ODSRP-LET: On-Demand Secure Routing Protocol based on Link Expiration Time

Parul Singh
M.Tech (CS), Student
Department of Computer Science & Applications
Maharshi Dayanand University, Rohtak, Haryana, India

Gopal Singh
Assistant Professor
Department of Computer Science & Applications
Maharshi Dayanand University, Rohtak, Haryana, India

ABSTRACT

In MANET, nodes (mobile devices) can move freely and hence the network changes it topology very frequently. Due to mobility of nodes, link expires and the node has to find another route for sending the data. So, that route must be found in which link does not expire before all the packets reach the destination. In this paper a new secure routing protocol is proposed, On-demand secure routing protocol based on LET (ODSRP-LET), which is based on Link Expiration Time (LET) for sending the data packets from source node to the destination node. The conventional routing protocols like AODV, DSDV, DSR, etc. sometimes form unreliable link which causes link breakage. To revive broken link, route maintenance activity is initiated which generates heavy control traffic. During link disconnection, loss of data packets also occurs. In this paper, a secure routing protocol is proposed which proposed to form a reliable link and link remain connected till all the packets reach the destination. The uninterrupted link time or link connectivity is determined using predicted Link Expiration Time (LET). With link reliability, security of data is also required. So, to provide security to the data of transmitted packets, asymmetric key cryptography (RSA algorithm) is used which provides confidentiality. On-demand secure routing protocol based on LET (ODSRP-LET) proposes to form reliable links to limit link disruptions. ODSRP-LET proposes to provide security as well as reliability.

General Terms

Link Expiration Time, Security.

Keywords

Link Expiration Time (LET), Security, Packets, Asymmetric Key Cryptography, and Reliable

1. INTRODUCTION

Mobile ad hoc network is non infrastructure i.e. it has no base stations or access points, and self-organizing. Due to the mobile nature of devices MANET has no fixed topology and it may change dynamically. So, in MANET, nodes (mobile devices) can move freely and hence the network changes it topology very frequently. In MANET, routing protocols have been designed to provide effective routes in the network which are followed by data packets. Depending on the network topology routing protocols can be divided into three types: reactive, proactive and hybrid. The present secure routing protocols provide security during data transmission and to data but for finding the route to the destination these protocols follow the same approach as followed by traditional routing protocols. So, with security, reliable route for sending the message is also needed. In an active connection, routes are subject to frequent disconnections. In such an environment, it is important to minimize disruptions caused by the changing topology. Many routing protocols have been proposed which improve their performance by using mobility prediction [1].

In this paper, ODSRP-LET is proposed which is based on mobility prediction. This is an on-demand source routing protocol in which the data packets contain source routes and LETs (amount of time two mobile nodes will stay connected). Route Request and Route Reply packets collect source routes and LETs so that once route is discovered, the source node place the entire route into the subsequent data packets. When the Route Reply packets containing the routes and LET reach the source node, the node chooses that route for sending the packets which is reliable i.e. during sending of data packets the link stay connected. If route is reliable, then the data packets follow that path should also be secure. So, security of data is also necessary. In the proposed protocol, the RSA algorithm is applied on data so that confidentiality of data must be maintained.

The paper is divided into five sections. Section 2 explains the previous work based on predicted Link Expiration Time. Section 3 discusses the proposed scheme i.e. on-demand secure routing protocol based on LET (ODSRP-LET). Section 4 discusses performance of the proposed protocol. Section 5 provides the conclusion.

2. RELATED WORK

An on demand Flow Oriented Routing Protocol (FORP) [2] routes real time traffic in MANET using mobility prediction. To minimize the disruption of the connection caused by mobility it uses mobility prediction method. In this protocol, the sender sends the flow to the destination by constructing a route to it on demand. If the source node has an expired route in its routing table, it broadcasts FLOW-REQ message to find the route to the destination. The node forwarding the message appends its own id and LET. At the destination RET is determined for the route by using the minimum of the set of LETs. A FLOW-SETUP message is sent back to the source node by destination node if the received route is more stable than the one currently in use. On receiving the message the intermediate nodes set up the flow state. The destination node generates the FLOW-HANDOFF message when the route is about to expire. When the source node receives the message, it determines the best route based on the information contained in the message. Then the source node sends the FLOW-SETUP message along the new route. This protocol routes real time IPV6 flows in highly mobile ad hoc wireless network.

Mobility prediction method is also applied on On-Demand Multicast Routing Protocol [3]. In this protocol, the source node establishes and updates the multicast routes and group membership on demand. The source node periodically broadcasts the JOIN DATA packet to the entire network. When the multicast receiver receives this packet it creates and broadcasts the JOIN TABLE to its neighbors. During this process, routes are constructed from sources to receivers. When the source sends JOIN-DATA packet; it appends its location, speed and direction. The next hop then predicts the link expiration time (LET) between itself and the previous hop. The minimum (between this value and MIN_LET) is included in the packet. The minimum between the last link expiration time and the MIN_LET value is the Route Expiration Time (RET). This value of RET is enclosed in the JOIN TABLE and broadcasted. When the source node receive many JOIN TABLE, it selects the minimum RET among all the JOIN TABLE. Then the source can build new routes by flooding the JOIN DATA. So, this protocol delivers data to multicast members using a mesh.

The LET based CDS (Connected Dominating Sets) algorithm [4] builds the CDS based on edge weights. Here the edge weights are the predicted link expiration time. The edge having the largest predicted LET is included into the CDS Edge List and the constituent nodes of the edge become part of CDS Node List. The neighbors and the incident edges are also said to be covered. If an edge has higher link expiration time and is the next candidate edge to be considered for inclusion into the CDS, this edge is added to the CDS Edge List if either of its end nodes of the edge has at least one neighbor node that is yet to be covered. This procedure is repeated until all the nodes are covered. Their simulation results show that LET-CDS has longer life time compared to MaxD-CDS, in networks of moderate and high density.

In QoS aware Multicast Routing Protocol with Mobility Prediction (MPQMRP) [5] the source node initiates the route discovery by broadcasting the route request packet to its neighbors. The node looks into its routing table for the destination when it receives the route request packet. The node checks the available bandwidth between them if it does not match. The node will use the location information for finding the LET between the nodes and for this the available bandwidth must be above the constrained bandwidth. After updating the information, the intermediate nodes then forward the route request packet to their neighbor nodes. Each node receiving the route request packet calculates the LET between the nodes. The destination node sends the route reply packet. On receiving the route reply packets the source node selects the path having maximum RET. This protocol also includes route maintenance process. This protocol routes data packets to group members in case of high mobility and frequent link disconnections.

Speed Aware Routing Protocol [6] algorithm is based on demand-supply optimization approach. During the route discovery phase, when the neighbor node receives route request packet from the source node, it determines whether the packet sending node is too fast to form a reliable route. If it is too fast, the neighboring node rejects the packet sending node as a potential one-hop link. The packet sending node is too fast to form a reliable route is determined by calculating the LET. This LET (supply LET) is measured against the predetermined value (LET demanded by the network) for the determination of route reliability. Here, the LET is calculated with respect to the packet sending node. When the value of supply LET is lower than that of addition of demanded LET and time lenience factor, the link is predicted to be ineffective for the required amount of time; and hence the packet is dropped and the sending node is excluded from route inclusion. This protocol mitigates the effects of high mobility of nodes by reducing the frequency of route disconnections and identifies the highly mobile node by predicting link expiration time.

Rhim, A., Dziong, Z. have proposed 3 prediction algorithms based on either Global Positioning System or Signal Strength or both. So the mobile nodes predict the remaining connectivity time with the neighbor nodes in order to avoid disconnections. They use Dynamic Source Routing protocol with few modifications that enable integration of link expiration time metric. [27]

A reliable on-demand routing protocol (RORP) is proposed by NC Wang, SW Chang, where the duration of time the mobile nodes stay connected is determined by using GPS and the request region is discovered between the source and destination node. Many routes from the source to the destination node could be found and the routing path that requires longest duration of time for transmission is selected. This protocol also performs route maintenance. [28]

The statistic results of link and path availability properties in ad hoc network are derived Dan Yu, Hui Li, Ingo Gruber. Specifically, the available time and available probability in single-hop link and multi-hop path are investigated. In their mobility model each node moves at a randomly chosen velocity, a random vector, with direction and speed elements. This model is applied to investigate the link available properties in ad hoc networks, for both single-hop link and multi-hop path. [29]

A new routing metric is proposed for MANETs by Izhar Ahmed, K. E. Tepe, B. K. Singh. It considers both coverage area as well as link expiration information. The aim is to obtain routes that last longer with few hopes as possible. [31]

3. PROPOSED SCHEME

The proposed protocol, On-demand secure routing protocol based on LET **(**ODSRP-LET), uses DSR as the underlying routing protocol. In this proposed protocol, when the receiving node receives a route request (RREQ) or route reply (RREP) packet, it calculates the LET of the node with respect to the sender. LET predicts the amount of time the two nodes will stay connected. In the proposed protocol, security is also provided by using RSA algorithm. Brief explanation of the mobility prediction method i.e. Link Expiration Time (LET), the Dynamic Source Routing (DSR) Protocol, and RSA algorithm, is given below.

3.1 Link Expiration Time (LET)

In [1] a mobility prediction method has been introduced which utilizes location and mobility information provided by GPS. Given the motion parameters of two neighboring nodes, the duration of time the two nodes will remain connected can be predicted as follows: Assume two nodes I and j be within the transmission range of each other. Let (x_i, y_i) and (x_j, y_j) be the coordinates of mobile nodes i and j respectively. Let v_i and v_j be the velocities, Θ_i and Θ_j be the direction of motion of nodes i and j, respectively, where $\Theta_i \geq 0$ and $\Theta_j \leq 2\pi$. Then, the amount of time the two nodes i and j will stay connected, $LET_{i\text{-}j}$, is predicted by the following formula:

$$LET_{i\text{-}j} = \frac{-(ab+cd)+\sqrt{(a^2+c^2)r^2-(ad-bc)^2}}{a^2+c^2}$$

Where, $a= v_i\cos\Theta - v_j\cos\Theta$, $b= x_i - x_j$, $c= v_i\sin\Theta - v_j\sin\Theta$, $d=y_i-y_j$

3.2 Dynamic Source Routing (DSR) Protocol

DSR [7] is a source routing protocol. In DSR route discovery is done in the same way as in AODV. But in DSR, the data packets contain the source routes that specify each node along the route to the destination. Here, nodes maintain route caches which contain the route to the destination. A source node discovers the route if its route cache has either expired route or no route. A source node initiates the route discovery by broadcasting RREQ packets to its neighbors. RREQ packets contain the destination IP address as well as source IP address. When neighbor nodes receive the RREQ they add their own addresses in the RREQ packet and then forwards it. When the RREQ reaches destination, it creates an RREP packet in which the destination node adds source route from RREQ. If the intermediate nodes have route to the destination node, then it appends the source route to the destination to the route present in the RREQ and then generates RREP. The RREP contains the reverse source route. There is another phase in the DSR: route maintenance. When a link break occurs, the nodes upstream of the break create a route reply (RERR) packet and it is forwarded to the source node. When RERR is received by the node, it removes from its route cache that error node and also all routes from that point where node is present in the route.

3.3 The RSA Algorithm

Ron Rivest, Adi Shamir and Len Adleman at MIT developed the asymmetric key cryptography system. This method is called as RSA algorithm. The approach used is that each communicating party possesses a key pair (one public key and one private key). To communicate securely public key is published and private key remains with the individual as secret. Hence, public key is used for encryption and private key is used for decryption of data. The prime numbers form the basis of the RSA algorithm. Its working is like that- multiply two large random prime numbers, and let the result of multiplication be N. Select the public key (K1) such that it is not a factor of (a-1)*(b-1), where a and b are large prime numbers. Then select the private key (K2) such that (a*K1)mod(a-1)*(b-1)=1 is true. Encrypt the plain text (PT) into cipher text (CT) like this: $CT=PT^{K1}mod(N)$. For decryption determine the plain text as follows: $PT=CT^{K2}mod(N)$.

3.4 Working of ODSRP_LET

Route discovery:

1. *Route request*: The source node broadcasts the Route Request (RREQ) packet to its neighbors. The source node places destination IP address as well its own IP address in the RREQ packet. The packet also contains sender node's spatial velocity and its spatial coordinates and these are determined by GPS. So the packet contains RREQ(S_IP, COORD, VELO, D_IP), where, S_IP is the sender IP address, COORD is the spatial coordinates and VELO is the velocity of sender node, and D_IP is the IP address of destination node. As the proposed protocol is source routing protocol so when the RREQ reaches the neighbor node, it calculates the LET with respect to the sender node and update their route to source and then append their IP address to the RREQ as well as replace sender node coordinates and velocity with its own coordinates and velocity in the packet. When any node receives the RREQ, it will calculate the LET with respect to the sender node. Thus, as the RREQ is forwarded throughout the network, the traversed path is accumulated in the packet.

2. *Route reply*: When the destination node receives the RREQ, it responds by creating a RREP. The destination node places the source route from the RREQ into the RREP and also places the LET_{S-R} (Link Expiration Time with respect to the sender node, here S is Sender and R is the Receiver) it calculated. The source route in the RREP is reversed and the RREP is unicast to the source node. So, each node receiving the RREP appended the LET it calculated when it had received the RREQ. The reply packet contains RREP(ROUTE; LET_{S-R}).

When all the RREP reaches the source node, it sends the data packets to that route which satisfies the following condition:

minimum($LET_{S-R)} \geq LET_{Demand}$

Here, minimum($LET_{S-R)}$ is the minimum of all the values of LET in the RREP packet and LET_{Demand} is the amount of time the sending node needs to send the packets.

$$LET_{Demand} = \frac{No.of\ packets\ to\ be\ send}{No.of\ packets\ to\ be\ send\ per\ second} seconds$$

If the source node receives more than one RREP which satisfy the above condition then that route will be chosen which has minimum LET and the other route will be cached. If all the values of LET of routes are equal then node can choose any route.

Fig 1 and Fig 2 illustrate this process. A set of six nodes has initial spatial coordinates as follows: node 1 (50,200), node 2 (150,300), node 3 (250,200), node 4 (150,100), node 5 (300,300), node 6 (300,100). Nodes 1, 2 and 6 travel in the same direction at speed of 10 m/s, 5 m/s and 15 m/s respectively. Dashed arrows show the direction of motion of nodes. But node 3, 4, and 5 travel in the opposite direction (at speeds 10 m/s, 25 m/s, and 10 m/s respectively) with respect to the nodes 1, 2, and 6. Suppose node 1 is the source node and node 6 is the destination node. Node 1 broadcasts the RREQ packet to its neighbor nodes as explained above. All the receiving nodes calculate the LET with respect to the sending nodes. When the destination node receives the RREQ it creates RREP which contains the source route as well the LET calculated by it and unicast the packet. Each intermediate node receiving the RREP packet appends the LET calculated by it as shown in Fig. 2. Suppose node 1 wants to send 30 packets to the destination node at the rate of 5 packets per second. Then, LET_{Demand}= 6 seconds. So, the path chosen by the node 1 for sending the packets is (1,2,5,6) because here the minimum(LET_{5-6}) is 6 seconds among all the links in that route, which is equal to LET_{Demand}. Other routes which has value of minimum(LET_{S-R}) larger than LET_{Demand} is not chosen because according to the proposed scheme that route is chosen which has value of minimum(LET_{S-R}) either equal to or greater than LET_{Demand} and not greater than other values of LET. For example, route (1,3,6), (1,2,3,6) are not chosen (LETs' are greater than LET_{Demand}) because their LETs are greater than the LET of route (1,2,5,6).

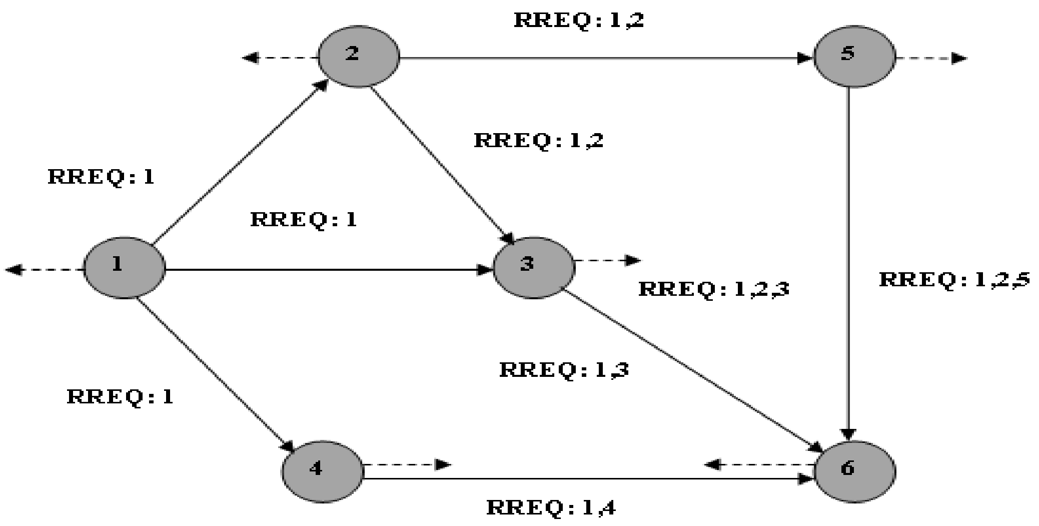


Fig 1: Route Discovery: RREQ Broadcast

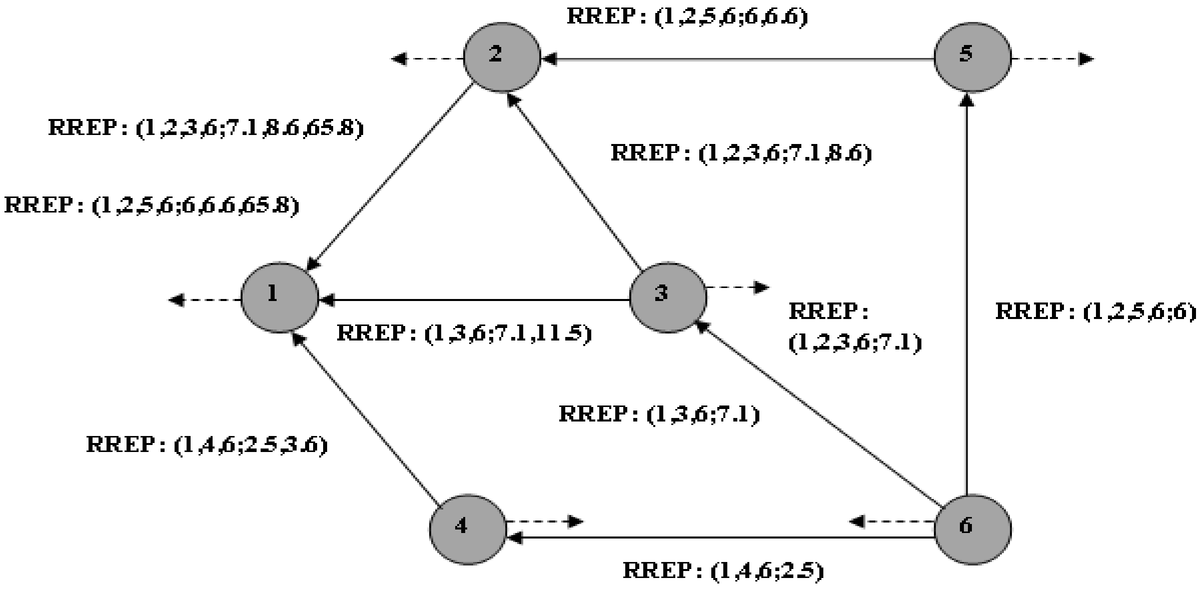


Fig 2: Route Discovery: RREP Propagation

3.5 Security in ODSRP-LET

Link reliability and link security both are important for the transmission of data in MANETs. The proposed protocol, ODSRP-LET, also proposes to provide security of data. It makes use of asymmetric key cryptographic algorithm (RSA algorithm) to offer routing security. RSA is based on the fact that it is easy to find and multiply large prime numbers but it is extremely difficult to factor their product. The private and public keys in RSA are based on very large prime numbers.

Here, assume that cryptography is applied during route discovery on RREQ and RREP packets. Suppose (K_{A+}, $K_{A-)}$ is the public and private key respectively of node A. Node A sends the RREQ by encrypting it with its neighbors' public key. A-> [RREQ]K_{B+}

Node B decrypts it with its private key and get back the original text: B-> [[RREQ]K_{B+}]K_{B-} => RREQ

Node B then sends the RREQ to its neighbors by encrypting it with their public keys. This process continues till the packet reaches the destination as shown in Fig 3. When destination node creates the RREP it will also apply this algorithm. Nodes during forwarding data through any route will also apply the algorithm.

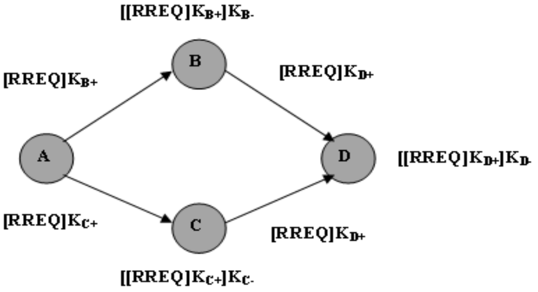


Fig 3: Encrypted RREQ

3.6 ODSRP-LET Algorithm

1. Determination of node coordinates and velocities.

2. Calculation of LET.

3. Determination of route for sending packets.

Algorithm for finding route for sending packets

```
For each route
  For each link
    If(minimum($LET_{S-R}$)==$LET_{Demand}$)
      Send all packets through this route   //after //sending packets no other //routes are checked
    End If
  End For
End For
If (no route is found)
 Set Min_LET= max_value   // max_value is any //constant value greater than //all the LETs of each route //already known
   For each route
     For each link
       If(minimum($LET_{S-R}$)>$LET_{Demand}$)
         If(Min_LET> minimum($LET_{S-R}$))
            Min_LET= minimum($LET_{S-R}$)
         End If
       End If
     End For
   End For
   If(Min_LET≠max_value)
     Send all packets through the route which has LET value equal to Min_LET
   Else
     No route found
   End If
End If
```

4. PERFORMANCE EVALUATION

This section evaluates the performance of proposed approaches via simulation. From Fig 1 and Fig 2 it has been concluded that the DSR protocol will choose the path (1,4,6) for sending the packets as it has less no. of hops and the distance between each node is less. But the link (1-4) expires in 2.5 seconds and then the node has to send data through different route. If it has no route in its cache, route discovery is again initiated by it. But in the proposed protocol, that path will be chosen which does not get expires before whole data get transferred. So, there is no link breakage and because of this no loss of packets (if occurs, it is very less) and overhead get reduced

From Fig 4, it has been concluded that at lowest speed of node, it has highest Link Expiration Time (LET). LET decreases as the node speed increases. At highest speed, the LET becomes constant and reaches zero (no connection). If the relative speed is negative then LET is maximum.

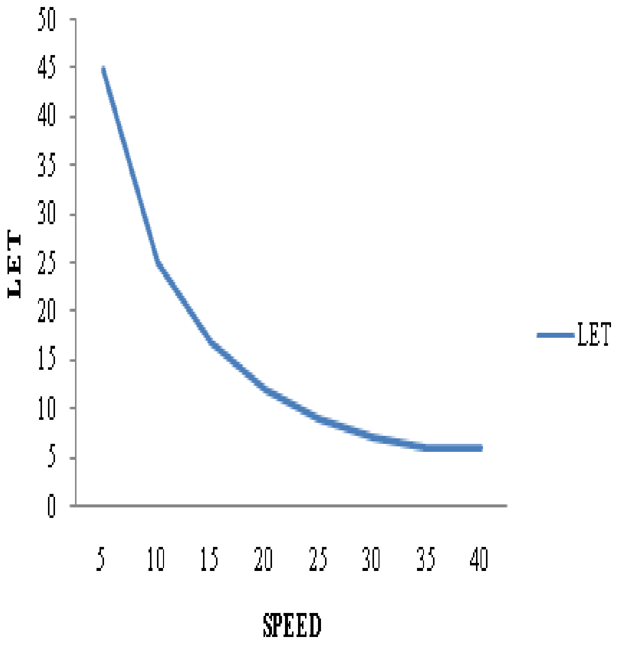


Fig 4: Speed vs LET

Packet Delivery Ratio: The ratio of the average number of data packets received by the destination node to the number of data packets transmitted by the multicast source. Packet delivery ratio is high at low mobility but it start decreasing becomes lowest at moderate mobility because speed increases and packets are more to transmit so packet delivery decreases. As the mobility increases more, packet delivery ratio also starts increasing because at this stage there are only few packets to transmit as nodes send few packets so they are delivered.

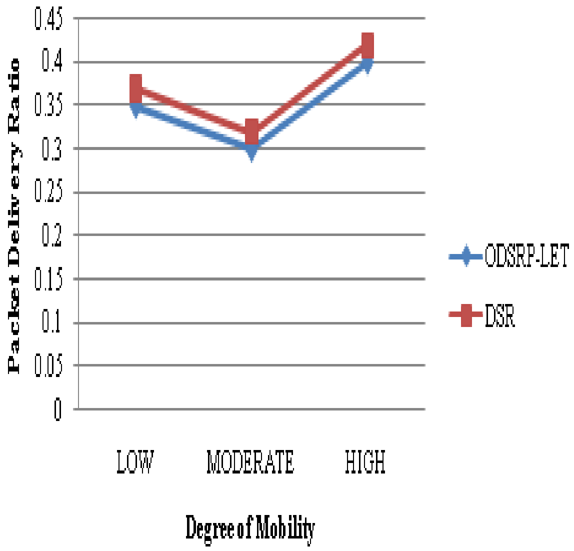


Fig 5: Degree of Mobility vs Packet Delivery Ratio

4.1 Analysis Using MATLAB

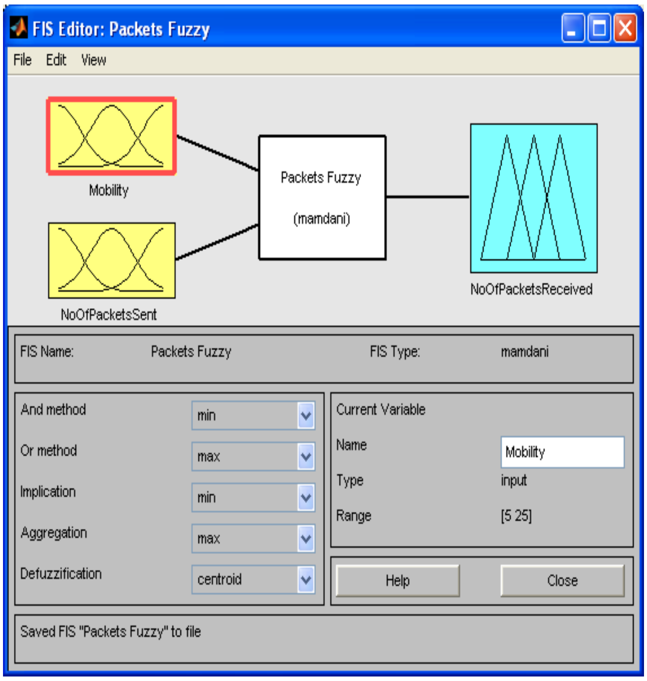
Here the analysis is done using fuzzy logic approach of MATLAB. There are some rules on the basis of which analysis is done. Mobility factor of node is considered here. Fuzzy systems are used to approximate functions. The fuzzy can be used to model any continuous function or system. The quality of fuzzy approximation depends on the quality of the rules. The result always approximates some unknown non linear function that can change in time. The basic unit of fuzzy function approximation is ―if then rules. A fuzzy system is a set of if- then rules that maps input to output.

To implement Fuzzy logic on MATLAB, mobility of nodes is considered the important factor. Here we found the impact of mobility on number of packets received, route length, number of routes, and no. of intermediate nodes. For this fuzzy rules are created. From these rules, the analysis is done how mobility of nodes affects the number of packets received, route length, number of routes, and no. of intermediate nodes. Here the mobility is assumed between 5 and 25 m/sec.

In Table 1, the mobility of nodes is between 5 and 25 m/sec and number of packets sent is assumed between 0 and 100. The first rule is defined as-If the mobility of nodes is LOW and the packets sent by the node are MORE then the other nodes receive MORE number of packets.

Table 1. Impact of mobility and packet sent on packets received by node

Mobility	No. of Packets Sent	No. of Packets received
LOW	MORE	MORE
MODERATE	MORE	LESS
HIGH	MORE	VERY LESS
HIGH	LESS	MORE



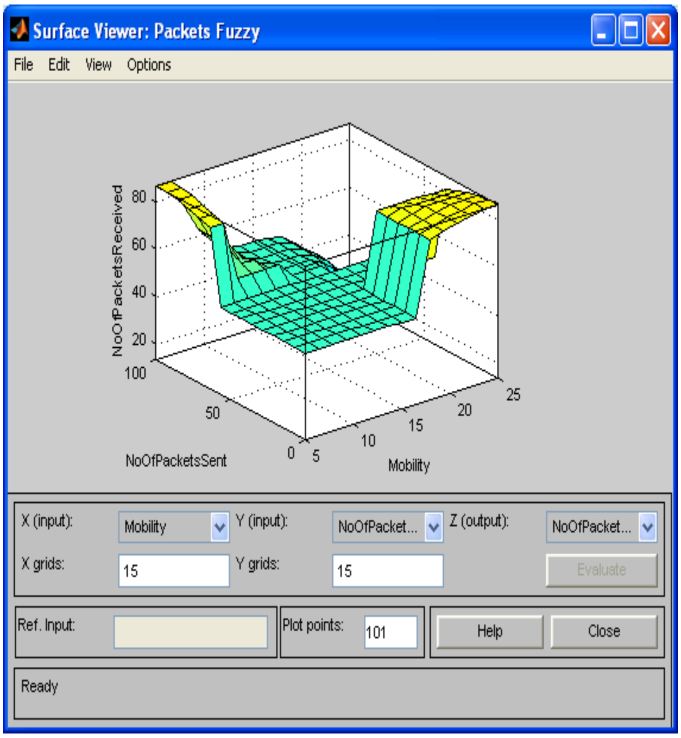
FIS Name: Packets Fuzzy
FIS Type: mamdani

And method: min
Or method: max
Implication: min
Aggregation: max
Defuzzification: centroid

Current Variable
Name: Mobility
Type: input
Range: [5 25]

Saved FIS "Packets Fuzzy" to file

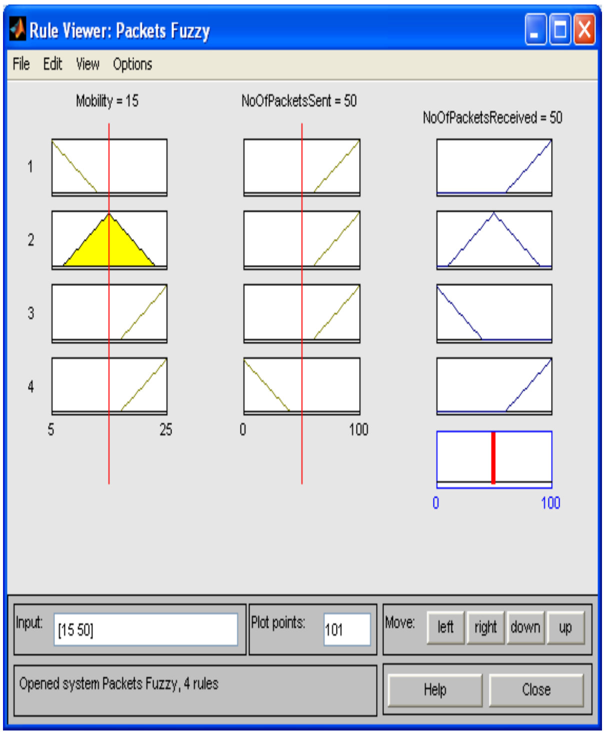
Fig 6: Fuzzy Logic system with two input producing output No. of Packets Received



X (input): Mobility
Y (input): NoOfPacket...
Z (output): NoOfPacket...
X grids: 15
Y grids: 15
Ref. Input:
Plot points: 101

Ready

Fig 7: Surface viewer



Input: [15 50]
Plot points: 101

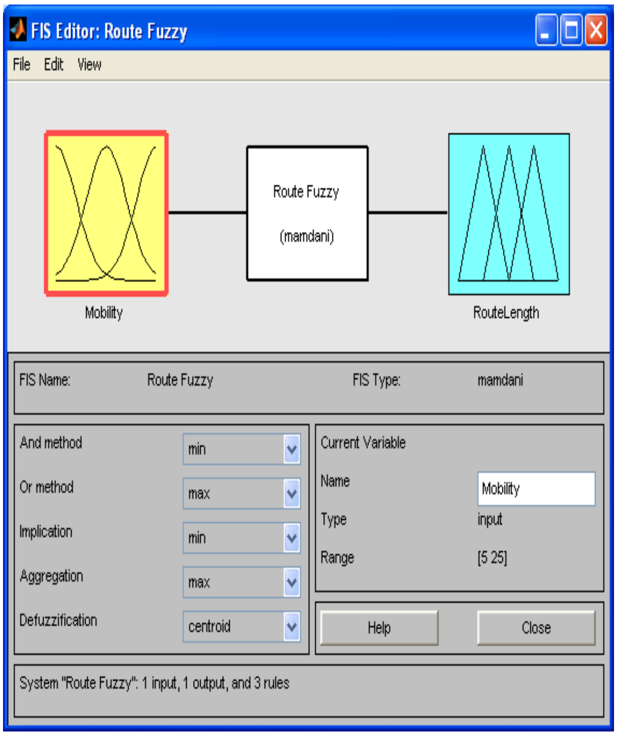
Opened system Packets Fuzzy, 4 rules

Fig 8: Fuzzy Rule Base viewer

In Table 2, the mobility is assumed between 5 and 25 m/sec. Here the route length is assumed between 0 and 1, 0 is considered as VERY LESS route length and 1 is considered as MORE (longest) route length. The first rule is defined as-If the mobility of nodes are HIGH then the length of route is MORE (Longest).

Table 2. Impact of mobility on route length

Mobility of node	Route Length
HIGH	MORE
MODERATE	LESS
LOW	VERY LESS



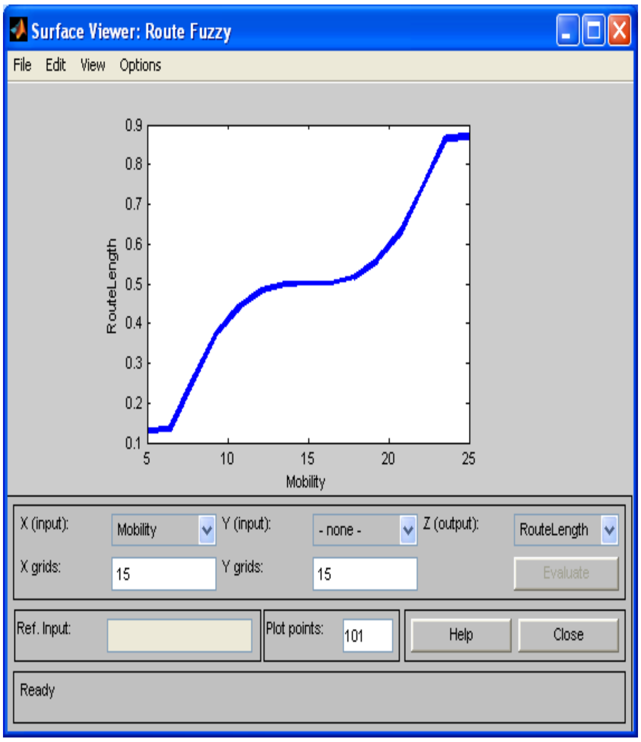
FIS Name: Route Fuzzy
FIS Type: mamdani

And method: min
Or method: max
Implication: min
Aggregation: max
Defuzzification: centroid

Current Variable
Name: Mobility
Type: input
Range: [5 25]

System "Route Fuzzy": 1 input, 1 output, and 3 rules

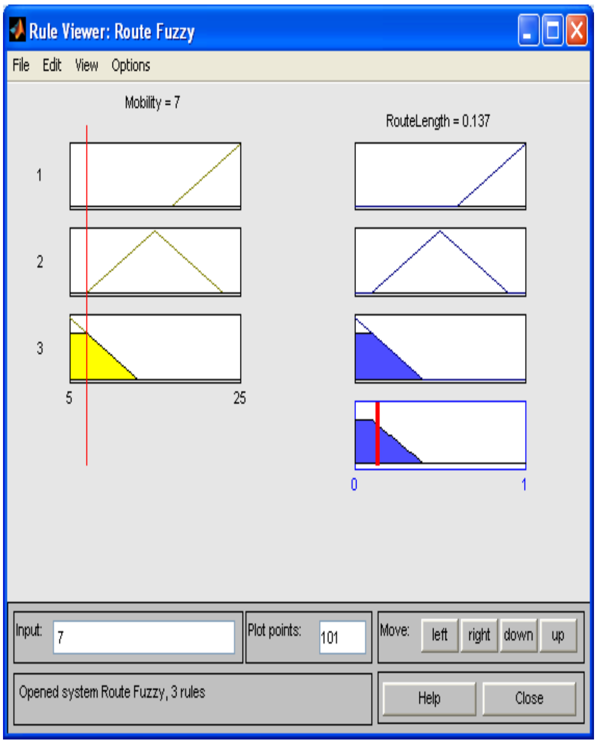
Fig 9: Fuzzy Logic system with one input producing output Route Length



X (input): Mobility
Y (input): - none -
Z (output): RouteLength
X grids: 15
Y grids: 15
Ref. Input:
Plot points: 101

Ready

Fig 10: Surface viewer



Mobility = 7
RouteLength = 0.137

Input: 7
Plot points: 101

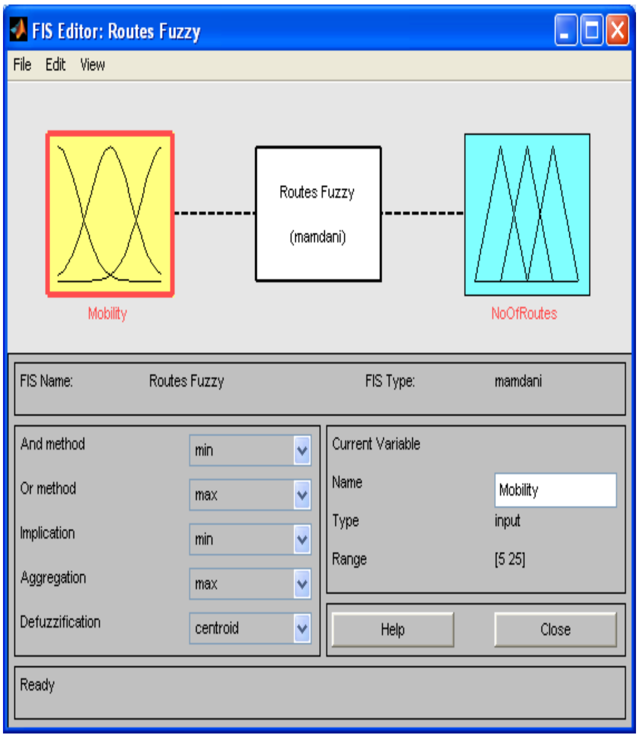
Opened system Route Fuzzy, 3 rules

Fig 11: Fuzzy Rule Base viewer

In Table 3 mobility of node is assumed between 5 and 25 m/sec. Here number of routes is assumed between 0 and 1, 0 is VERY LESS and 1 is MORE number of routes. The first rule is defined as-If the mobility of nodes are LOW then the number of routes formed are MORE.

Table 3. Impact of mobility on no. of routes

Mobility of node	No. of routes
LOW	MORE
MODERATE	LESS
HIGH	VERY LESS



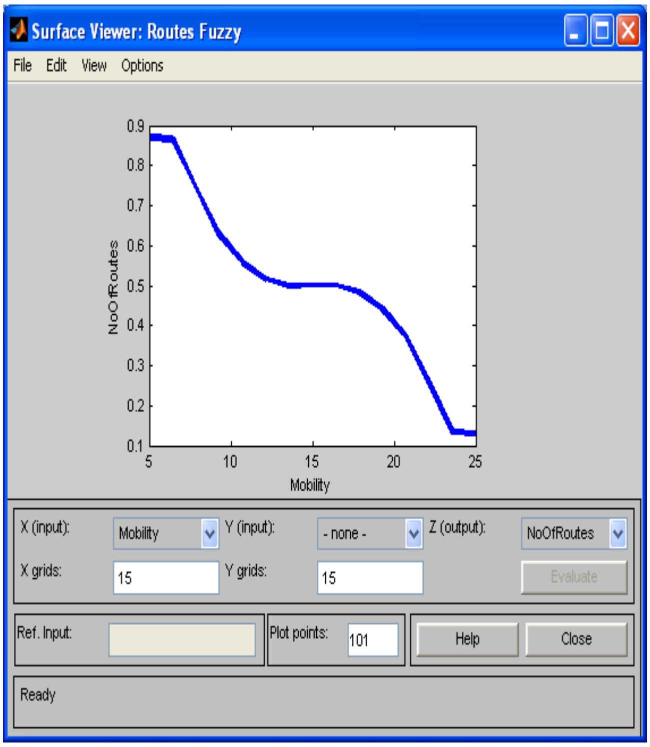
FIS Name: Routes Fuzzy
FIS Type: mamdani

And method: min
Or method: max
Implication: min
Aggregation: max
Defuzzification: centroid

Current Variable
Name: Mobility
Type: input
Range: [5 25]

Ready

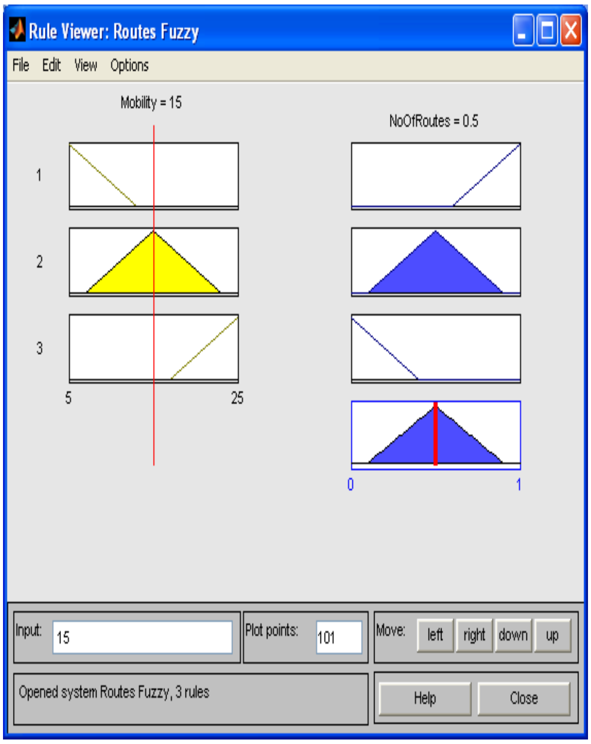
Fig 12: Fuzzy Logic system with one input producing output No. of Routes



X (input): Mobility
Y (input): - none -
Z (output): NoOfRoutes
X grids: 15
Y grids: 15
Ref. Input:
Plot points: 101

Ready

Fig 13: Surface viewer



Input: 15
Plot points: 101

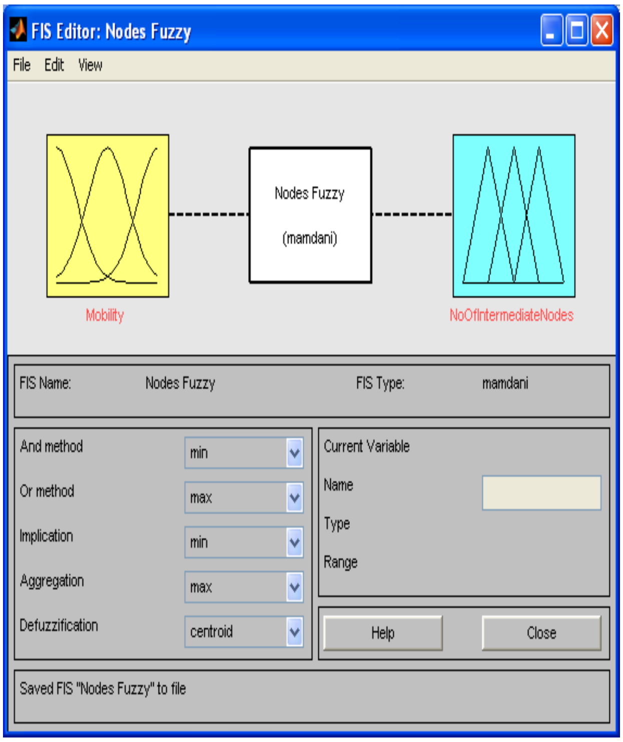
Opened system Routes Fuzzy, 3 rules

Fig 14: Fuzzy Rule Base viewer

In Table 4, mobility of nodes is between 5 and 25 m/sec. Here, number of intermediate nodes is assumed between 0 and 1, 0 is the VERY LESS number intermediate nodes and 1 is the MORE no. of intermediate nodes. The first rule is defined as-If the mobility of nodes is HIGH then no. of intermediate nodes in the route is MORE.

Table 4. Impact of mobility on no. of intermediate nodes

Mobility of node	No. of Intermediate nodes
HIGH	MORE
MODERATE	LESS
LOW	VERY LESS



FIS Name: Nodes Fuzzy

FIS Type: mamdani

And method: min

Or method: max

Implication: min

Aggregation: max

Defuzzification: centroid

Current Variable

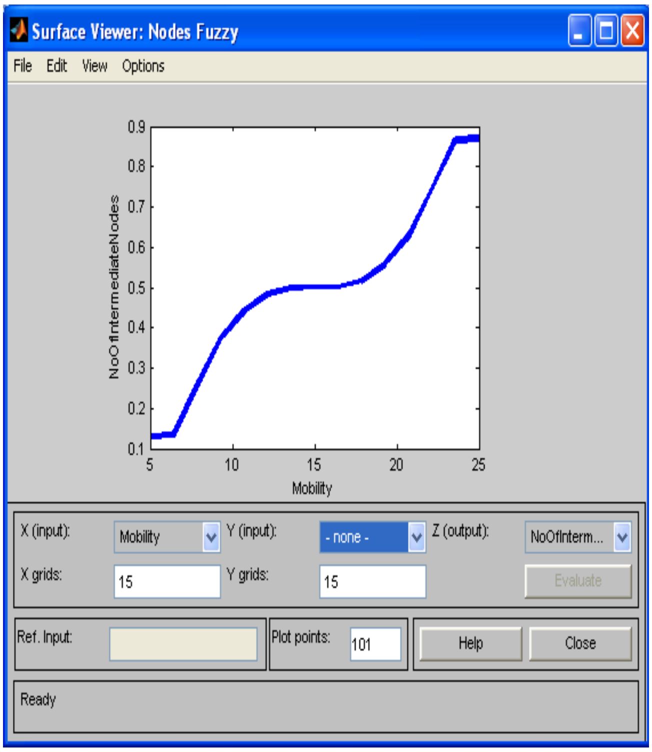
Name

Type

Range

Saved FIS "Nodes Fuzzy" to file

Fig 15: Fuzzy Logic system with one input producing output No. of Intermediate Nodes



X (input): Mobility

Y (input): - none -

Z (output): NoOfInterm...

X grids: 15

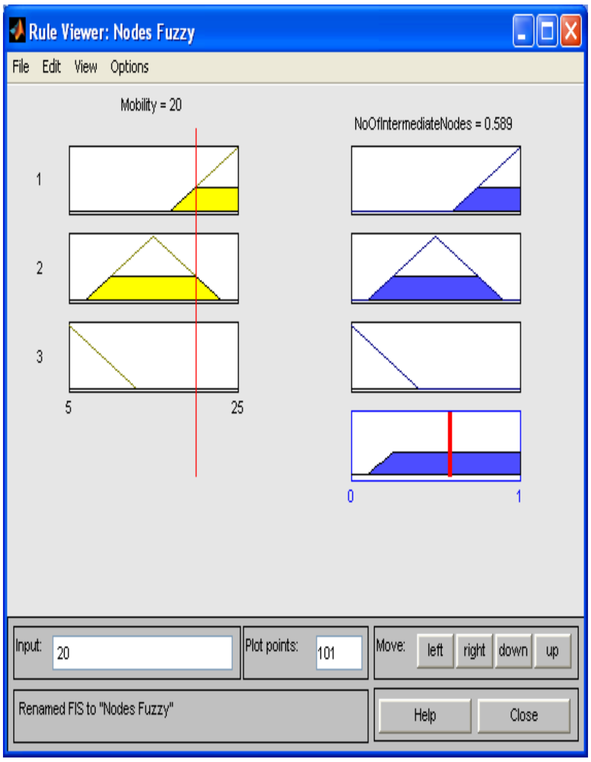
Y grids: 15

Ref. Input:

Plot points: 101

Ready

Fig 16: Surface viewer



Mobility = 20

NoOfIntermediateNodes = 0.589

Input: 20

Plot points: 101

Renamed FIS to "Nodes Fuzzy"

Fig 5.14 Fuzzy Rule Base viewer

5. CONCLUSION

In this paper a secure routing protocol is proposed which is based on predicted Link Expiration Time. Link breakage which is caused by highly mobile nodes generates additional control overhead. The proposed protocol tries to reduce this overhead. This protocol proposes to provide reliable links on the basis of its LET value. ODSRP-LET proposes to provide increase in link reliability and decrease in control traffic. With reliable links, this protocol also proposes to provide confidentiality of data. For security, the RSA Algorithm is applied to secure the confidentiality of data. So, security and reliability both are proposed in this protocol.

6. REFERENCES

[1] W. Su, S.-J. Lee, M. Gerla, "Mobility Prediction and Routing in Ad Hoc Wireless Networks", Int'l J. Network Management, vol. 11, no. 1, pp. 3-30, Feb. 2001.

[2] Su, William, and Mario Gerla. "IPv6 flow handoff in ad hoc wireless networks using mobility prediction," In Global Telecommunications Conference, 1999. GLOBECOM'99, vol. 1, pp. 271-275. IEEE, 1999.

[3] Lee, Sung-Ju, William Su, and Mario Gerla. "On-demand multicast routing protocol in multihop wireless mobile networks." Mobile Networks and Applications 7.6 (2002): 441-453.

[4] P. Fly, N. Meghanathan, "Predicted Link Expiration Time Based Connected Dominating Sets for Mobile Ad Hoc Networks", IJCSE, Vol. 2 No. 6, 2010.

[5] G. Santhi, Dr. A. Nachiappan, "Adaptive QoS Multicast Routing with Mobility prediction in MANETS", IJASUC, Vol. 1, No. 3 ,2010.

[6] Kirthana Akunuri, Ritesh Arora, Ivan G. Guardiola, "A Study of Speed Aware Routing for Mobile Ad Hoc Networks", International Journal of Interdisciplinary

Telecommunications and Networking, Volume 3, Issue 3, July 2011, pages 40-61.

[7] Rhim, A., Dziong, Z., "Routing based on link expiration time for MANET performance improvement", Communications (MICC), 2009 IEEE 9th Malaysia International Conference.

[8] NC Wang, SW Chang, "A reliable on-demand routing protocol for mobile ad hoc networks with mobility prediction", Computer Communications, Volume 29, Issue 1, December 2005, pages 123-135.

[9] Dan Yu, Hui Li, Ingo Gruber, "Path Availability in Ad Hoc Network".

[10] Izhar Ahmed, K. E. Tepe, B. K. Singh, "Reliable Coverage Area Based Link Expiration Time (LET) Routing Metric for Mobile Ad Hoc Networks", Ad Hoc Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 28, 2010, pp466-476-Springer.

[11] Johnson, David B., and David A. Maltz. "Dynamic source routing in ad hoc wireless networks." Mobile computing. Springer US, 1996. 153-181.