SECURE POSITION BASED OPPORTUNISTIC ROUTING FOR HIGHLY DYNAMIC MOBILE AD HOC NETWORKS

Lekshmi M.S, PG Student*

Ms.C.Jeyanthi, Associate Professor*

Abstract

This approach addresses the problem of delivering data packets for highly dynamic mobile ad hoc networks in a reliable and timely manner. Most existing ad hoc routing protocols are susceptible to node mobility, especially for large-scale networks. Driven by this issue, we propose an efficient Position-based Opportunistic Routing (POR) protocol which takes advantage of the stateless property of geographic routing and the broadcast nature of wireless medium. The additional latency incurred by local route recovery is greatly reduced and the duplicate relaying caused by packet reroute is also decreased. In the case of communication hole, a Virtual Destination-based Void Handling (VDVH) scheme is further proposed to work together with POR. Both theoretical analysis and simulation results show that POR achieves excellent performance even under high node mobility with acceptable overhead and the new void handling scheme also works well. Our proposed approach focuses on routing in highly dynamic mobile Adhoc networks, which will focus on reducing delay and routing overhead. To enhance our communication to be efficient one, we propose our Secure Position Opportunistic Routing protocol.

Index Terms—Geographic routing, opportunistic forwarding, reliable data delivery, void handling, mobile ad hoc network.

* **PSN College of Engineering & Technology, Tirunelveli**

INTRODUCTION:

Mobile ad hoc networks (MANETs) have gained a great deal of attention because of its significant advantages brought about by multihop, infrastructure-less transmission. However, due to the error prone wireless channel and the dynamic network topology, reliable data delivery in MANETs, especially in challenged environments with high mobility remains an issue. Traditional topology-based MANET routing protocols (e.g., DSDV, AODV, DSR) are quite susceptible to node mobility. One of the main reasons is due to the predetermination of an end-to-end route before data transmission. Owing to the constantly and even fast changing network topology, it is very difficult to maintain a deterministic route. The discovery and recovery procedures are also time and energy consuming. Once the path breaks, data packets will get lost or be delayed for a long time until the reconstruction of the route, causing transmission interruption. Geographic routing (GR) 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 while void handling mechanism is triggered to route around communication voids. No end-to-end routes need to be maintained, leading to GR's high efficiency and scalability. However, GR is very sensitive to the inaccuracy of location information. In the operation of greedy forwarding, the neighbor which is relatively far away from the sender is chosen as the next hop. If the node moves out of the sender's coverage area, the transmission will fail. In GPSR (a very famous geographic routing protocol), the MAC-layer failure feedback is used to offer the packet another chance to reroute. However, our simulation reveals that it is still incapable of keeping up with the performance when node mobility increases. In fact, due to the broadcast nature of the wireless medium, a single packet transmission will lead to multiple receptions. If such transmission is used as 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. However, most of them use link- state style topology database to select and prioritize the forwarding candidates. In order to acquire the internode loss rates, periodic network-wide measurement is required, which is impractical for mobile environment. The batching used in these protocols also tends to delay packets and is not preferred for many delay sensitive applications. Recently, location-aided opportunistic routing has been proposed which

directly uses location information to guide packet forwarding. However, just like the other opportunistic routing protocols, it is still designed for static mesh networks and focuses on network throughput while the robustness brought upon by opportunistic forwarding has not been well exploited. In this paper, a novel 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. In this way, as long as one of the candidates succeeds in receiving and forwarding the packet, the data transmission will not be interrupted. Potential multipath is exploited on the fly on a per packet basis, leading to POR's excellent robustness.

A position-based opportunistic routing mechanism which can be deployed without complex modification to MAC protocol and achieve multiple reception without losing the benefit of collision avoidance provided by 802.11. The concept of in-the-air backup significantly enhances the robustness of the routing protocol and reduces the latency and duplicate forwarding caused by local route repair. . In the case of communication hole, we propose a Virtual Destination-based Void Handling (VDVH) scheme in which the advantages of greedy forwarding (e.g., large progress per hop) and opportunistic routing can still be achieved while handling communication voids. We analyze the effect of node mobility on packet delivery and explain the improvement brought about by the participation of forwarding candidates. . The overhead of POR with focus on buffer usage and bandwidth consumption due to forwarding candidates' duplicate relaying is also discussed. Through analysis, we conclude that due to the selection of forwarding area and the properly designed duplication limitation scheme, POR's performance gain can be achieved at little overhead cost. . Finally, we evaluate the performance of POR through extensive simulations and verify that POR achieves excellent performance in the face of high node mobility while the overhead is acceptable. This saves the overhead of maintaining unused routes at each node, but on the other hand the latency for sending data packets will considerably increase.

To solve this problem the Secure Position based Opportunistic Routing in Manet has been proposed. All the nodes in an ad hoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighboring nodes. During network initiation all nodes will be strangers to each other. A trust estimator is used in each node to evaluate the trust level of its

neighboring nodes. The trust level is a function of various parameters like length of the association, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, average time taken to respond to a route request etc.

The remainder of this paper is organized as follows: Section 1 reviews related work in the field. Section 2 details the techniques for trust value calculation and a and Section3 contains the simulation results of our work .section 4 concludes our work

I. RELATED WORK

A. Position Based Opportunistic Routing

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 or piggyback in the data packet's header. While for the position of the destination, we assume that a location registration and lookup service which maps node addresses to locations is available. It could be realized using many kinds of location service. For example, the location of the destination could be transmitted by low bit rate but long range radios, which can be implemented as periodic beacon, as well as by replies when requested by the source. 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, similar to the destination location prediction scheme. By performing such identification check before greedy forwarding based on location information, the effect of the path divergence can be very much alleviated. In conventional opportunistic forwarding, to have a packet received by

multiple candidates, either IP broadcast or 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, while the latter requires complex coordination and is not easy to be implemented. In POR, we use similar scheme as the MAC multicast mode. The packet is transmitted as unicast (the best forwarder which makes the largest positive progress toward the destination is set as the next hop) in IP layer and multiple receptions are achieved using MAC interception. 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 due to medium reservation. As the data packets are transmitted in a multicast-like form, each of them is identified with a unique tuple (src_ip, seq_no) where src_ip is the IP address of the source node and seq_no is the corresponding sequence number. Every node maintains a monotonically increasing sequence number, and an ID_Cache to record the ID (src_ip, seq_no) of the packets that have been recently received. If a packet with the same ID is received again, it will be discarded. Otherwise, it will be forwarded at once if the receiver is the next hop, or cached in a Packet List if it is received by a forwarding candidate, or dropped if the receiver is not specified.

The packet in the Packet List will be sent out after waiting for a certain number of time slots or discarded if the same packet is received again during the waiting period (this implicitly means a better forwarder has already carried out the task). 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. By using the feedback from MAC layer, node S will remove node A from the neighbor list and select a new next hop node for the subsequent packets. The packets in the interface queue taking node A as the next hop will be given a second chance to reroute. For the packet pulled back from the MAC layer, it will not be rerouted as long as node S overhears node B's forwarding.

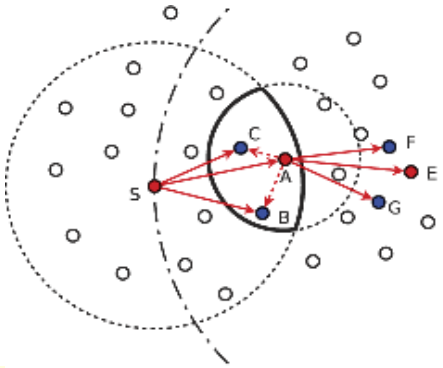

Figure 1: Operation of POR in Normal situation

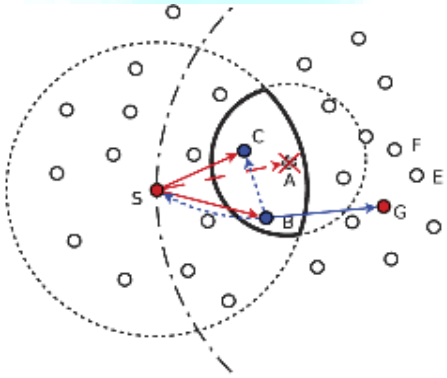

Fig 2: Operation of POR when the next hop fails to receive the packets

>> Selection and Prioritization of Forwarding Candidates

One of the key problems in POR is the selection and prioritization of forwarding candidates. Only the nodes located in the forwarding area would get the chance to be backup nodes. 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

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 Figure 3.1 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. According to the required number of

backup nodes, some (maybe all) of them will be selected as forwarding 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. The candidate list will be attached to the packet header and updated hop by hop. Only the nodes specified in the candidate list will act as forwarding candidates. The lower the index of the node in the candidate list, the higher priority it has.

B. Virtual Destination -Based Void Handling

In order to enhance the robustness of POR in the network where nodes are not uniformly distributed and large holes may exist, a complementary void handling mechanism based on virtual destination is proposed.

The first question is at which node should packet forwarding switch from greedy mode to void handling mode. In many existing geographic routing protocols, the mode change happens at the void node, e.g., Node B in Figure 3 Then, Path 1 (A-B-E-_ _ _) and/or 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 Figure3.2, 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. Of course, if the void node happens to be the source node, packet forwarding mode will be set as void handling at that node without other choice (i.e., in this case, the source node is the trigger node).

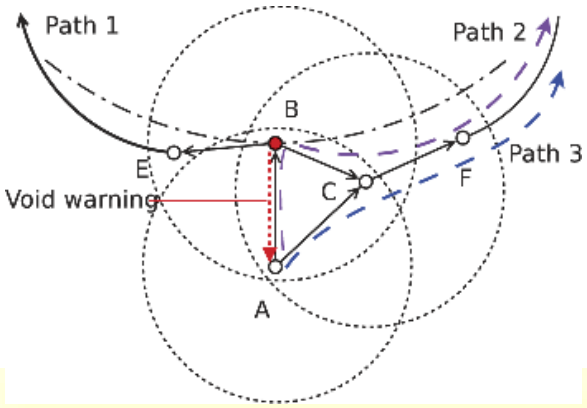

Figure 3: Potential path around the void

>>. *Virtual Destination*

To handle communication voids, almost all existing mechanisms try to find a route around. During the void handling process, the advantage of greedy forwarding cannot be achieved as the path that is used to go around the hole is usually not optimal (e.g., with more hops compared to the possible optimal path). More importantly, the robustness of multicast-style routing cannot be exploited. 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, 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, e.g., _ (_=4 in our simulation). With the help of the virtual destination, the potential forwarding area is significantly extended. Strictly speaking, our mechanism cannot handle all kinds of communication voids, since not all the neighbors of the current node are covered. However, for most situations, it is effective. For those communication holes with very strange shape, a reposition scheme has been proposed to smooth the edge of the hole. VDVH thus still has the potential to deal with all kinds of communication voids. Figure4 shows an example in which VDVH achieves the optimal path of seven hops while GPSR undergoes a much longer route of 15 hops.

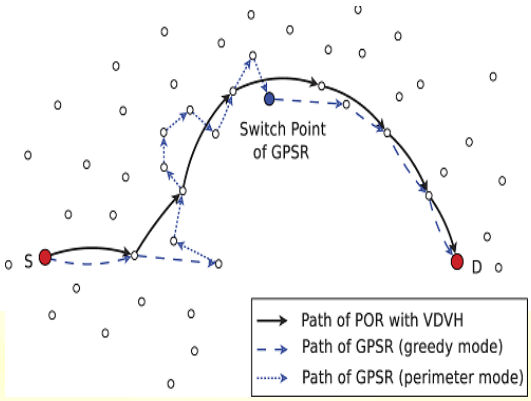

Figure 4: The paths exploited by VDVH and GPSR.

II.SECURE POSITION BASED OPPORTUNISTIC ROUTING PROTOCOL

In order to enhance the performance and for the secure transmission of packets an Opportunistic Routing protocol is used. It should focus on routing in highly dynamic mobile ad hoc networks, which will reduces delay and routing overhead. Security is a major challenge in mobile ad hoc networks due to wireless nature. In our approach the nodes in the forwarding group should also have the possibility to act as a compromised node which will also affect data delivery. To solve this problem the Secure Position based Opportunistic Routing in Manet has been proposed.

All the nodes in an ad hoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighboring nodes. During network initiation all nodes will be strangers to each other. A trust estimator is used in each node to evaluate the trust level of its neighboring nodes. The trust level is a function of various parameters like length of the association, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, average time taken to respond to a route request etc. Accordingly, the neighbors are categorized into friends (most trusted), acquaintances (trusted) and strangers (not trusted).

(i) Node i is a stranger (S) to neighbor node j:

Node i have never sent/received messages to/from node j. Their trust levels between each 1`other will be very low. Any new node entering ad hoc network will be stranger to all its neighbors. There are high chances of malicious behavior from stranger nodes.

(ii) Node i is an acquaintance (A) to neighbor node j:

Node i have sent/received few messages from node j. Their mutual trust level is neither too low nor too high to be reliable. Chances of malicious behavior will have to be observed.

(iii) Node i is a friend (F) to neighbor node j:

Node i sent/received plenty of messages to/from node j. The trust levels between them are reasonably high. Probability of misbehaving nodes may be very less.

Based on these trust relationship the forwarding nodes are selected to forward data.

III.SIMULATION RESULT

The nodes are generated by using random topology, in which nodes are positioned random manner by using Ns2 simulation .It is shown in the figure5.

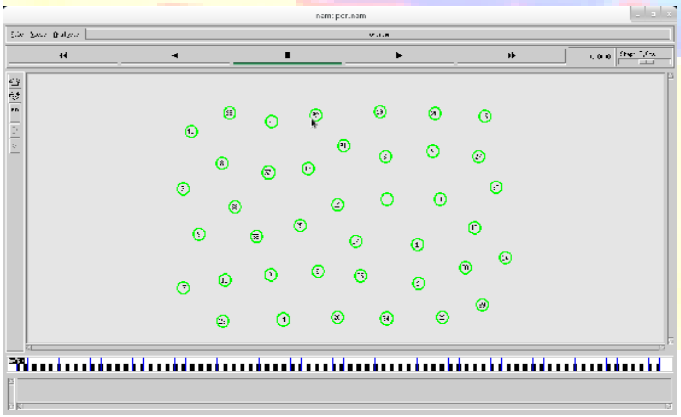

Figure5: Random Topology

IV.CONCLUSION

Presented an Opportunistic Routing Protocol for Highly Dynamic Mobile Adhoc Networks. For the efficient and secure communication a Secure Position Opportunistic Routing protocol is used. The forwarding node should be selected based on the trust level of the neighboring nodes. The trust level is a function of ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor. The nodes are generated by using the random topology. In future we consider, for avoiding frequent link failure, a mobility prediction mechanism will used.

V.REFERENCES

[1] Aristotelis Tsirigos and Zygmunt J. Haas, "Analysis of Multipath Routing, Part 2: Mitigation of the Effects of Frequently Changing Network Topologies," IEEE Trans. Wireless Comm., vol. 3, no. 2, pp. 500- 511, Mar. 2004.

[2] William Navidi and Tracy Camp, "Stationary Distributions for the Random Waypoint Mobility Model," IEEE Trans. Mobile Computing, vol. 3, no. 1, pp. 99-108, Jan.Feb. 2004

[3] Dongjin Son, Ahmed Helmy, and Bhaskar Krishnamachari "The Effect of Mobility Induced Location Errors on Geographic Routing in Mobile Ad Hoc Sensor Networks: Analysis and Improvement Using Mobility Prediction," IEEE Trans. Mobile Computing, vol. 3, no. 3, pp. 233-245, July/Aug. 2004.

[4] A. Valera, W. Seah, and S. Rao, "Improving Protocol Robustness in Ad Hoc Networks through Cooperative Packet Caching and Shortest Multipath Routing," IEEE Trans. Mobile Computing, vol. 4, no. 5, pp. 443-457, Sept./Oct. 2005.

[5] Dazhi Chen, Jing Deng, and Pramod K. 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] Richard J. La, and Yijie Han "Distribution of Path Durations in Mobile Ad Hoc Networks and Path Selection"IEEE ACM Trans on networking, vol. 15, no. 5,oct 2007.

[7] Xiaoxia Huang, Hongqiang Zhai, and Yuguang Fang, "Robust Cooperative Routing Protocol in Mobile Wireless Sensor Networks," IEEE Trans. Wireless Comm., vol. 7, no. 12, pp. 5278-5285, Dec. 2008.

[8] F. Wu, T. Chen, S. Zhong, L.E. Li, and Y.R. Yang, "Incentive- Compatible Opportunistic Routing for Wireless Networks," Proc. ACM MobiCom, pp. 303-314, 2008.

[9] Eric Rozner, Jayesh Seshadri, Yogita Ashok Mehta, and Lili Qiu, "SOAR: Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh Networks," IEEE Trans. Mobile Computing, vol. 8, no. 12, pp. 1622-1635, Dec. 2009.

[10] Noa Arad and Yuval Shavitt, "Minimizing Recovery State in Geographic Ad Hoc Routing," IEEE Trans. Mobile Computing, vol. 8, no. 2, pp. 203-217, Feb. 2009.

[11] Kai Zeng, Zhenyu Yang, and Wenjing Lou, "Location-Aided Opportunistic Forwarding in Multirate and Multihop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 6, pp. 3032-3040, July 2009.

[12] M.-H. Lu, P. Steenkiste, and T. Chen, "Design, Implementation and Evaluation of an Efficient Opportunistic Retransmission Protocol," Proc. ACM MobiCom, pp. 73-84, 2009.

[13] Shengbo Yang, Chai Kiat Yeo, and Bu Sung Lee "Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks," IEEE Trans .mobile computing, vol. 11, no. 1, Jan 2012