Secured Transaction Based Routing protocol in Dynamic Mobile Ad hoc Networks

**Publication History**
Received: 23 January 2015
Accepted: 3 March 2015
Published: 1 April 2015

**Citation**
Thamayanthi M, Priya V. Secured Transaction Based Routing protocol in Dynamic Mobile Ad hoc Networks. Discovery, 2015, 30(116), 2-9
Secured Transaction Based Routing protocol in Dynamic Mobile Ad hoc Networks

Thamayanthi.M
St.Joseph’s College of Engineering and Technology,
Thanjavur, India
iamthami@gmail.com

Priya.V
St.Joseph’s College of Engineering and Technology,
Thanjavur, India
spsivapriya5@gmail.com

Abstract—The main aim of this project is concerned with delivering data in secured and timely manner in a dynamic mobile ad hoc networks. Most existing ad hoc routing protocols are susceptible to node mobility, especially for large-scale networks. Geographic routing uses location information to forward data packets, in a hop-by-hop routing fashion. Greedy forwarding is used to select next hop forwarder with the largest positive progress toward the destination. A new Position-based Opportunistic Routing (POR) protocol is proposed. Here the forwarding candidate cache the packet that has been received using MAC interception. If the selected forwarder does not forward the packet in certain time slots, suboptimal candidates will forward the packet in some order. Potential multipath leads to POR’s excellent robustness. Also it proposes a Virtual Destination-based Void Handling (VDVH) in case of handling communication voids.

Keywords—Position based Opportunistic Routing (POR), void handling, geographic routing, MANET.

I. INTRODUCTION

Mobile ad hoc networks, MANET have its significances by multihop and infrastructure less data transmission. High mobility of node make the traditional routing protocols (DSDV, AODV, DSR) susceptible and not suitable for large scale networks. These algorithm require predetermination of end to end routing. Since it is mobile networks, predetermination of end to end are not possible to found. If there is any path breakage, the data either lost or there may be delay at the destination. Geographic information makes use of the location information of the nearby nodes. If the location information is inaccurate then it is not effective.

In Greedy forwarding, the forwarder node is the node far away from the source. Any of the node is out of the coverage range then the node is not reachable and the transmission gets failed. In GPSR, a famous GR protocol MAC failure feedback is send to the to the forwarder node thereby the packet is rerouted and data is received at the destination. General problem in data transmission is that single transmission of packet leads to multiple reception due to interruption, traffic, etc. Location based POR has been proposed now. It directly uses location information for guiding packet forwarding. Like other opportunistic routing protocols, it is designed for static mesh networks and focuses on network throughput. In this paper, a Position-based Opportunistic Routing (POR) protocol is proposed, in which several forwarding candidates cache the packet that has been received using MAC interception. If the best forwarder does not forward the packet in certain time slots, suboptimal candidates will take turn to forward the packet according to a locally formed order. The data transmission will not be interrupted if the candidate succeeds in receiving and forwarding the packets. Duplicate relaying is important fact to be considered in forwarding packets in node mobility and in collision. For this certain scenarios are made and explained in the overview. In the case of communication hole, Virtual Destination-based Void Handling (VDVH) scheme in which the advantages of greedy forwarding and opportunistic routing can be achieved incase of handling communication voids. Finally, we evaluate the performance of POR through extensive simulations and verify that POR achieves excellent performance in high node mobility.

II. POSITION-BASED OPPORTUNISTIC ROUTING

A. Overview

The design of POR is based on geographic routing and opportunistic forwarding. The nodes are assumed to be aware of their own location and the positions of their direct neighbors. Neighborhood location information can be exchanged using one-hop beacon in the data packet’s header. In this scenario, some efficient and reliable way is also available. When a source node wants to transmit a packet, it gets the location of the destination first and then attaches it to the packet header. Due to the destination node’s movement, the multihop path may diverge from the true location of the final destination and a packet would be dropped even if it has already been delivered into the neighborhood of the destination. To deal with such issue, additional check for the destination node is introduced. At each hop, the node that forwards the packet will check its neighbor list to see whether the destination is within its transmission range. If yes, the packet will be directly forwarded to the destination.
In conventional opportunistic forwarding, to have a packet received by multiple candidates, either IP broadcaster an integration of routing and MAC protocol is adopted. The former is susceptible to MAC collision because of the lack of collision avoidance support for broadcast packet in current 802.11. In POR we use similar scheme as the MAC multicast mode. The use of RTS/CTS/DATA/ACK significantly reduces the collision.

and all the nodes within the transmission range of the sender can eavesdrop on the packet successfully with higher probability. The basic routing scenario of POR can be simply illustrated in Fig. 1. In normal situation without link break, the packet is forwarded by the next hop node (e.g., nodes A, E) and the forwarding candidates (e.g., nodes B, C; nodes F, G) will be suppressed (i.e., the same packet in the Packet List will be dropped) by the next hop node’s transmission. In case node A fails to deliver the packet (e.g., node A has moved out and cannot receive the packet), node B, the forwarding candidate with the highest priority, will relay the packet and suppress the lower priority candidate’s forwarding (e.g., node C) as well as node S. For the packet pulled back from the MAC layer, twill not be rerouted as long as node S overhears node B’s forwarding.

B. Selecting forwarding candidates

One of the key problems in POR is the selection and prioritization of forwarding candidates. The forwarding area is determined by the sender and the next hop node. A node located in the forwarding area satisfies the following two 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 ideally all the forwarding candidates can hear from one another. In Fig. 1, the area enclosed by the bold curve is defined as the forwarding area. The nodes in this area, besides node A (i.e., nodes B, C), are potential candidates. The priority of a forwarding candidate is decided by its distance to the destination. The nearer it is to the destination, the higher priority it will get. When a node sends or forwards a packet, it selects the next hop forwarder as well as the forwarding candidates among its neighbors. The next hop and the candidate list comprise the forwarder list. Algorithm 1 shows the procedure to select and prioritize the forwarder list.

Algorithm 1. Candidate Selection
ListN : Neighbor List
ListC : Candidate List, initialized as an empty list
ND : Destination Node
Base : Distance between current node and ND

if find(ListN,ND) then
next_hop⇐ND
return
end if
for i⇐0 to length(ListN) do
ListN[i].dist⇐dist(ListN[i],ND)
end for
ListN.sort()
next_hop⇐ListN[0]
for i⇐1 to length(ListN) do
if dist(ListN[i],ND)>=base or length(ListC)=N then
break
else if dist(ListN[i],ListN[0])<R/2 then
ListC.add(ListN[i])
end if
end for

Every node maintains a forwarding table for the packets of each flow (identified as source-destination pair) that it has sent or forwarded. Before calculating a new forwarder list, it looks up the forwarding table to check if a valid item for that destination is still available. The forwarding table is constructed during data packet transmissions and its maintenance is much easier than a routing table. It depends on the local information and takes less time to construct. Forwarding table records the active flow only.

C. Limitation on Possible Duplicate Relaying

Some forwarding candidates may fail to receive the packet due to the high mobility and collision. If the next forwarding candidate also follows the same, then the propagation area increases with destination as centre and radius can be as large as the distance between the source and the destination. To limit such duplicate relaying, the packet that has been forwarded by the source and the next hop node is transmitted by opportunistic fashion and is allowed to be cached by multiple candidates.

Here instead of allowing the packets to be cached by many candidates, it can be made more effective by forwarding only to the next hop and the very next priority node. Only the source and the next hop node need to calculate the candidate list, while for the packet relayed by a forwarding candidate, the candidate list is empty. The propagation area of a packet is limited to a certain
band between the source and the destination, as illustrated in Fig. 2.

Fig. 2. Duplicate relaying is limited in the region enclosed by the bold curve.

III. MAC MODIFICATION

A. MAC Interception

In the network, some alteration on the packet transmission scenario is made. Just send the packet via unicast, to the best node which is elected by greedy forwarding as the next hop. In this way, we make full utilization of the collision avoidance supported by 802.11 MAC. While on the receiver side, we do some modification of the MAC-layer address filter: even when the data packet’s next hop is not the receiver, it is also delivered to the upper layer but with some hint set in the packet header indicating that this packet is overheard. It is then further processed by POR. Hence, the benefit of both broadcast and unicast (MAC support) can be achieved.

As the location information of the neighbors is updated periodically, some items might become obsolete very quickly especially for nodes with high mobility. This scheme introduces a timely update which enables more packets to be delivered.

B. Interface Queue Inspection

The main point of POR is that when an intermediate node receives a packet with the same ID, having same source and sequence number then it will drop that packet from its packet list. Besides maintaining the packet list, we also check the interface queue.

IV. VIRTUAL DESTINATION-BASED VOID HANDLING

For better POR in void handling special mechanism should be proposed based on virtual destination.

A. Trigger Node

The main thing is which node should forward packet from greedy mode to void handling mode. The change happens at void node mostly. e.g., Node B in Fig. 3. Then, Path 1 (A-B-E---) and Path 2 (A-B-C-F--•) (in some cases, only Path 1 is available if Node C is outside Node B’s transmission range) can be used to route around the communication hole.

From Fig. 3, it is obvious that Path 3 (A-C-F---•) is better than Path 2. If the mode switch is done at Node A, Path 3 will be tried instead of Path 2 while Path 1 still gets the chance to be used. A message called void warning, which is actually the data packet returned from Node B to Node A with some flag set in the packet header, is introduced to trigger the void handling mode. As soon as the void warning is received, Node A (referred to as trigger node) will switch the packet delivery from greedy mode to void handling mode and rechoose better next hops to forward the packet.

B. Virtual Destination

In order to enable opportunistic forwarding in void handling, which means even in dealing with voids, we can still transmit the packet in an opportunistic routing like fashion; virtual destination is introduced, as the temporary target that the packets are forwarded to. Virtual destinations are located at the circumference with the trigger node as center (Fig. 4), but the radius of the circle is set as a value
that is large enough (e.g., the network diameter). They are used to guide the direction of packet delivery during void handling. Compared to the real destination D, a virtual destination (e.g., D0 left and D0 right) has a certain degree of offset in Fig. 4.

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. Fig. 5 shows an example in which VDVH achieves the optimal path of seven hops while GPSR undergoes a much longer route of 15 hops.

1) Switch Back to Greedy Forwarding: A fundamental issue in void handling is when and how to switch back to normal greedy forwarding. From Fig. 4 we can see that the forwarding area in void handling can be divided 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. Therefore, a scaling parameter is introduced for the candidates located in A-II. The progress toward the virtual destination made by these nodes is multiplied by a coefficient \( n(0<n<1) \), called scaling parameter.

2) Path Acknowledgment and Disrupt Message: In VDVH, if a trigger node finds that there are forwarding candidates in both directions, the data flow will be split into two where the two directions will be tried simultaneously around the communication void. Path acknowledgment and reverse suppression are introduced. Once the packet reaches the destination, a path acknowledgment will be sent along the reverse path to inform the trigger node. Then, the trigger node will give up trying the other direction. For the same flow, the path acknowledgment will be periodically sent.

On the other hand, if a packet that is forwarded in void handling mode cannot go any further or the number of hops traversed exceeds a certain threshold but it is still being delivered in void handling mode, a DISRUPT control packet will be sent back to the trigger node as reverse suppression. Once the trigger node receives the message, it will stop trying that direction.

V. MEMORY CONSUMPTION AND DUPLICATE RELAYING

One main concern of POR is its overhead due to opportunistic forwarding, as several copies of a packet need to be cached in the forwarding candidates, leading to more memory consumption, and duplicate relaying would possibly happen if the suppression scheme fails due to node mobility. In memory consumption if a packet is received by a forwarding candidate C, it will be cached for a period of \( \Delta t \) most according to the forwarding scheme. We can get the following upper bound for the length (number of packets cached) of the packet list \( Q_i \) at \( C_i \) for each flow:

\[
Q_i \leq r_i \Delta T
\]

where’s is the packet sending rate at the source of the dataflow. Suppose \( r_s = 100 \) packets/s (which is relatively heavy traffic); since we have set \( T = 0.01 \) s, \( Q_i \) would not exceed, indicating that the opportunistic forwarding scheme used in our protocol will not consume much memory resource.

A. No Forwarding Candidate Is Involved (\( N = 0 \))

In this case there are two possible cases: 1) the packet sent from S is successfully received by C0, so it is forwarded only once; and 2) C0 fails to receive the packet (i.e., it has moved out), then S reselects another next hop for this packet, and thus the packet is forwarded twice at this hop.

B. One Forwarding Candidate Is Involved (\( N = 1 \))

Here the source of duplication is not only S’s rerouting, but also C1’s duplicate relaying due to its moving out (i.e., C1 is no longer within C0’s transmission range but is still within S’s transmission range)

C. Two Forwarding Candidates Are Involved (\( N = 2 \))

When two forwarding candidates are involved, we have to take duplicate relaying into more consideration. Though C1 and C2 will be suppressed by C0 with high probability, in the case that C0 moves out and C1 forwards the packet instead, C2 may not be successfully suppressed (as illustrated in Fig. 6b) since the initialized distance between C1 and C2 can be as far as R and they are much more likely to get separated (i.e., being outside each other’s transmission range).

- Packet delivery ratio: The ratio of the number of data packets received at the destination(s) to the number of data packets sent by the source(s).
• End-to-end delay: The average and the median end-to-end delay are evaluated, together with the cumulative distribution function of the delay.
• Path length: The average end-to-end path length (number of hops) for successful packet delivery.
• Packet forwarding times per hop (FTH): The average number of times a packet is being forwarded from the perspective of routing layer to deliver a data packet over each hop.
• Packet forwarding times per packet (FTP): The average number of times a packet is being forwarded from the perspective of routing layer to deliver a data packet from the source to the destination.

Among the metrics, FTH and FTP are designed to evaluate the amount of duplicate forwarding. For unicast style routing protocols, packet reroute caused by path break accounts for FTH being greater than 1. On the other hand, for those packets who fail to be delivered to the destination(s), the efforts that have already been made in forwarding the packets are still considered in the calculation of FTH, as FTH is calculated as follows:

$$FTP = \frac{N_s + N_f}{\sum_{i=0}^{N_{hi}} N_{hi}}$$

where $$N_s$$, $$N_f$$, and $$N_i$$ are the number of packets sent at the source(s), forwarded at intermediate nodes, and received at the destination(s), respectively. $$N_{hi}$$ is the number of hops for the ith packet that is successfully delivered. FTP averages the total number of times a packet is being forwarded on a per-packet basis:

$$FTP = \frac{N_s + N_f}{N_i}$$

VI. COMMUNICATION HOLE EFFECTIVENESS

To test the effectiveness of VDVH, we further evaluate the routing performance in mobile networks with a communication hole. We create a network topology. The source and destination nodes are fixed at the two ends of the rectangle while the remaining nodes move randomly. The central gray area is simulated as the communication hole with no mobile node distributed. By changing the maximum node speed, we obtain the simulation results. We can observe that in the face of communication hole, GPSR’s void handling mechanism fails to work well. Even when the maximum node speed is 5 m/s, only 90 percent of the data packets get delivered which is relatively poor compared to the other protocols. However, when the node mobility is high (e.g., when the maximum node speed is larger than 25 m/s), POR still performs better. As a summary, POR outperforms AOMDV and GPSR in packet delivery ratio, end-to-end delay, as well as resource (bandwidth) efficiency.

VII. RELATED WORK

Existing robust routing protocols for MANETs can be classified into two categories. One uses the end-to-end redundancy, e.g., multipath routing, while the other leverages on the hop-by-hop redundancy which takes advantage of the broadcast nature of wireless medium and transmits the packets in an opportunistic or cooperative way. Our scheme falls into the second category. Multipath routing, which is typically proposed to increase the reliability of data transmission in wireless ad hoc networks, allows the establishment of multiple paths between the source and the destination.

In the existing protocols, if the failure time exceeds a certain threshold, the guard node who has recently accomplished the forwarding will become the new intended node. A potential problem is that such substitution scheme may lead to suboptimal paths. Unlike RRP, our protocol uses location information to guide the data flow and can always archive near optimal path. On the other hand, our scheme focuses on the route discovery from the perspective of
network layer and no such complex MAC modification is necessary.

VII. CONCLUSION

In this paper, we address the problem of reliable data delivery in highly dynamic mobile ad hoc networks. Constantly changing network topology makes conventional ad hoc routing protocols incapable of providing satisfactory performance. Frequent link break due to node mobility, substantial data packets would either get lost, or experience long latency before restoration of connectivity. Thus MANET routing protocol POR which takes advantage of the stateless property of geographic routing and broadcast nature of wireless medium is proposed. Leveraging on natural backup in the air, broken route can be recovered in a timely manner. Simulation results also confirm the effectiveness and efficiency of POR: high packet delivery ratio is achieved while the delay and duplication are the lowest. Instead of sending the packets to all nearby nodes in POR using hop by hop broadcast scheme, only to two higher priority forwarder makes effective in time and reduces traffic and collision.

A virtual destination-based void handling scheme is proposed. By temporarily adjusting the direction of data flow, the advantage of greedy forwarding as well as the robustness brought about by opportunistic routing can be achieved when handling communication voids. Traditional void handling method performs poorly in mobile environments while VDVH works quite well.

REFERENCES


