Reliable Data Delivery in Mobile Ad-Hoc Network using Fisheye State Routing

S.Ganesh
M.Tech student in Computer Science and Engineering,
Dr.MGR Educational and Research Institute University,
Chennai-600095, India.

***Abstract*— This paper addresses the problem of reliable data distribution in dynamic large scale mobile ad-hoc network, for which existing routing protocols are not suitable. An efficient Position-based Opportunistic Routing (POR) protocol is good in delivering the data in highly dynamic MANETs. But it is affected by the over heading problem and moreover there are no data confidentiality and data security. So we proposed a proactive routing algorithm known as Fish Eye state routing algorithm. This FSR algorithm provides excellent solution for delivering data in highly dynamic ad-hoc networks by updating and communicating nodes and nodes position and delivering data without over heading. Our proposed scheme works well in a large network of high mobility nodes. But still there is some susceptibleness to security threaten i.e., packets dropping by malicious nodes in the network. Our security scheme is proposed to minimize the number of black holes or malicious nodes or selfish nodes in the path to the destination, thus the number of data packets dropping can be minimized, and we secured the FSR protocol with security. In the case of communication hole, a Virtual Destination-based Void Handling (VDVH) scheme is further proposed to work together with FSR.**

***Keywords*- FSR, MANET, POR, VDVH**

I. INTRODUCTION

Mobile ad hoc networks (MANETs) have grown in wide range because of its significant advantages established by multihop, infrastructure-less transmission. But due to the error prone wireless channel and the dynamic network topology, data delivery in MANETs with high mobility remains an issue.

Existing routing protocols such as DSDV, AODV, and DSR are quite susceptible to node mobility because of the predetermination of an end-to-end route before data transmission. As the network topology is constantly changing, it is very difficult to maintain a deterministic route. It takes too much of time to discover and recover paths. Once the path breaks, reconstruction of the route without data loss is impossible. So we utilize Greedy forwarding to select the most suitable neighbor that can be the one which minimizes the distance to the destination in each step while void handling mechanism is triggered to route around communication voids.

Geographic Routing (GR) doesn't maintain any prior route information and location information. In the operation of greedy forwarding, the neighbor which minimizes the distance to the destination is chosen as the next hop. The transmission may fail, when the node moves out of its source's coverage area. In GPSR (a very famous geographic routing protocol), the MAC-layer failure feedback is used to offer the packet another chance to reroute. But test simulation reveals that it is still incapable of keeping up with the performance when node mobility increases. Due to the broadcast nature of the wireless medium, a single packet transmission will lead to multiple receptions. If such transmission is used as a backup, the robustness of the routing protocol can be significantly enhanced.

The concept of such multicast-like routing strategy has already been demonstrated in opportunistic routing. Most routing strategies use link-state style topology database to select and prioritize the forwarding candidates. In order to acquire the internodes loss rates, periodic network-wide measurement is required, which is impractical for mobile environment.

A Position based opportunistic routing strategy was introduced in which several forwarding candidates' cache the packet that has been received using MAC interception. If the best forwarder fails to transmit the packet within a certain time, any other candidate that formed locally in an order may transmit the packet. Thus the transmission will not be interrupted, since there are some candidates to transmit packets. POR's excellent robustness is achieved by exploiting potential multipath on the fly, on a per packet basis.

The POR overcomes the limitation of the traditional opportunistic routing and it provides advantages over the system in data delivery in the highly dynamic MANET system. But in terms of packet over heading and security the POR fall miserably and the system achieves considerable loss. Also the void handling mechanism which is the method of overcoming the communication hole in the MANETS the existing void handling procedure fails in most cases.

Thus we proposed a new approach for the reliable data delivery in highly dynamic MANETs and to overcome the limitations of POR. Our proposed Fish Eye routing system checks the packet over heading and provides security in data transmission in highly dynamic networks and also we implemented security in the routing protocol. The new system has improved over POR in data delivery, packet transmitting rate, security etc.

The new Void handling mechanism Virtual Destination-based Void Handling (VDVH) is used to handle communication voids.

II. MOBILE AD-HOC NETWORK

Mobile ad hoc networks (MANETs) represent a self configuring infrastructure less networks that consists of dynamic wireless mobile nodes. They are self configuring i.e., they don't have any predefined structure. Key applications include disaster recovery, transportation, heavy construction, mining, defense, and special event management. Ad hoc networking exists for more than 20 years. Previously a tactical network is the only communicating network in military side. New technologies such as Bluetooth, IEEE 802.11 and Hyper LAN enable eventual commercial MANET deployments other than the military domain. Nowadays Ad-hoc networks are mostly used for communication purpose, because of its mobility and self configuring nature.

A. Communication nodes

In MANETs the nodes communicate with each other without any infrastructure. Each node is independent and each node can communicate with any other node in any manner. The Ad-hoc mechanism works mainly on Mobile systems and Vehicle systems in small, large and city based scenarios. The communicating nodes are mobile nodes which can range from small hand held mobile phones, PDA's to Tablets and Laptops. These mobile systems are low processing power, low battery power and limited data transmission capacity.

B. Proactive routing protocol

Proactive protocols maintain the routing information for every known destination at each source. All nodes exchange their information periodically and also at every topology change. They maintain up-to-date routing information from each node to every other node.

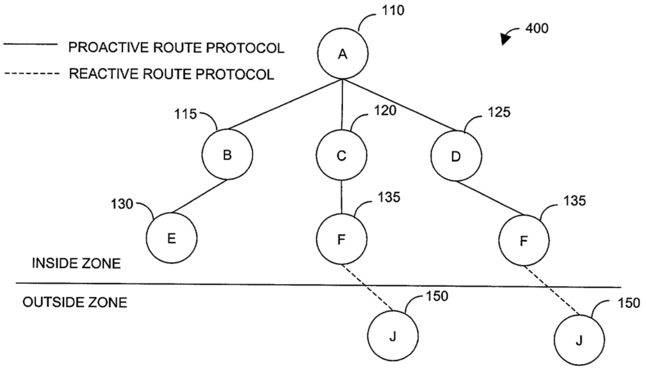

Fig. 1 proactive protocol operations

C. Data forwarding in position opportunistic method

Opportunistic network is a network, in which routes are established spontaneously between the mobile nodes. In this, communication between the nodes is possible, even if there is no root exists. Here the nodes don't have any knowledge about the network topology. Routes are built dynamically i.e., the paths are not predetermined. For the next hop, a node is opportunistically chosen only if it would bring the message closer to the final destination. In opportunistic networking no assumption is made about the existence of a complete path between two nodes wishing to communicate. The nodes that are communicating need to be present in the same network and time.

In position-based opportunistic routing mechanism, multiple receptions without losing the benefit of collision avoidance can be achieved. The concept of in-the-air backup first gets the location of the destination and then attaches it to the packet header.

As the destination node's location is keep on changing, the packet would be dropped repeatedly in the neighborhood of the destination. So additional check is introduced, in which the node that's going to forward the packet will check its neighbor list for its transmission range. If the destination node lies in that range, then the packet will be forwarded. Thus by checking the location information, the effect of multipath divergence is greatly reduced.

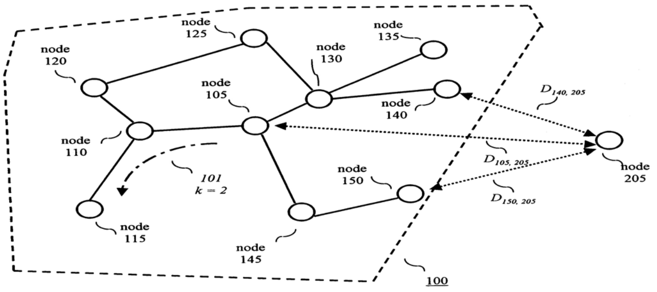

Fig. 2 Data forwarding using POR

In POR, it is very difficult to maintain a deterministic route as the nodes are highly dynamic and performance gets degraded when node mobility increases. Packet over heading may occur. The discovery and recovery procedures for neighbor nodes are also time and energy consuming. Malicious nodes and node path not detected as no security over this issue. Attacks by attackers in mobile system e.g., DoS attacks. The highly dynamic nature of the system makes the protocol forced to select the malicious path.

III. SECURE FISHEYE STATE ROUTING PROTOCOL

The system has mobile nodes which are present in highly dynamic network. Each node has its own power resource and computing power and location finding routing mechanism of the next hop node. Each node has specific speed of movement and direction and communication range. The system has "n" number of nodes. A node communicates with each other through Ad-hoc mode thus it is free of any infrastructure based communication.

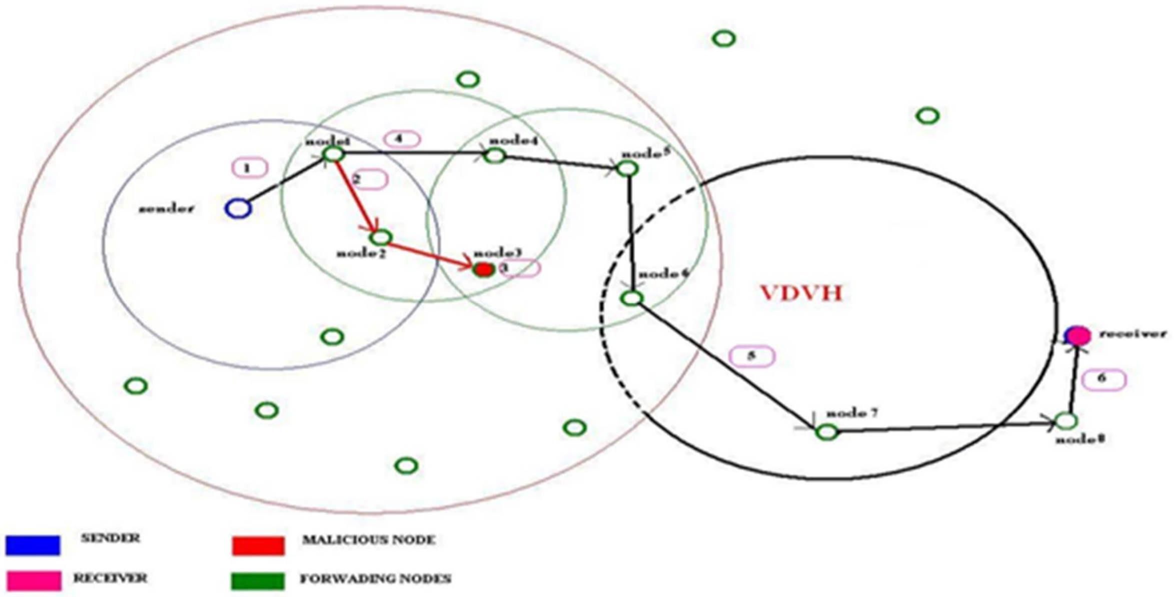

Fig. 3 FSR candidate selection

D. Fisheye state routing protocol

Fisheye State Routing (FSR) protocol is best suited for large scale and high mobility ad hoc wireless networks, which greatly reduces routing overhead. The name fisheye itself implies, that fish eye has the ability to see objects the better way when they are nearer to its focal point i.e., FSR maintains detailed and accurate information about the nearest nodes then farther nodes and exchange information periodically only with their neighbors.

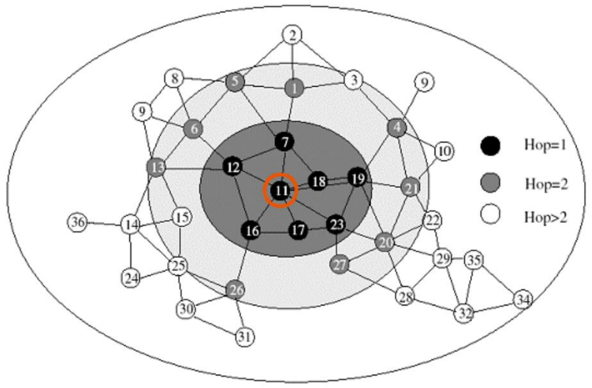

Fig. 4 Scope of FSR

1) FSR algorithm

```
Step i : Initialize Ai, TTi, NEXTi, Di
Step ii : if (pkt.Queue≠empty)
for each pkt Є pkt.Queue
Aiß Ai U {pkt.source}
source ß pkt.source
TTi.LS(j) ß TTi.LS(j) U {source}
for each j Є V
do
if ( j≠i) ^ (pkt.SEQ(j)) > TTi.SEQ(j))
then TTi.SEQ(j) ß pkt.SEQ(j);
TTi.LS(j) ß pkt.LS(j);
Step iii : for each j Є Ai do
if weight(i,j) = ∞
Ai = Ai – {j};
Step iv : for each x Є Ai do
TTi.LS(i) ß TTi.LS(i) U {x};
message.senderid ß i;
for each x Є N do
for ScopeLevel l:= 1 to L do
if ((Clock() mod UpdateIntervall = 0)
^ (Di(x) Є FisheyeScopel)) // Di(x) is calculated using
//Disjkstra"s Shortest path algorithm
then message.TT ß message.TT U {TTi.LS(x)};
step v : broadcast(j,message) to all j Є Ai;
```

E. Securing fish eye state routing protocol

The threats from the internal nodes are difficult to detect as they are from trusted sources. Threats on the MANET can be broadly divided into 2 categories

2) External threats

In the presence of an authentication protocol to protect the upper layers, external threats are detected in the physical and data link layers. The external threats again can be divided into two categories: Passive threats or threats to confidentiality or Eavesdropping and Active Threats or threats to the integrity and availability.

3) Internal threats

The threats posed by internal nodes are very serious; as internal nodes have the necessary information to participate in distributed operations. Internal threats also can be divided into two types; active threats and passive threats. Internal nodes can misbehave in a variety of different ways such as failed nodes, badly failed nodes, selfish nodes or malicious nodes.

F. Black hole attack

The black hole attack comes under the category of passive attacks which is launched by a selfish or malicious node to benefice itself in terms of conserving its energy or battery power. A node which is a black hole has two properties – it participates in the route discovery process and the second property is that, it sometimes does not forward the data packet towards to destination. These nodes create problems with data transmission if they come in the route to destination. Most of the nodes in MANET are resource constrained, as they mostly rely on batteries as their power source; so to conserve their battery power, they may act maliciously. So, when the data packets are forwarded to the destination these selfish nodes simply do not forward the data packets towards the destination. So all the packets move up to that node and disappear, which results in data packet dropping. So, that node acts as a black hole. The black hole attack can be launched both on control packets and data packets. Here we considered only the case of data packets, because in FSR algorithm the number of control packets is less compared to the data packets. But, when forwarding data packets if some of the packets are dropped, then alternate route is searched to forward the packets even if that route is the shortest one. This increases the time complexity of the protocol.

4) Solution to minimize black hole attacks in FSR

The problem can be minimized by selecting the appropriate route where the number of malicious nodes will be minimum. This can be done in a two step process (i) By detecting the malicious nodes (ii) By avoiding the malicious node while computing optimal path.

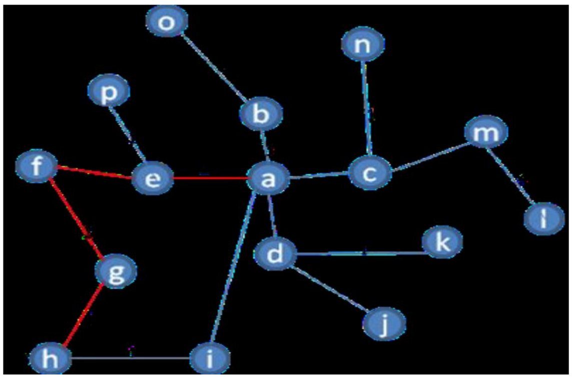

Fig. 5 Minimization of black hole attack

G. Selection of forwarding candidates

The sender and the next hop node will determine the forwarding area. A node in the forwarding area must satisfy the following conditions: 1) it makes positive progress toward the destination; and 2) its distance to the next hop node should not exceed half of the transmission range of a wireless node (i.e., R=2) so that all the forwarding candidates can hear from one another. Based on the destination distance the priority of a forwarding candidate is decided. The nodes that are nearer to the destination will get the highest priority. When a node forwards a packet, the neighbor nodes in the forwarding area from the candidate list is selected as the next hop forwarder. When the index of the node in the candidate list is lower, it gets the highest priority.

H. Secure FSR

The fisheye technique is used to reduce the routing overhead. The name fisheye itself implies, that fish eye has the ability to see objects the better way when they are nearer to its focal point i.e., FSR maintains detailed and accurate information about the nearest nodes then farther nodes and exchange information periodically only with their neighbors. Secure FSR overcomes the packet dropping problem by finding the alternate route and transmission.

IV. VIRTUAL DESTINATION-BASED VOID HANDLING

All the existing mechanisms try to find a route around in case of communication voids. During this process, the greedy forwarding used to go around the hole which is usually worse, so it is not applicable. The robustness of multicast-style routing cannot be exploited. In order to enable opportunistic forwarding in void handling, virtual destination is introduced which acts as a temporary target to which the packets are forwarded. For those communication holes with very strange shape, a reposition scheme has been proposed to smooth the edge of the hole. Given the work that has been done in, VDVH thus still has the potential to deal with all kinds of communication voids.

5) Switch back to greedy forwarding

A fundamental issue in void handling is when and how to switch back to normal greedy forwarding. They are used to guide the direction of packet delivery during void handling. Let us divide the forwarding area in void handling into two parts: A-I and A-II. To prevent the packet from deviating too far from the right direction or even missing the chance to switch back to normal greedy forwarding, the candidates in A-I should be preferred and are thus assigned with a higher priority in relaying. After the packet has been forwarded to route around the communication void more than two hops (including two hops), the forwarder will check whether there is any potential candidate that is able to switch back. If yes, that node will be selected as the next hop, but the mode is still void handling. Only if the receiver finds that its own location is nearer to the real destination than the void node and it gets at least one neighbor that makes positive progress towards the real destination, it will change the forwarding mode back to normal greedy forwarding.

V. CONCLUSION

Our security scheme is proposed to minimize the number of black holes or malicious nodes or selfish nodes in the path to the destination, thus the number of data packet dropping can be minimized, we secured the FSR protocol with security. In case of communication hole, a Virtual Destination-based Void Handling (VDVH) scheme is further proposed to work together with FSR. Thus we proposed a new approach for the reliable data delivery in highly dynamic MANETs and to overcome the limitations of POR. Our proposed Fish Eye routing system checks the packet over heading and provides security in data transmission in highly dynamic networks and also we implemented security in the routing protocol.

REFERENCES

[1] M. Mauve, A. Widmer, and H. Hartenstein, “A Survey on Position-Based Routing in Mobile Ad Hoc Networks,” IEEE Network, vol. 15, no. 6, pp. 30-39, Nov./Dec. 2001.

[2] D. Chen and P. Varshney, “A Survey of Void Handling Techniques for Geographic Routing in Wireless Networks,” IEEE Comm. Surveys and Tutorials, vol. 9, no. 1, pp. 50-67, Jan.-Mar. 2007.

[3] Z. Ye, S. Krishnamurthy, and S. Tripathi, “A Framework for Reliable Routing in Mobile Ad Hoc Networks,” Proc. IEEE INFOCOM, pp. 270-2

[4] K. Zeng, Z. Yang, and W. Lou, “Location-Aided Opportunistic Forwarding in Multirate and Multihop Wireless Networks,” IEEE Trans. Vehicular Technology, vol. 58, no. 6, pp. 3032-3040, July 2009.80, 2003.

[5] D. Chen, J. Deng, and P. Varshney, “Selection of a Forwarding Area for Contention-Based Geographic Forwarding in Wireless Multi-Hop Networks,” IEEE Trans. Vehicular Technology, vol. 56, no. 5, pp. 3111-3122, Sept. 2007.

[6] M. Marina and S. Das, “On-Demand Multipath Distance Vector Routing in Ad Hoc Networks,” Proc. Ninth Int’l Conf. Network Protocols (ICNP ’01), pp. 14-23, Nov. 2001. S. Mueller, R. Tsang, and D. Ghosal,

[7] “Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges,” Performance Tools and

[8] Applications to Networked Systems, pp. 209-234, Springer, 2004.

[9] Michiardi P. and Molva R. (2002) “Simulation-Based Analysis of Security Exposuresin Mobile Ad Hoc Networks,” Proc. European Wireless Conf.

[10] Johnson D. and Maltz D. (1996) “Dynamic Source Routing in Ad Hoc Wireless Networks,”
Mobile Computing, pp. 153-181, chapter 5, Kluwer Academic.

AUTHOR’S PROFILE

Author S.Ganesh is an M.Tech student in Computer science & engineering, Dr.MGR Educational and Research Institute University, Chennai, Tamil Nadu, India.