Improved Flooding with QoS Metrics in MANET Grid

S. Nithya Rekha
Department of Computer Science & Engineering
College of Computer
Qassim Private Colleges Buraydah
Al-Qassim,Kingdom, Saudi Arabia
rekhasiva24@gmail.com

R. Uma Rani
Department of Computer science
Sri Sarada College for Women (Autonomous)
Salem, Tamilnadu, India
umainweb@gmail.com

***Abstract*- Mobile Ad Hoc Networks (MANETs) exemplify a complex distributed network, which is characterized by the lack of any infrastructure. The lack of infrastructure though on one hand purports many significant advantages over the infrastructure-based networks, these networks have additional constraints that conventional networks do not have. For example, the connection establishment is costly in terms of time and resource where the network is mostly affected by connection request flooding. The proposed approach presents a way to reduce flooding in MANETs with Speed by applying Grid Fisheye state protocol (GFSR). With certain Quality of Service (QOS), this protocol is compared and analyzed in Grid FSR in NS3 simulator**

Keywords - MANET-Fisheye State Routing (FSR) protocol, Grid Fisheye State Routing (GFSR) protocol, Intimacy Factor, Friend node, strange node, Speed, Throughput, delay.

1. INTRODUCTION

Flooding is dictated by the propagation of connection-request packets from the source to its neighborhood nodes. The proposed architecture embarks on the concept of sharing neighborhood information. The proposed approach focuses on exposing its neighborhood peer to another node that is referred to as its friend node, which had requested/forwarded connection request. If there is a high probability for the friend node to communicate through the exposed routes, this could improve the efficacy of bandwidth utilization by reducing flooding, as the routes have been acquired, without any broadcasts (Pei, 2000)(Hwang, 2006) (S. Nithya Rekha, 2012). Friendship between nodes is quantized based on empirical computations and heuristic algorithms. The nodes store the neighborhood information in their cache that is periodically verified for consistency. Inconsistent routes are erased rather than being updated after a record-validity period. The vicinity information is tracked based on a -- I'm alive signal to other nodes. These broadcasts are limited to a hop count of one and executed when the network activity is feeble. In this paper, it is focused to reduce flooding performance of the Fisheye State Routing (FSR) protocol in Grid using ns-3 network simulator under different performance metrics scenario in respect to Speed with Certain QOS (Dmitri D, 2002) metrics. The principal objective of a routing protocol is efficient discovery and establishment of a route between the source and the destination so that there can be a timely and efficient delivery of information between them. Simulation results show the performance of this proposed method.

2. RESEARCH MOTIVATION

It can greatly reduce the redundant messages, thus saving much network bandwidth and energy. It can also enhance the reliability of broadcasting. It can be used in static or mobile wireless networks to implement scalable broadcast or multicast communications. As a result, the proactive approach provides a better quality of service by this new approach of Probability of calculating the Intimacy factor with neighbor node and friend node. The simulation results demonstrate the advantages of this approach. In the early research the author had severe investigation to reducing flooding with Nodes, Density, Pause time (Rekha, 2012) (Chandrasekar, 2012)

In ad hoc mobile wireless networks, energy consumption is an important issue as most mobile hosts operate on limited battery re-sources. Existing models for evaluating the energy consumption behavior of a mobile ad hoc network have shown that the various components of energy related costs include transmission

power as well as the power of reception (Modiano, 2005). Most of the existing ad-hoc routing algorithms select the shortest path using various resources (C.Chandrasekar, 2014)(S.Nithya Rekha, 2012). However the selected path may not consider all the network parameters and this would result in link instability in the network. The problems with existing method are frequent route change with respect to change in topology, congestion as result of traffic and battery limitations since it's an infrastructure less network. The set of simple rules were evaluated with proactive protocols namely Grid Fisheye-State Routing (GFSR) protocol in the NS-2 simulation environment based on metrics such as throughput, delay, overhead, jitter and also considers the importance of the objects (nodes).

3. PROPOSED RESEARCH IN GRID FSR

3.1. Propagating Neighborhood Information Study: Timeouts and Cache

In order for the destination node to know the location of the destination or the receiver they have to acquire the route through the process of flooding. Flooding involves broadcasting of a packet to all the nodes of the network requesting the route of the destination node (S. Nithya Rekha, 2012). The nodes either respond with a reply back to the sender if in case, the current receiving node of the packet is the destination, or otherwise they forward the packet to other nodes. The destination node responds to the sender with the connection acknowledgement. The route from sender to destination path is traced by the acknowledge packet by forwarding hosts.

Though the process of flooding helps the sender to dynamically obtain the location of the destination and the route over which information could be transmitted, it unnecessarily augments the load on the network as all the nodes in the network participate in the process of flooding (Rekha, 2012),(Aggelou, 2005). If there is a frequency of flooding may altogether lead to the instability of the network. The direct implication of this observation is that flooding should be kept as infrequent as possible(S.Nithya Rekha, 2012). One standard method to reduce the flooding mechanism is to supply the nodes with a small cache where the routes could be stored for future location. The further problem is processed by continuously changing characteristic of the ad hoc network environment as the routes are stored in a cache. There is always a possibility for the destination nodes to move from their place to another or even switch off. In order to keep the data in the cache consistent they can be updated as frequently as possible as the cache produce a static value. The routes in cache must be updated and validated every so often. The direct implication of this is that broadcast will be done frequently, which is to be avoided at all costs.

A new parameter referred to as the timeout period (S. Nithya Rekha, 2012) is introduced to alleviate the problems arising. The timeout period is maintained for every route of the destination stored in the cache. This parameter reflects the lifetime of a route. The route in cache is deleted when timeout value expires. The frequency of broadcasts is reduced through this. The value of the timeout period reflects the frequency at which flooding occurs and if it is chosen to be a large number there is still a possibility of the route to become invalid before the expiry of the cache. Therefore, the timeout value has to be practically chosen.

An outline of the Reduced flooding algorithm for broadcasting in MANET

Algorithm Reduced Flooding (**m, p**)
Protocol receiving ( )
On receiving a broadcast message **m** at node **A** do the following:
If message **m** is received for the first time then
Broadcast **(m)** with probability **P** {local broadcast primitive to nodes within range}
End if
End Algorithm

Figure 1. An outline of the Reduced flooding algorithm for broadcasting in MANET

3.2. Neighborhood Nodes

The nodes in this approach obtain the routes only when demand arises. The nodes use the common flooding approach to acquire the routes. Gradually flooding decreases in the initial phases. The most common method of using a cache is a fixed timeout period for each route. The timeout value is chosen for the nodes which are equipped with a small cache to save the routes. The other constraints of the conventional network are selected by the timeout value. However, the variation in the approach comes from the fact that the expiry of the timeout period does not trigger an update. The routes of the destination in the cache are further erased after the timeout period. The nodes may then have to use flooding again to recover the routes, but in order to avoid that routes are shared between the nodes based on some criteria.

The primary focus of this protocol is on sharing information about the neighborhood of a peer with another node in the network. The neighborhood reflects the entries of routes in the cache. The sharing of neighborhood information is not a mandatory task rather it is done at the discretion of the nodes concerned. The given approach intends to minimize the flooding requests that are needed to acquire the same information in the absence of the sharing mechanism.

3.3. Intimacy Factor

Acceptance of the data is processed by sharing of neighborhood information by receiving node which decides the node that started its communication between the two is ready. This result could be made based on a parameter called the intimacy factor. The intimacy factor reflects the level of trust between the two nodes that communicate. A threshold level of intimacy factor could be defined called as IFTHRES, which could then be compared against the intimacy factor, calculated between two communicating nodes to determine, when exactly to begin the sharing of neighborhood information. If the intimacy factor calculated is greater than IFTHRES then the receiving node can make a request to the sender enquiring its acceptance to the information about the routes to nearby nodes. This request is optional and the receiver does so with prudence.

After the receiver ensures the node that initiated the communication is ready to receive the neighborhood information, it posts a request to the sender. The sender can accept or reject the request. It can take into account the load on the link, the load on it, and its power level before posting to the receiver its approval. This can ensure that the sharing of routes may not exhaust the limited resources available. The sharing of the information or routes begins after the transmission of the sender's consent to the request. The receiver shares a percentage of its cache entries with its friend node, depending upon the control levels and other criteria. The sender then comes to know the locations with good possibility to send messages to these of various destinations close to the receiver. There may be destinations, in which case the flooding process required for acquiring the same, have been eliminated.

3.4. Designing Approach

In a MANET, the presented approach could be modeled in the following way.

Total number of nodes in the network = T_n
Total number of nodes in cache = K_n
Unknown nodes = U_n

The network is considered to have T_n as number of nodes. The initiator of communication or the sender is assumed to have knowledge of routes of certain number of nodes in the network. The sender is ignorant of the route of the other nodes, of which a few may be near the receiver, with which the sender is currently communicating. The receiver is assumed to have a similar knowledge of routes of various nodes in the network.

Route Gain Ratio (RGR) = (contents of sender's cache) ~ (contents of receiver's cache) (1)

$RGR \propto \eta$, where η is the efficiency of the protocol.

After the receiving the routes of the nodes in the neighborhood of the receiver, these are stored in the cache of the sender. The basic understanding is that, given that the sender has contacted the receiver, it has a good

probability to communicate with the nodes nearby the receiver. Equation(1) Calculating the probability that the sender communicates with any of the unknown nodes or nodes for which it does not have the location, a clear understanding of the working efficiency of the protocol can be obtained.

Number of nodes (given): T_n

Probability that an unknown node is contacted by the sender: P_u

The approach will prove to be efficient only if the sender can utilize the information obtained from the receiver before it expires. Time available for the sender for utilizing the routes: T_{out}

Assuming the average time spent per node as, Average time spent in communicating with a node: $T_{avg,}$

Total number of calls possible before routes expires in Equation (2):

$$T_{out} / T_{avg} = T_c \quad (2)$$

Total number of unknown nodes: U_n (nodes whose route are unknown to sender)

Probability that an unknown node is contacted: P_u

$$P_u = (U_n \, C \, T_{calls}) / (T_n \, C \, U_n) \quad (3)$$

In Equation (3), when T_n is large, P_u tends to be very small. The maximum efficiency is gained only when the unknown node contacted is one which exposed by the receiver to the sender during the sharing of neighborhood information.

Let number of nodes exposed = E_n. Probability that a node exposed is contacted: P_e in Equation (4)

$$P_e = (E_n C \, T_c) / (U_n \, C \, E_n). \quad (4)$$

Probability that the node contacted forms a subset of the nodes exposed in Equation (5):

$$P = P_c * P_{e.} \quad (5)$$

If the probability that the node contacted is from the set of nodes whose routes have been exposed by the receiver, then the protocols succeeds in eliminating the flooding requests which otherwise would have been required to contact the unknown nodes. Considering the MANET environment to consist of a large number of nodes n and the probability P_u being small, Poisson distribution could used to model the situation as following.

Total number of nodes = $n = T_n$

Probability that an exposed node is communicated = P

Let x be the number of exposed nodes contacted by the sender. Then, $nP = \lambda$.

The set of routes that are exposed are only valid until the timeout period, after which they are deleted from the cache. The quantity of maximum concern here is the number of exposed nodes that are contacted.

Probability that x nodes are contacted = P(X = x)

$$P(X = x) = (e^{-\lambda} \lambda^{x}) / x! \quad (6)$$

$$P(X = x) = (e^{-np} \lambda^{x}) / x! \quad (7)$$

$$P(X = x) = (e^{-n (Pc* Pe)} \lambda^{x}) / x! \quad (8)$$

Where $P_c = (U_c \, C \, T_c) / (T_c \, C \, U_n)$

$$P_e = (E_n \, C \, T_c) / (U_n \, C \, E_n) \quad (9)$$

Total exposed nodes contacted: $T_e = P*E_n$

The higher the value of T_e, the lesser the broadcasts required for getting the routes for the unknown nodes. The probability that no exposed node is contacted is given by P(X = 0)

$$P(X = 0) = e^{-n (Pc^* Pe)} \quad (10)$$

In Equation (10), $P_c * P_e > 0$ and always a finite quantity,

$$P(X = 0) = e^{-n(Pc^*Pe)} = e > 0. \quad (11)$$

3.5. Increasing the Probability

The probability of contacting an exposed node is therefore never zero. To improve the probability and decrease further the flooding process that are carried out, the value of P(X=x) must be closer to unity. (S. Nithya Rekha, 2012)(Chandrasekar, 2012). To increase the number of exposed nodes contacted there exists two possible approaches, one by improving the value of E_n and the other wherein P is increased. Boosting the value of E_n is not under the control of the designer. E_n signifies the number of exposed nodes and is directly dependent on the neighborhood of the receiver that exposes the routes of the nodes to the sender. The value of E_n depends on the topology of the network, the density of the network and the mobility of the nodes in the network.

Although E_n is strictly not under the control of the network designer, the value of E_n can be enhanced considerably by increasing the number of nodes exposed. In general, the receiver might then be expected to expose routes of the direct contacts it has, to the sender. In order to escalate further the probability of contacting an exposed node, it can augment the sample space of the nodes exposed. In other words, it can expose more nodes. This involves the receiver exposing nodes that are connected to it even through multi-hop links. The different nodes can be exposed one by one based on priorities assigned to them according to the distance of the exposed node from the receiver. The receiver on receiving the message stops sending the routes. The second method of increasing the probability P to improve the value of T_e proves to be more feasible. In order to amplify the value of P the number of nodes that can be contacted before the exposed routes become invalid, can be boosted. This implies that the timeout period should be increased. If timeout value is enhanced then it can have two impacts on the network. The first impact is one, which would lead to lesser number of flooding, due to less frequent updates and a higher value of probability of contacting an exposed node. The second would promote a chance for the data or the routes to be corrupted between the timeout periods. As a consequence of this, a tradeoff has to be struck between consistency of data and the reduction of flooding requests. The below figure1 explains the flooding with increased probability in FSR protocol in Random way point model mobility (Rekha, 2012).

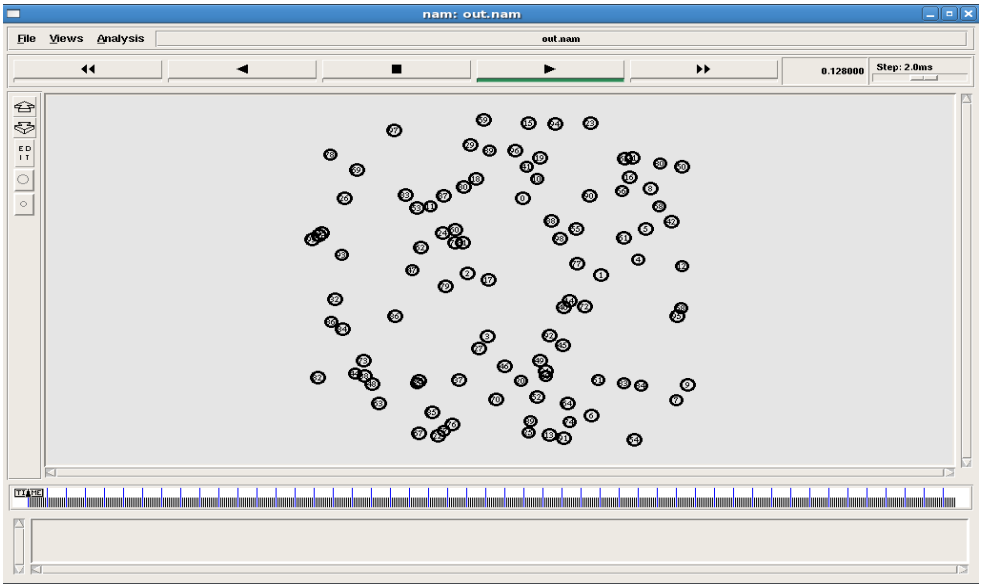

Figure 2. Flooding in FSR Protocol without Grid

3.6. Friend & Stranger Nodes

In general, when two nodes start communicating with each other the sender or the initiator of the communication is moved to the stranger node state with respect to the receiver. As the communication proceeds, the intimacy factor is augmented based on some well-defined method. After the intimacy factor crosses the threshold value, the stranger node moves to the friend node state again with respect to the receiving node. This transformation between the states indicates that the receiver now is starting to trust the sender and share some information regarding the routes of nodes in its vicinity. The change of state triggers the sharing of routes, which is initiated by the receiver at the end of the ongoing transactions. The speed of this state change is a very important parameter in the design of the protocol. The faster the change, the earlier the sender or the initiator obtains the neighborhood information. This also has the consequence of a malicious node being able to quickly get the location of various destinations and launch an attack on the network. After the state change, the receiver is identified as being ready to receive the request for sharing the information regarding nearby nodes. The nodes that are acquired from the receiver are stored in the cache with a timeout period. Like any ordinary route that is stored in the cache after the expiry of the timeout period as per the norms of the protocol the routes are cleared.

The method of shifting the state of a source node or the initiator of a communication, from stranger node to friend node could be based either on some empirical or heuristic algorithms. Empirically this could be done by maintaining a track of the messages transmitted between the nodes concerned or calculating the time during which the communication persists. It should also be noted that when the time of communication is taken into account, the factor could affect the sharing process In fact, it could bring down the efficiency of the protocol as the time to make use of the routes acquired is reduced. A balance therefore must be found between the two parameters. On the other hand, if the factor is based on the messages transmitted, a counter must be maintained by the receiver to count the packets received. In the aforementioned situation, the counter value could be directly used as the intimacy factor or could be weighted by any suitable constant to give the intimacy factor values.

Let the number of packets transmitted by the stranger node to receiver by Pt.

$Pt \propto k^*$ Intimacy Factor, where k is some constant.

There also remains a good chance for the routes exposed to be already known to the sender. Under such circumstance, if possible the sender tries to correct the information that is maintained in the cache of the receiver. The sender then posts a "Gratis Reply" to the receiver. This informs the receiver the route, which was declared corrupt, and the new route that has to replace the corrupted one. A comparison is therefore required at the sender's side when it's receiving the exposed nodes' routes to ensure that the routes are correct. If during the comparison process the sender or the friend node to the receiver, identifies a route that is already known to it but is different from the one exposed by the receiver, it has to be able to discriminate between the right and the faulty route. The faulty one need not always be a wrong route, but can be an old route for which a newer version exists. A mechanism can be used to either accept a standard reference or to communicate a chosen reference across nodes whichever proves feasible.

4. RESULTS AND DISCUSSION

The Network simulator 3 has been used to analyze the parametric performance of Fisheye State Routing Protocol (FSR) in Grid .The metric based analysis is shown in Figure 3 to Figure 8. We simulate flooding protocols using Network Simulator 3. From figure 2, we can see the full flooding carried out during simulation and in figure 3 we can see the flooding reduced fully in Grid architecture. Moreover, performance of flooding protocols using Grid FSR has reduced flooding with respect to Speed. The Speed is increased from 20 m/sec. Thus, the expectation that the efficient flooding scheme has improved the Grid FSR performance with various parameters.

4.1 Performance Metrics

4.1.1 End-to-End Delay

A specific packet is transmitting from source to destination and calculates the difference between send times and received times. Delays due to route discovery, queuing, propagation and transfer time are included in

the delay metric. Certainly Figure 4 shows decrease in delay as in Flooding is reduced in FSR within Grid scenario.

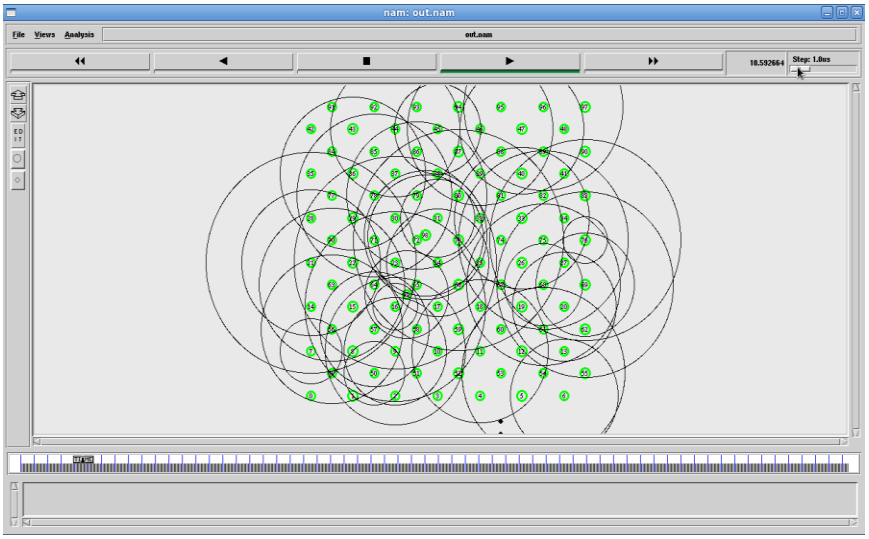

Figure 3. Increased Flooding in GFSR

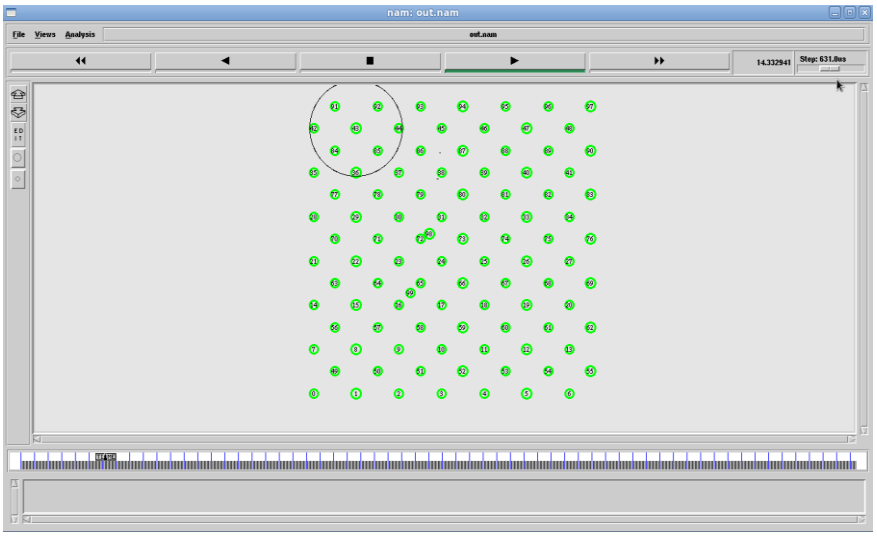

Figure 4. Flooding Reduced in GFSR

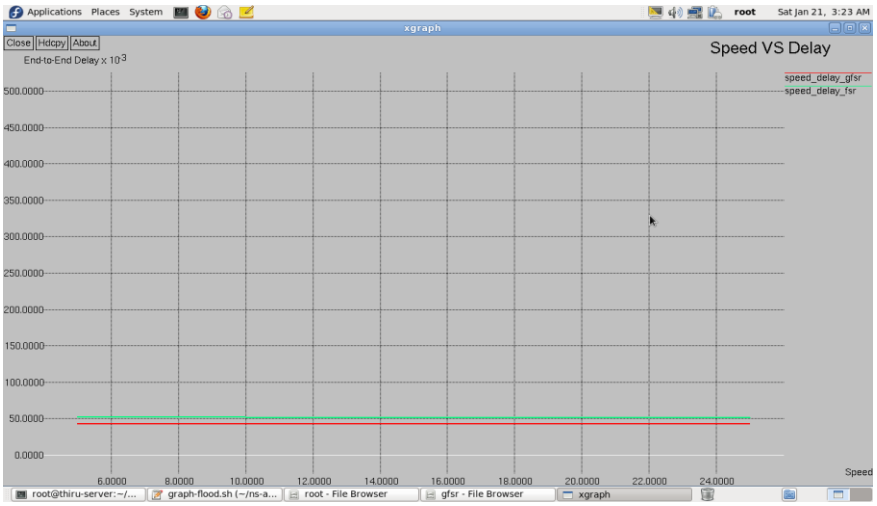

Figure 5. Speed Vs Delay in FSR&GFSR

4.1.2 Throughput

Throughput is the average rate of successful data packets received at destination. It is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second. The result is shown in Figure 6 where throughput is high in GFSR architecture.

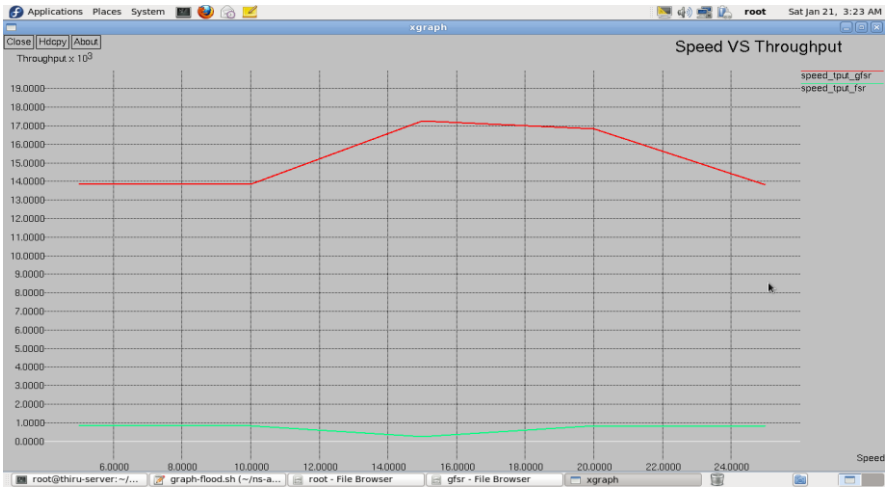

Figure 6. Speed Vs Throughput in FSR&GFSR

4.1.3 Jitter

Jitter is the variation of the packet arrival time. In jitter calculation the variation in the packet arrival time is expected to be low. The delays between the different packets need to be low for better performance in ad-hoc networks. It becomes a matter of concern if it is more than the threshold value, which is different for data. The result is shown in Figure 7 which has low performance in GFSR.

4.1.4 Control Overhead

The result shows that overhead is little high in GFSR than FSR in Figure 8. But there is an average reduced overhead in GFSR. Network Control overhead (NCO) is used to show the efficiency of the MANET's routing protocol scheme. It is defined, as the ratio of the number of control messages (the number of routing packets, Address Resolution Protocol (ARP), and control packets e.g., RTS, CTS and ACK) propagated by each node throughout the network and the number of the data packets received by the destinations. The reductions of network control overhead at higher data rate are very significant. This is because the same amounts of routing and control message are needed to route CBR traffic at lower data rate as well as at higher data rate. In reduced flooding, the control overhead can be reduced substantially.

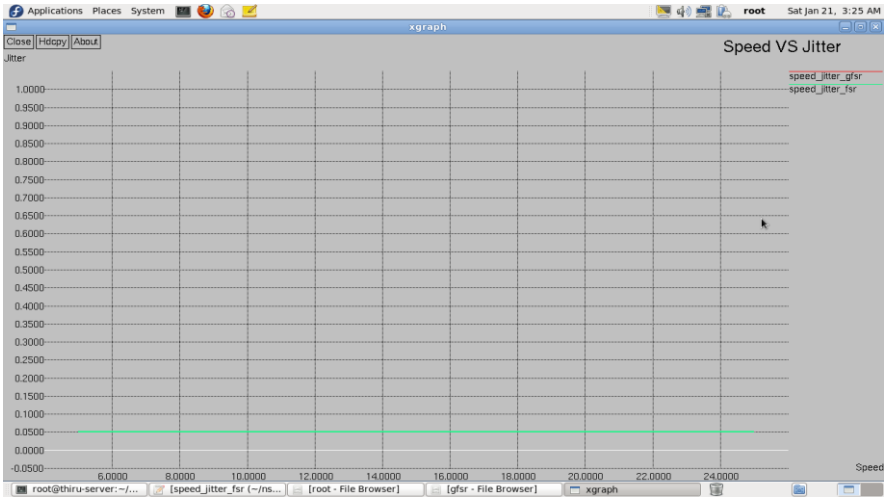

Figure 7. Speed Vs Jitter in FSR&GFSR

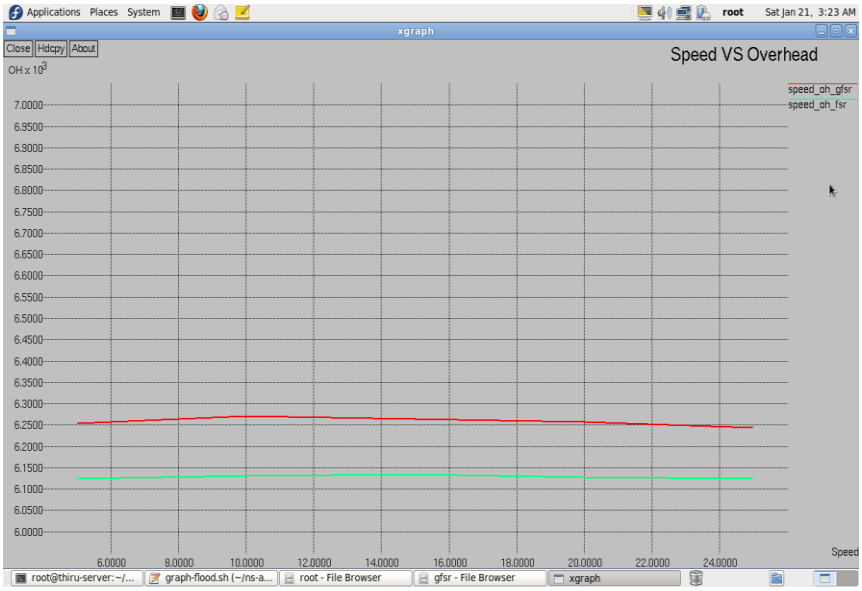

Figure 8. Speed Vs Overhead in FSR & GFSR

5. CONCLUSION

It is efficient to say that this paper have proposed a reduced flooding with QOS parameters such as delay, throughput, overhead, jitter with the variation of Speed in Grid FSR. We proposed a new scheme that dynamically calculates the probability with intimacy factor from source to destination. Simulation results show that the proposed Grid FSR protocol generates reduced flooding with QOS metrics. The simulation results also show that the proposed GFSR protocol has improved performance in flooding when the network speed is also increased.

REFERENCES

Aceves (1996). An efficient routing protocol for Wireless Networks. Journal of Mobile Networks and Applications, 1 (2), 183-197.

Aggelou (2005). Mobile Ad Hoc Networks – From Wireless LANs to 4G Networks.

Boyd (2002). Optimal power control in interference-limited fading wireless channels with outage- probability specifications. IEEE Transaction Wireless Communications, 1 (1), 46 – 55.

Bush (2005). A Simple Metric for Ad Hoc Network Adaptation. IEEE Journal on Selected Areas in Communications, 23 (12), 2272 –2287.

C.Chandrasekar (2014). An Energy Efficient Routing to Reduce Flooding in Weighted Rough Set Model using MANET. International Journal of Communication Networks and Distributed Systems –Inderscience journal, 13 (1), 83–105.

Chandrasekar (2012). A Strategy to Reduce Flooding in Grid Fisheye State Routing (GFSR) Protocol with Weighted Rough Set Model in MANET. International Journal of Mobile Network Design and Innovation (Inderscience Journal), 4 (4), 192 – 200.

Chandrasekar (2012). An Improved Approach in Flooding with Packet Reachability in Fisheye State Routing (FSR) protocol using MANET. Journal of Theoretical and Applied Information Technology (JATIT), 40 (1), 98-104.

Colagrosso (2007). Intelligent broadcasting in mobile ad hoc networks: three classes of adaptive protocols. EURASIP Journal on Wireless Communications and Networking .

Dassanayake (1997). User mobility modeling and characterization of mobility patterns. IEEE Journal on Sel. Areas in Communications, 15 (7), 1239–1252.

Dmitri D. Perkins (2002). A survey on quality of service support in wireless adhoc networks. Journal of Wireless Communication, Mobile Computing (WCMC), 2 (5), 503–513.

G. Pei (2000). Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks. IEEE International Conference on Communications, 1, 70-74.

Gerla (1998). Global State Routing: A New Routing Scheme for Adhoc Wireless Networks. IEEE ICC'98, (pp. 171-175).

Hwang (2006). Efficient Fisheye State Routing Protocol using Virtual Grid in High density Adhoc Networks. 8th International Conference on Advanced Communication Technology, 1475 – 1478.

Jang-Ping Sheu (2003). Energy - Conserving Grid Routing Protocol in Mobile Ad Hoc Networks. In The handbook of ad hoc wireless networks by CRC Press, Inc.

Bani Yassein (2006). Performance Analysis of Adjusted Probabilistic Broadcasting in Mobile Ad Hoc Networks. International Journal of Wireless Information Networks, 13 (2), 127-140.

Manoj (2004). Ad Hoc Wireless Networks: Architectures and protocols.

Modiano (2005). Finding Minimum Energy Disjoint Paths in Wireless Ad- Hoc Networks.

O.K. Tonguz (2006). Ad Hoc Wireless Networks – A Communication - Theoretic Perspective.

Rekha (2012). A Reduced Flooding Algorithm and Comparative Study of Grid Fisheye State Routing Protocol for MANET. International Journal of Scientific & Engineering Research, (IJSER), 3 (4), 1-10.

Rekha (2012). Performance Analysis of Probabilistic Rebroadcasting in Grid FSR for MANET. International Journal of Computer Science Issues (IJCSI), 9 (2).

Nithya Rekha (2012). Effect of Quality Parameters in Efficient Routing Protocol – Grid FSR with Best QoS Constraints. International Journal of Computer Applications, (IJCA), 37 (2), 51-57.

S. Xu (2007). An Analysis Framework for Mobility Metrics in Mobile Ad Hoc Networks. EURASIP Journal on Wireless Communications and Networking.

S.Nithya Rekha (2012). A Comparative Analysis of Probabilistic Broadcasting to reduce Flooding with FSR (Fisheye State Routing) Protocol and Grid FSR using MANET. The American Institute of Physics (AIP) - The Sixth Global Conference on Power, Control and Optimization. Las Vegas.

T. Camp (2002). A survey of mobility models for ad hoc network research. Inderscience Journal of Wireless Communication and Mobile Computing, Special issue on Mobile Ad Hoc Networking Research,Trends and Applications, 2 (5), 483–502.

Y.U. Chee Tseng (2002). The Broadcast Storm Problem in a Mobile Ad Hoc Network. Wireless Networks, 8, 153–167.