC protocol, we use MAC/ 802_11 for the movement. As mentioned in the ns2 manual, there is an Interface Queue between the two layers i.e. Logical Link layer and the Media Access Control layer.

V. SIMULATION RESULT

A. *Packet Delivery Ratio:*

The packet delivery ratio is obtained by dividing the number of received data packets by the number of generated data packets.

Following figure shows the packet delivery ratio with respect to number of nodes. As shown in figure 7.9 Packet delivery ratio for our Mobility, Trust and Willingness based secure routing scheme (MTSR) increases as the number of node rises compare to the Administrator and trust based secure routing scheme (ATSR).

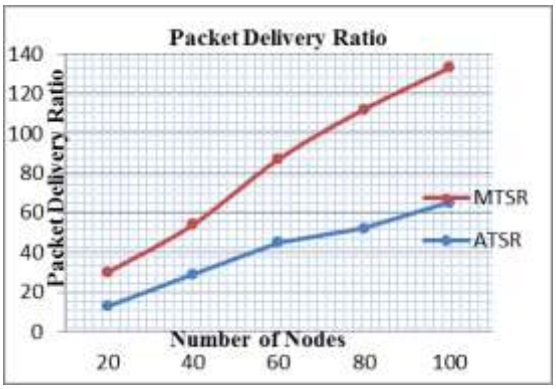

Fig. 1: Number of nodes vs. Packet Delivery ratio

B. *End To End Delay:*

The end-to-end delay is defined as the time a data packet is received by the destination minus the time the data packet is generated by the source. The following figure 7.10 shows average end to end delay for ATSR and MTSR routing scheme. In our routing scheme end to end delay is more as compare to the ATSR scheme because our routing scheme provides more security for packet transmission as well as for node authentication which takes more time so delay is higher.

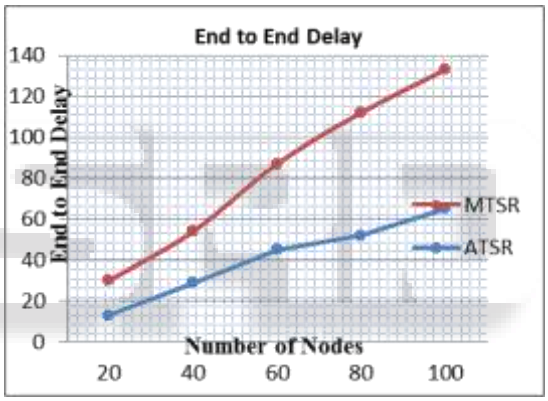

Fig. 2: Number of nodes vs. End to End Delay

C. *Admin Count:*

Admin count means the number of nodes found on the route from source node to destination node. As shown in figure 7.11 the rate of admin count for our MTSR routing scheme is low for less number of nodes but it increases gradually as the number of node increases. As we can see in the figure the rate of admin count for ATSR routing scheme is more for few numbers of nodes but as the number of nodes rises it is varying.

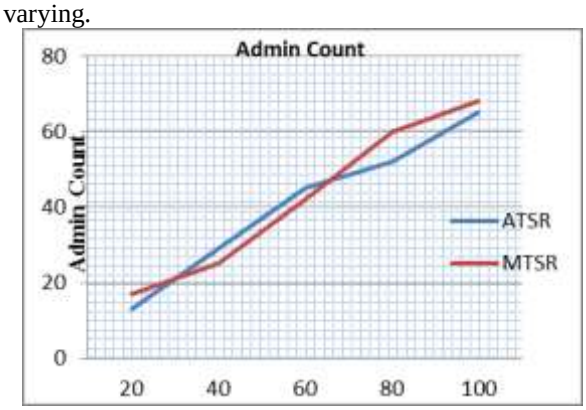

Fig. 3: Number of nodes vs. Admin Count

VI. CONCLUSION

In the proposed system we have implemented Mobility, Willingness and Trust built safe routing scheme in Mobile adhoc network which is simulated in NS-2 and its performance is compared with the existing Administrator and Trust built safe routing scheme in Mobile Adhoc network. This scheme is inspired from OLSR and more protected for communication between nodes.

In this scheme data packets can be routed by using most stable nodes from the network to the destination. It uses RSA asymmetric key algorithm for encryption and decryption of packets. It also uses the aggregate signature scheme for node authentication. The MTSR scheme performance is calculated with the help of various metrics like End to end delay, Packet delivery ratio and Admin count. We did the comparison of performance of both routing schemes. Simulation was carried out on different movable nodes.

The result of the simulation show that Packet delivery ratio of MTSR routing scheme is high in low dense network as compare to the existing ATSR scheme and it decreases gradually in both schemes in more dense network. The end to end delay of MTSR scheme is more as compare to the existing system because our system provides more security of the packets.

Admin count ratio (number of nodes involved in transmitting packets) is high for low dense and more dense network but for moderate density network number of admin nodes are low in proposed system as compared to the existing system. It is fact that any single routing scheme does not surpass the other routing scheme; their performance is based on various situations.

REFERENCES

[1] Sreeleja N. Unnithan ,Vijitha S., “Mobility based Stable Routing Scheme for Reliability in MANET “ , International Journal of Advance Research In Science And Engineering, Feb 2015.
[2] M. Rajendiran, S.K. Srivatsa, “Route efficient on demand multicast routing protocol with stability link for MANETs”, Indian Journal of Science and Technology, June 2012.
[3] SumanHalder, ParthaPratim Meta and Sukla Banerjee,“Mobility Aware Routing Protocol In Ad-Hoc Network”, CS & IT-CSCP, 2012.
[4] Rajashekhar C. Biradar, Sunilkumar S. Manvi, “Information Priority Based Multicast Routing inMANETs “,International Journal of Wireless & Mobile Networks (IJWMN), June 2011.
[5] Arnab Banerjee, Dipayan Bose, Aniruddha Bhattacharya, Himadri Nath Saha, Dr. Debika Bhattacharyya, “Administrator and Trust based secure routing in Manet“ , International Conference on Advances in Mobile Network, Communication and its Applications,2012.
[6] Ricardo de Oliveira Schmidt, Marco Antônio Sandini Trentin , “ MANETs Routing Protocols Evaluation in a Scenario with High Mobility”, IEEE 2008
[7] T. Clausen, p. Jacquet, "Optimized link State routing protocol (olsr)", RFC 3626 , workshops,2008.
[8] Xiaoqi li, lyu m.r., jiangchuan liu, "A trust model Based routing protocol for secure ad hoc Networks",aerospace conference,IEEE, Proceedings 2004.
[9] C. Perkins,E. Belding-royer,S. Das, "Ad hoc on demand Distance Vector (aodv) Routing." IETF. RFC 3561, JULY 2003.

