IJST EXPLORE International Journal of Science and Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-7318

International Journal of Science and Technology Volume 1 No. 9, September, 2012

Optimized Stable and Reliable Routing (OSRR) Mechanism in MANET

Ankit Verma, A.K.Vatsa
Shobhit University, Meerut, UP, India

ABSTRACT

Mobile ad-hoc Networks are highly dynamic networks and Quality of Service (QoS) routing in such networks is usually limited by the network breakage due to either node mobility or link breakage of the mobile nodes, limited battery power, node shutdown or failure, and many more factor. To fulfill certain QoS parameters like routing in presence of multiple mobile nodes and the stable path among communicating nodes are essential. Such paths aid in the optimal stability and reliability in case of path breakages. Therefore, in this paper we proposed an optimized stable and reliable routing mechanism in MANET that's includes route discovery through node selection and edge selection based on various parameters. Thereafter optimal path is selected based on Global weight.

Keywords: *MANET (Mobile Ad Hoc Networks), Routing, Multicast, Optimal Route, Link Stability, Node Selection*

1. INTRODUCTION

`

In recent years, the network is infrastructure based which results in more problems at the time of disaster and at natural calamities. It is essential to build and use the network that does not have infrastructure that's why MANET came in existence. MANET [1, 2] is collection of mobile/semi mobile nodes with no existing pre-established infrastructure, forming a temporary network. MANETs differs it from wired networks in the way that they have fast and unpredictable topology that changes due to nodes mobility and in this no dedicated routers is required to do routing every node works as a router and a host, it also have the capacity of changing channel capacity due to environmental effects and use multi hop approach to deliver data. Such networks are characterized by dynamic topologies network[6], bandwidth constrained existence and variable capacity links, energy constrained operations, and highly prone to security threats. Due to all these features routing [3] is a major issue considered in MANET and it affect the QoS of network.

Quality of Service (QoS)[17,18] based routing in MANET is defined as a routing mechanism under which paths for flows are determined based on some knowledge of resource availability in the network as well as the QoS requirement of flows. The main objectives of QoS based routing[8] are dynamic determination of feasible paths for accommodating the QoS of the given flow under the policy constraints such as path cost, provider selection, power aware source [4] etc. The Optimal utilization of resources for improving total network throughput and graceful performance degradation during overload conditions will give better throughput.

Therefore QoS based routing becomes challenging in MANET, as nodes should keep an up-to-date information about link status. Also due to the dynamic nature of MANETs, maintaining the precise link state information is very difficult. Finally, the reserved resource may not be guaranteed because of the mobility [13] caused path breakage or power depletion of the mobile hosts. QoS routing should rapidly find a feasible new route to recover the service for that different parameters are analyzed to get the optimized and feasible path. Our motive in this paper is to design a routing technique, which considers stability and reliable [19] routing among the best path by selecting the best node.

Routing in MANETs has to contend with several limitations such as scarce bandwidth and energy, presence of unidirectional links and dynamically changing topologies [6]. In addition, packet radios have limited transmission range depending upon environmental conditions such as interference and fading effects. Since MANET nodes can continuously move, wireless links between nodes can be disrupted. The underlying routing mechanism has to be capable of constructing and maintaining routes in a timely manner. The routing mechanism has to accomplish this without generating excessive control overhead given the bandwidth and energy limitations. Multi-point communications [1] is important for MANETs since typical applications require nodes to work together in groups to accomplish certain tasks. However these approaches cannot be readily adopted for MANETs on account of the dynamically changing topology. This changing topology trigger frequent routing table updates which results in excessive

channel overhead and slow convergence. Hence MANETs require different techniques for creating and maintaining efficient and durable routes. One of the technique to provide an optimized path with routing mechanism will be discussed in this paper

This paper is organized in sections. The section – 1 describes the introductory information under heads of Introduction. On basis of intensive literature survey the related information is mention in section – 2 under head of background. Section – 3 mention the proposed work of problem identified in this paper. The conclusion and future scope are mentioned in Section – 4 and section – 5 respectively. Finally all papers referred in this paper are enlisted under heads of References in Section – 6.

2. BACKGROUNDS

The recent studies extensively focused on the stable and reliable path discovery. They provide link-disjoint and stable node and paths which selects multiple routes on demand based on the different parameter. MANET [1,2] is collection of mobile/semi mobile nodes with no existing pre-established infrastructure, forming a temporary network **.**As Mobile Ad hoc networks are characterized by low bandwidth, high packet loss, and dynamic, potentially frequent topology changes. In addition, nodes in ad hoc networks are mobile and wireless, they typically need to rely on a limited energy supply [4,6].

The wireless environment is broadcast in nature and nodes within transmission range of each other share the use of the available bandwidth. Thus, the effective bandwidth along a path in an ad hoc network is heavily dependent on the number of actively transmitting nodes within transmission range[1] of the nodes along that path; each node along a multi-hop path also shares the available bandwidth with the node before and after it in the path. Overall, the bandwidth in an ad hoc network may be significantly lower than the nominal bandwidth the network hardware can support.

Ad hoc networks are characterized by a potentially highly dynamic topology[1]. Topology variations can happen on a variety of time-scales and can be caused by node motion, propagation effects, depletion of battery resources on a node, node shutdown or failure. Ad hoc networks are also much more prone to packet loss than wired networks. The reception of a packet at a node depends on the signal-to-noise ratio [28] at which it is received, which in turn is affected by concurrent transmissions in the vicinity of the node, as well as by the propagation environment. Loss in the wireless environment may also be caused by interference sources that emit signal at a frequency overlapping the one used by the ad hoc network.

There are different address allocation schemes. The major requirement of ad hoc addressing schemes is ensuring the uniqueness of node addresses so that no ambiguity appears when they try to communicate. This is not as trivial as it seems, especially because of the dynamic topology of ad hoc networks. A MANET can be split into several parts and several MANETs can merge into one. Tens to thousands of nodes coexisting in a single network may participate concurrently in the configuration process. Moreover, the wireless nature, such as limited bandwidth, power, and high error rate makes the problem even more challenging. Besides handling a dynamic topology, the protocols much take into account scalability, robustness, and effectiveness. Various protocols use various initial methods [23] uses Duplicate Address Detection (DAD), Boleng[30] uses Agent discovery, Patchipulusu [31] uses Leader Discovery and PACMAN [22] directly. Also most of the papers discuss about the IP auto-configuration when a new node joins or when the sub network joins another network but none of them discusses when a new network is initialized and there is no assignment of addresses or there is no Leader and there is no coordinator in the network. Consider the case during Military Operations or during the war where the soldiers carry the mobile devices which help them in communication among themselves, which happens in a remote place where is no network available, in such places a new network has to be initialized to initiate the communication among the devices. In such a place there are no address assignment done to the nodes or there is no DAD scheme or there is no Leader or coordinator among the mobile devices. IP address auto-configuration for such a network will be done. The IP Address assignment can be done using either Conflict Detection Allocation (CDA) or Conflict-Free Allocation (CFA). DAD is intended to detect conflicts with addresses. CDA then it works on selecting an available address and performs the DAD (Duplicate Address Detection). DAD is able to help detect conflicts with local address. In contrast to CDA, no duplicate detection is performed by the CFA method Duplicate Address Detection (DAD) is important to avoid misrouting. DAD is of two types Strong Dad and Weak DAD

Mobile Ad Hoc networks pose a problem of finding stable multi-hop routes [32] for communication between source to destination. The proposed approach of this focuses on the node prediction by using different approaches. Predicting the node movement can be done by avoiding the frequent link failures in Ad hoc environments. This approach allows to identifying the stable paths, reusing of paths, and avoid the link failures .Node prediction can be done by comparing the Received Power with the Adjacent Nodes and Predicting the Direction of the Nodes Based on the Node Velocity and some other factors .Due to movement of nodes in MANET is random link breakages in these networks are something common. This problem

causes high data loss and delay. In order to decrease these problems, the idea of link breakage prediction has appeared. In link breakage prediction, the availability of a link is evaluated, and a warning is issued if there is a possibility of link breakage. In this paper a new approach of link sability to avoid link breakage in MANETs is being proposed.

3. PROPOSED WORK

The routing Mechanism that establishes a route from source to destination in MANET will discussed in section 3.1 and 3.2

3.1 OSSR Principle

- **Address allocation scheme**

The address of mobile or wireless devices change from time to time .The wireless nodes, moving from one place to another have different points of presence in the network. The major requirement of ad-hoc addressing is to prevent nodes from duplicate addressing. Various protocols use various initial methods for address allocation like [23] uses Duplicate Address Detection (DAD).Firstly, allotted a unique Node ID to all nodes using Random number generator and IP address assignment of all nodes can be done by using either conflict detection allocation (CDA)[23] or conflict-free allocation (CFA).Before the IP Address is assigned to a node and used, however, a node must attempt to verify that this tentative address is not already in use by another node in the network. Specifically, it can be done by Strong DAD containing the tentative address as the target. If another node is already using that address, it will return a message saying so. If another node is also attempting to use the same address, it will also send the message for the target as well, and on getting the acknowledgment of it, the node has to change its tentative address and repeat the process again. The exact delay time for the DAD is network specific and may be set by network management. An address on which the DAD procedure is applied is said to be tentative until the procedure is completed successfully. A Tentative address is the address whose uniqueness is being verified, prior to its assignment to the node. A tentative address is not considered "assigned to a node" in the traditional sense.

It should be noted that DAD must be performed prior to assigning an address to a node in order to prevent multiple nodes from using the same address simultaneously. If a node begins using the address in parallel with DAD, and another node is already using the address, the node performing DAD will erroneously process traffic intended for the other node, resulting in such possible negative consequences as the resetting of open TCP connections. The detection and resolution of address conflicts are the indispensable part of address auto-configuration protocol operation

- **Node selection scheme**

In MANETS, potentially all the nodes are in motion. So it is difficult to different parameter of nodes. So in our approach we use a model to find the different metrics so that on the selection of that best nodes is to be taken. We derive both exact and approximate (but simple) expressions of these probabilities. For node prediction we use different approaches these are:

Trust value*:* The trust value[29] generated by trust model essentially performs the function of trust derivation, computation, and application .No matter what kind of trust models, two types of evolutions, direct trust and indirect trust, are available. Direct trust is first-hand information for neighbours and easy to obtain where indirect trust refers to the trust in indirect way. Trust evaluation in routing procedure is a remark of a sender after it gets the service of a forwarding node. More specifically, a node *j* will give his neighbour's *k* a trust score after the node *k* transmits a packet or replies a packet that the node *j* sends. Packet dropping is always due to poor wireless communication quality or heavy traffic. Thus we use packet forwarding ratio to evaluate the quality of forwarding.

Packet Forwarding Ratio (FR) is the proportion of packets which have actually been forwarded correctly. Correct forwarding means the forwarding node not only transmits the packet to his next hop node but also forwards devotedly. For instance, a malicious neighbour node forwards the data packet after tampering with data. If the sender monitors this illegal modification, The *FR* of the neighbour will decrease. In our model, each node derives trust factors from packet forwarding ratio.
$FR(t_i)$ is defined as follows:

$$FR(t_i)=\begin{cases}\dfrac{N_C(t_i)-N_C(t_i-w)}{N_A(t_i)-N_A(t_i-w)}, & t_i > w \\ \dfrac{N_C(t_i)}{N_A(t_i)}, & t_i \le w\end{cases}$$

……..(1)

Where,

$N_C(t_i)$: the cumulative count of correct forwarding
$N_A(t_i)$: the total count of all requesting before time t
W: length of the time window.

During trust computation, a linear aggregate method is used to estimate the overall trust in a node according to trust factors, and a minimal value method is used to compute a path's trust. Trust values from the two trust factors (CFR and DFR) are assigned weights in order to determine the overall trust level for a particular node. The direct trust in node *k* by node *j* is represented as *Tjk* and is given by the following equation:

$$\mathbf{T_{jk}(ti) = w_1 \times CFR_{jk}(ti) + w_2 \times DFR_{jk}(ti)} \quad \text{……..(2)}$$

Where CFR_{jk} (ti) and DFR_{jk} (ti) respectively represent the control packet forwarding ratio and data packet forwarding ratio observed by node j for forwarding node k at time ti and w1 and w2 reflect the weights assigned to CFR and DFR respectively.

Node degree: No of neighborhood node to a particular node or the maximum no of node reside in any range of node. It can be find by calculating the signal strength of the neighbouring nodes In mobile ad hoc networks, nodes communicate with each other through the wireless channel, the strength of the node receives may be defined by

$$Pr = \frac{Pt\,Gt\,Gr\,At^2\,Ar^2}{l\,d^2} \quad \text{……..(3)}$$

Where,P_r=Received power

P_t=Transmitted power
G_tG_r=gain of transmitting and receiving antenna

At , Ar = antenna Altitude of the Tx and Rx

.l_d=distance b/w Tx and Rx

Battery power: Mobile nodes are battery driven. Thus, the energy resources for such networks are limited. Also, the battery power of a mobile node depletes not only due to data transmission but also because of interference from the neighboring nodes. Thus, a node loses its energy at a specific rate even if it is not transferring any data packet. Hence the lifetime of a network largely depends on the energy levels of its nodes. Higher the energy level, higher is the link stability and hence higher the network lifetime.
Stability: It is also useful parameter to decide the cluster head. Most stable node elect as a cluster head of cluster. There are following parameter to calculate the stability of node.

- Calculate the Distance between source nodes S and the neighboring Nodes N
- Then calculate the mean distance (MD_A) of its entire neighbor

$$MD_A = \frac{1}{N}\sum_{n=1}^{N} D_{A,n} \quad \text{……..(4)}$$

- Stability calculated by using the difference between two value of Mean distance at t and t-1.
- Calculated by the formula of stability factor (ST_A)

$$\mathbf{ST_A = MD_t - MD_{t-1}} \quad \text{……..(5)}$$

Node Lifetime: The Lifetime of the node is calculated both based on its residual energy and its past history because the active node that is used for many data-transmissions consumed more energy and have very shorter lifetime. Every T seconds node i reads the instantaneous residual energy value and the corresponding estimated energy drain rate e_{vi} is obtained.

Node life time (NLT) is defined as

$$\mathbf{NLT = E_n / e_{vi}} \quad \text{……..(6)}$$

Where, E_n is the residual energy of node i,
e_{vi} is the energy drain rate

Link Selection Scheme

In MANETS, there are so many link from source to destination. So it is difficult to select best reliable and stable link amongst them. So in our approach we use a model to find the different metrics so that on the basis of that best link is to be taken. For link prediction we use different approaches these are:-

Link Expiration Time: The mobility factor is proposed as Link Expiration Time (LET)[27], it used to identify the duration of the link will be alive. The velocity and direction of the movement is constant. The position of node i and node j is denoted as xi and xj , the velocity and direction of node i and node j is denoted as (vi, vj) and (θi, θj) (0<=θi , θj<2π) respectively. On that basis we will calculate link expiration time which will be describe as
Link Expiration Time:

$$LET = \frac{(-(ab+cd) + \sqrt{(a^2+c^2)r^2 - (ad-bc)^2}\ )}{(a^2+c^2)} \quad \text{……..(7)}$$

Where,
a = vi cosθi - vjcosθj
b = xi - xj
c = vi sinθi - vj sinθj
d = yi – yj

Best path: At any point, the Routing Request message (RREQ) and Routing Reply RREP contain a list of all the nodes visited with their trust score added to the total of trust score for each not along the path (C_{Ti}). Whenever a node receives a RREQ or RREP messages, it will check the updates of the route to the source node. Then it will select the best path (Bp) [12]among them and it will be defined as:

$$(Bp)\ Max = \left\{ \frac{\sum_{Ti \in P_i^{[s,d]}} C_{Ti}}{\sqrt{\Delta(P_i) \cdot \Delta(P_i)}} \right\}$$

……..(8)

Where, C_{Ti} = The total of trust score for each node along path
$\Delta(Pi)$ = The total of hop counts on the path Pi

Link Stability rate (LSR): It is also useful parameter to decide the best link. Most stable link select as a reliable link of cluster to send data. For MANETs routing algorithms to be able to select paths that are more likely to be stable. We propose a stability model to estimate link stability based on Link Expiration Time and Drain Rate and is defined as:

LSR = Link Expiration Time / Drain Rate
……..(9)

Drain Rate is defined as a metric for energy dissipation rate in a given node. Total energy consumption is calculated in every T sec by every node and the Drain Rate is measured by exponentially averaging the values of previous and newly calculated values

DRi = α DRold + (1-α) DRnew ……..(10)

Where, α is selected between 0 and 1 that gives higher priority to updated information. If the Drain rate is higher, then the node is faster to deplete its energy.

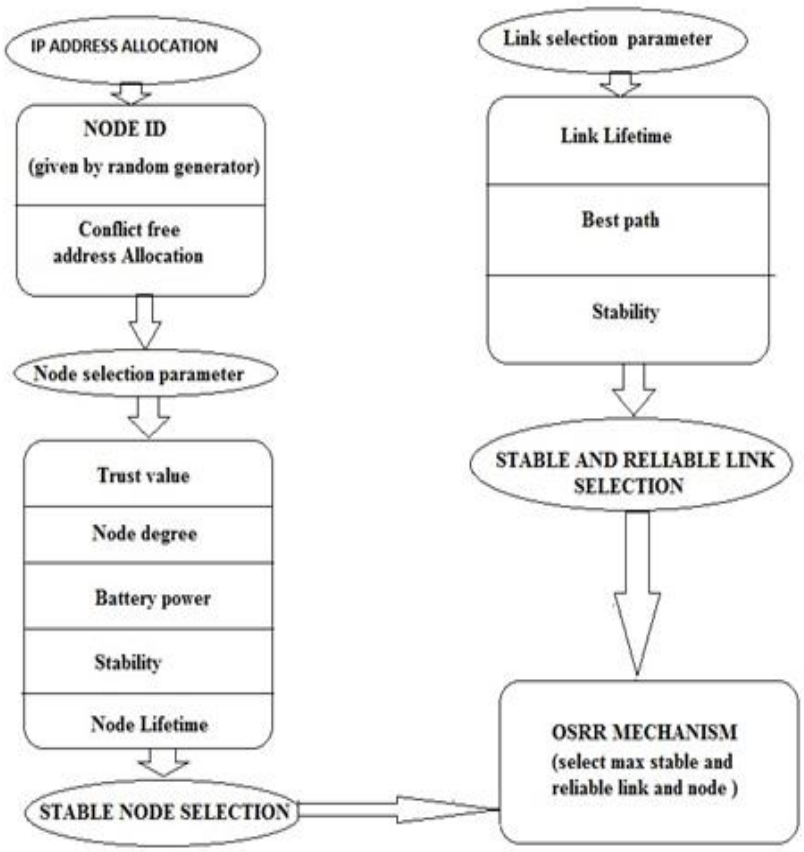

Figure 1: Flow Chart of Optimized Stable and Reliable Routing (OSRR) Mechanism

3.2 OSSR Routing Mechanism

Phase-1:

AddressAllocation( )

Assign Node Id for each node of MANET
No of Node = N;
For (i=0; i<N; i++)
{
NodeId[i]=RandomNoGenerator( );
}
DAD( ) // DAD = Duplicate address detection
{
initially address = unassigned
At any time t
Set $s_{addr}(t) = \{A_i (t) = addr\}$

// $A_i (t)=i^{th}$ Node ID at time t

If ($news_{addr} (t) == s_{addr}(t)$)
No assignment of that address to any one
Else
Assign the address
}

/*Random No Generator generate different random Node id for each node in MANET and the node address assignment of all nodes can be done by using either conflict detection allocation (CDA) or conflict-free allocation (CFA) */

Phase-2: Route Discovery by Node Selection and Link selection in mesh based Network

a) **Calculate the values of following parameters for each node in mesh network**

Step-(i): Node Trust Computation

NodeTrust( )
{
If (trustvalue==0 || trustvalue<0.5)
{
Don't Forward RREQ packet
// its signifies complete distrust
}
Else if (trustvalue==1)
{
Forward RREQ packet
// Its signifies absolute trust
}
Else if (trustvalue>0.5)
{
More correct chances occur than failures.
}
Else if (trustvalue=0.5)
{
Failure probability is equal to that of correct forwarding
}**}**

Step (ii): Node degree computation:

Nodedegree( )
{
If ($P_r >= P_{th}$)
//compare received power(P_r)with threshold value (P_{th})
Degree++;
Else if ($P_r < P_{r\_th}$)
Degree=degree;
}

Step (iii): Node Battery power computation:

Batterypower ( )
{
If (Battery Power<= $P_{Threshold}$)
// compare with Threshold power
{

//Node sends the low Battery power Signal to Its Neighbor and recalculates the Global weight for each node
}
Else (Battery Power> $P_{Threshold}$)
{
No requirement;

// calculate the weight for each node
}
}

Step (iv): Node stability computation
StabilityFactor( )
{
For (i=0; i<n; i++)
// for all the nodes in a cluster
{
Int max_value ,
If ($ST_A > ST_{ATHR}$)
// ST_A =stability factor
{
Less stable;
Else
More sable;
}
}

Step (v): Node lifetime computation

Nodelifetime( )
{
if(NLT> NLT_{thr})

{
Select node;
// Update trust-value and lifetime and Forward updated RREQ
Else
Not selected;
}}

GlobalweightNode ()

{
For (i=0; i<n; i++)
{
WGN [i]= (WT[i]* FT[i])+ (WD[i]*FD[i])+(WB[i]*FB[i])+ (WSN[i]*FSN[i]) + (WNL[i]*FNL[i]);

// WGN [i] = Global Weight of node

where,

FT[i]= Trust factor
WT[i]=Partial Weight factor for trust factor
FD[i] =Node degree
WD[i]=Partial Weight factor for node degree
FB[i]=Battery power
WB[i]=Partial Weight factor for Battery
FSN[i]= Stability
WSN[i]=Partial Weight factor for Stability
FNL[i]= Node Lifetime
WNL[i]=Partial Weight factor for Node Lifetime
If(WGN [i]> WGN_{THR})
{
Select that node for communication and forward the RREQ packet
}
}

b) Calculate the values of following parameters for each link in mesh topology:

Step (i):Link lifetime computation

LinkLifetime( )

{
If (LET>= LET_{thr})
{
Select that route and check for best path
}
Else
{
Check for new route
}

Step (ii):Best path computation

Bestpath ( )

{
If(B_P>min_value)
// min_value means minimum value require for link formation
Select that path
}
Else
{
Check and wait for new path
}

Step (iii):Link stability rate computation

Linkstability( )

{
If(LSR>LSR_{Thr})
//compare with threshold value

{

link is more stable and reliable

}

Else

{

select another link

}

}

GlobalWeightLink ( )

{
For (i=0; i<n; i++)
{
WGL [i]= (WL[i]* FL[i])+ (WBP[i]*FBP[i]) + (WSL[i]*FSL[i])

// WGN [i]= Global Weight of Link

Where

FL[i] =LET= Link Lifetime
WL[i]=Partial Weight factor for Link Lifetime
FBP[i]= B_P = best path
WBP[i]=Partial Weight factor for best path
FSL[i] = LSR = Stability
WSL[i]=Partial Weight factor for stability
If (WGL [i] >WGL_{thr})

//compare with threshold value

{
Select that link for communication and forward RREQ
}

c) Calculate the optimal path values between Source and destination

OptimalPathSelection( )

{

```
For (i=0; i<n; i++)
{
WG[i]= WGN [i] * WGL [i]
}
OPTIMAL ROUTE= MAX(WG[i])

// select maximum value of WG[i] which will provide optimal stabile and reliable routing
}
```

Phase-3: Request Reply Message for maintenance:

In Mesh based Multicast Routing the node selection is performed with the help of RR and RP packets [24].

The frame format for Route Request packet:

SID	DID	TTL	HOP SEQUENCE	LSR	Node Sequence	VE

Where

SID: It carries the source address of node.
DID: It carries the destination address of node
Time to Live (TTL): It is used to limit the life time of packet, initially, by default it contains zero.
Hop sequence: It carries the hop count; the value of hop count is incremented by one for each node through which packet passes. Initially, by default this field contains zero value
LSR: when packet passes through a node, its LSR value with the node from which it has received this packet is updated in the LSR field. Initially, by default this field contains zero value
Battery power: It is used to determine the battery power. The node's current battery power are changed time to time depends on the node movement and stability

Route Reply packet:

Contains the following information in

SID	DID	TTL	HOPS	LET	BEST PATH	LSR

SID: It carries the source address of node.
DID: It carries the destination address of node
Time to Live (TTL): It is used to limit the life time of packet, initially, by default it contains zero.
Hop sequence: It carries the hop count; the value of hop count is incremented by one for each node through which packet passes. Initially, by default this field contains zero value.
LET: Link expiration time
BEST PATH: Select the best path among different paths in a cluster

LSR: when packet passes through a node, its LSR value with the node from which it has received this packet is updated in the LSR field. Initially, by default this field contains zero value

4. CONCLUSION

The proposed OSRR routing mechanism integrates a node selection with a stable and reliable link to establish and maintain trustworthy routes in the network. With the inclusion of this mechanism, it is expected that optimized stable and reliable routing protocol (OSRR) protocol would result in a higher percentage of successful data delivery inspite of mobility among nodes. It is also expected that the end-to-end delay and normalized routing load will be higher because the packets may need to take a longer route (which is more stable and reliable) and the nodes need to generate more routing messages. This shows that the use of OSRR does provide a higher percentage of successful data delivery. Therefore, it can be concluded that OSRR provides both stable and reliable route among communicating nodes.

5. FUTURE SCOPE

The proposed OSRR routing mechanism is more efficient and effective but as number of nodes over network is scaled up beyond certain limit then performance might be reduced because the packets may need to take a longer route (which is more trusted) and the nodes need to generate more routing messages. Also, we can explore more by considering parameter such as the probability factor, energy factor, and others more accurate, stable and reliable path will be discovered.

REFERENCES

[1] Perkins, H. D. Hughes and C. B. Owen, "Factors Affecting the Performance of Ad Hoc Networks," Proceedings of the IEEE International Conference on Communications (ICC), pp.2048-2052, 2002.

[2] Chlamtac, M. Conti and J. J.-N. Liu, "Mobile Ad hoc networking imperatives and challenges" Ad Hoc Networks, Vol. 1, pp.13-64, 2003

[3] M. Abolhasan, T.A. Wysocki, and E. Dutkiewicz, "A Review of Routing Protocols for Mobile Ad hoc Networks", Ad hoc Networks, Vol. 2, pp. 1-22, 2004.

[4] M. Maleki, K. Dantu and M. Pedram, "Power-aware source routing protocol for mobile ad hoc networks", Proceedings of the IEEE international symposium on low power electronics and design, pp.72-75, 2002.

[5] E. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE

Personal Communications Magazine, vol. 6, No. 2, April 1999

[6] Hasnaa Moustafa and Houda Labiod, "A Performance Analysis of Source Routing-based Multicast Protocol (SRMP) Using Different Mobility Models", CNRS. 0-7803-8533-0/04/$20.00 (c) IEEE, 2004

[7] Dr. Shuchita Upadhayaya and Charu Gandhi, "Node Disjoint Multipath Routing Considering Link and Node Stability protocol: A characteristic Evaluation", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 1, No. 2, PP-18-25, January 2010

[8] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Ad Hoc Networking, Addison-Wesley, pp. 139-172, 2001.

[9] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector Routing (AODV)", IETF RFC 3561, 2003.

[10] M. K. Marina and S. R. Das, "On-Demand Multipath Distance Vector Routing in Ad hoc Networks", Proceedings of the Ninth International Conference on Network Protocols (ICNP}, IEEE Computer Society Press, pp. 14-23, 2001.

[11] Damianos Gavalas "Encyclopedia of Next Generation Networks and Ubiquitous Computing"

[12] H. Sh. Jassim, S. Yussof, S.K. Tiong, K.H. Chong and S.P. Koh. Path Selection Technique for Highly Transmission Ratio and Reliable Routing in Manet, Journal of Applied Sciences, 11: 3744-3749, , 2011

[13] W.Su, S.Ju Lee and M.Gerla, "Mobility Prediction in Wireless Networks" MILCOM, Vol. l, pp.491-495, 2000.

[14] L.Wang, L.Zhang, Y.Shu and M.Dong, "Multipath source routing in wireless ad hoc networks", Proceedings of Canadian Conference on Electrical and Computer Engineering, Vol. 1, pp. 479-483, 2000.

[15] S. J. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad hoc Networks", Proceedings of the IEEE International Conference on Communications (ICC), Vol 10, pp. 3201-3205, 2001.

[16] Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, vol. 6, No. 2, April 1999.

[17] X.Li, Ph.D. thesis on "Multipath Routing and QoS Provisioning in Mobile Ad hoc Networks", Queen Mary University of London, 2006.

[18] S.Upadhayaya and C. Gandhi, "Quality Of Service Routing In Mobile Ad Hoc Networks Using Location And Energy Parameters", International Journal of Wireless & Mobile Networks (IJWMN), Vol. 1, No 2, pp. 138-147, 2009

[19] Clausen, T., Jacquet, P., Laouiti, A., Minet, P., Muhlethaler, P., Qayyum, A., and Viennot, "Optimized Link State Routing Protocol", Experimental RFC 3626, 2003

[20] S.Zahoor Ul HUQ,Dr. K.E.Sreenivasa Murthy, Dr. B.Satyanarayana, D.Kavitha "Analysis of efficient address allocation schemes in mobile ad hoc networks" International Journal of Engineering Science and Technology, Vol. 2(3), 227-231, 2009.

[21] Rajashekhar Biradar, Sunilkumar Manvi,"Mesh based multicast routing in MANET: stable link based approach ", International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, 1793-8163, april, 2010.

[22] M. Mohsin and R. Prakash, "IP Address Assignment in a Mobile Ad Hoc Network," Proc. MILCOM, vol. 2, pp. 856–61, Oct. 2002

[23] C. Perkins, J. T. Marinen, R. Wakikawa, E. M. Belding-Royer, and Y. Sun, IP address auto configuration for ad hoc networks, IETF Draft, 2001.

[24] R. Biradar, and S. Manvi, Mesh based multicast routing in MANET: Stable link based approach, International Journal of Computer and Electrical Engineering, vol. 2, no. 2, pp. 1793-8163, 2010.

[25] N. H. Vaidya, Weak duplicate address detection in mobile ad hoc networks, in Proceedings of ACM Mobile Ad hoc Network , pp. 206-216,2002

[26] S. Zahoor Ul Huq, K. E. Sreenivasa Murthy, B. Satyanarayana, and D. Kavitha, "Analysis of efficient address allocation schemes in mobile ad hoc networks" International Journal of Engineering Science and Technology,vol. 2, no. 3, pp. 227-231, 2010.

[27] I.Gurber and H.Li, "Link expiration Times in Mobile Ad hoc networks", Workshop on Wireless Local networks, in IEEE Local Computer network Conference (LCN), Tamba, Nov.2002.

[28] R.Dube, et al., "Signal stability based adaptive routing for ad hoc mobile networks", IEEE pers. Communication, vol.4, no.1, pp.36-45, 1997.

[29] "Trust-based On-demand Multipath Routing in Mobile Ad Hoc Networks", IET Information Security

[30] J. Boleng, "Efficient Network Layer Addressing for Mobile Ad Hoc Networks," Proc. Int'l Conf. Wireless Networks, pp. 271–77 ,June 2002.

[31] P. Patchipulusu, "Dynamic Address Allocation Protocols for Mobile Ad Hoc Networks" M.Sc. thesis, Comp. Sci., Texas A&M Univ. ,2001.

[32] Saleem. Sheik Aalam, "Node Prediction - Routing in Mobile Ad Hoc Networks" ISSN 1450-216X Vol.65 No.2, pp. 260-267, (2011)

AUTHORS PROFILE

Avimanyou Kumar Vatsa is working as Assistant Professor and Coordinator - CSE at Shobhit University, Meerut, (U.P.), INDIA. He obtained his M-Tech (Computer Engineering) with Hons. from Shobhit University and B-Tech(I.T.) from V.B.S. Purvanchal University, Jaunpur (U.P.). He has worked as software engineer in software industry. He has been in teaching from more than one decade. During this short period of time, he has been supervised several dissertation of M.Tech. students. He is on the editorial board and reviewers of several international and national journals in networks and security field. He has been member of several academic and administrative bodies. During his teaching he has been coordinated many Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national, international journals and conferences. His area of research includes MANET (Mobile Ad-Hoc network), Network Security, Congestion Control and VOIP-SIP (Voice over IP).

Ankit verma is working as Assistant Professor in Electronics and Communication Engineering Department at Dewan v.s. Institute of Engineering and Technology, Meerut (U.P). He is pursuing M.Tech in Communication Engineering at Shobhit University, Meerut (U.P) and completed B.Tech (ECE) from MIT, Moradabad affiliated to U.P. Technical University, Lucknow (U.P). His area of research includes Wireless Technology, Mobile Ad-hoc Network & Network Security.