Secure Position based Opportunistic Routing for Mobile Ad Hoc Networks

Aju Jacob, Rajeev S.K

Abstract— Mobile Ad Hoc Networks (MANETs), which provide data networking without infrastructure, represent one kind of wireless networks. A MANET is a self-organizing and adaptive wireless network formed by the dynamic gathering of mobile nodes. Due to the mobility of mobile nodes, the topology of a MANET frequently changes and thus results in the disability of originally on-the-fly data transmission routes. The dynamic properties of MANETs are therefore challenging to protocol design. This paper proposes a Position Based Opportunistic Routing Protocol (POR) and Void Handling Based on Virtual Destination (VHVD) which solves the problem of delivering data packets for highly dynamic mobile ad hoc networks in a timely and reliable way. A security scheme is proposed to minimize the number of black holes or malicious nodes or selfish nodes in the path to destination, thus the number of data packet dropping can be minimized. This protocol takes advantage of the stateless property of geographic routing and the broadcast nature of wireless medium. When a data packet is sent out from the source node, some of the neighbor nodes will be the forwarding candidates, and it will forward the packet if it is not forwarded by the best forwarder in a particular period of time. By utilizing such in-the-air backup, communication is maintained without being interrupted.

Index Terms— AODV, Geographic Routing, Mobile ad hoc network, Malicious nodes, Opportunistic forwarding, Reliable data delivery, Void handling.

I. INTRODUCTION

In an ad hoc network [1], mobile nodes communicate with each other using multi hop wireless links without infrastructure. Each node in the network also acts as a router, forwarding data packets for other nodes. A central challenge in the design of ad hoc networks is the development of dynamic routing protocols that can efficiently find routes between two communicating nodes. In MANET [1] nodes moves randomly, therefore the network may experience sudden and unpredictably change in topology. Nodes in MANET normally have limited transmission ranges, therefore some nodes cannot communicate directly to other nodes and those are beyond the limit of range of mobile node. So many protocols have been proposed for MANETs for achieving the efficient routing. Every protocol uses a new searching methodology for new route or modifying a known route, when hosts move. Existing routing protocols such as DSDV, AODV [2] and DSR [3] 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, the data packets will get lost or be delayed for a long time until the reconstruction of the route, causing transmission interruptions. So we utilize Greedy forwarding to select the most suitable neighbour 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 [4].

Geographic Routing (GR) [5] doesn't maintain any prior route information and location information. In the operation of greedy forwarding, the neighbour which is relatively far away from the sender is chosen as the next hop. The transmission may fail, when the node moves out of its source's coverage area. In GPSR [6], 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 [7] [8]. However, most of them uses 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. The batching used in these protocols also tends to delay packets and is not preferred for many delay sensitive applications.

A Position based opportunistic routing strategy was introduced here 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

- *Aju Jacob is currently pursuing masters degree program in Applied Electronics and Instrumentation Engineering in Kerala University, India. E-mail: ajujacob88@gmail.com*
- *Rajeev S.K is the Head of the Electronics and communication department of Younus College Of Engineering & Technology, Kerala, India. He guided Aju Jacob for this work.*

transmit packets. POR's excellent robustness is achieved by exploiting potential multipath on the fly, on a per packet basis. Communication hole is handled by Virtual Destination-based Void Handling (VDVH) scheme [9].

2 POSITION-BASED OPPORTUNISTIC ROUTING

2.1 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 neighbours. 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 multi-hop 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 neighbourhood 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 neighbour list to see whether the destination is within its transmission range. If yes, the packet will be directly forwarded to the destination. In POR, the packet is transmitted as unicast, i.e. the best forwarder which makes the largest positive progress toward the destination is set as the next hop. Multiple reception is achieved using MAC interception. The use of RTS/CTS/DATA/ACK significantly reduces the collision.

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.

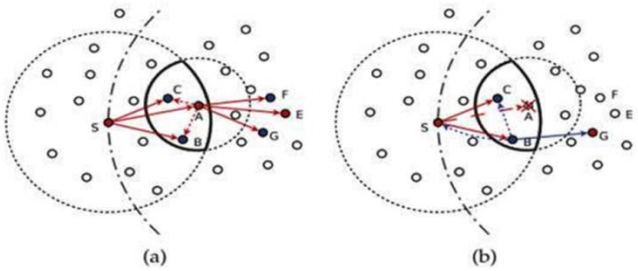


Fig 1: (a) The operation of POR in normal situation. (b) The operation of POR when the next hop fails to receive the packet.

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. By using the feedback from MAC layer, node S will remove node A from the neighbour 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.

2.2 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. 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. According to the required number of backup nodes, some of them will be selected as forwarding candidates

2.3 Giving priority to forwarding candidates

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 neighbour 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. Every node maintains a forwarding table for the packets of each flow 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 the establishment of the forwarding table only depends on local information, it takes much less time to be constructed. Therefore, we can set an expire time on the items maintained to keep the table relatively small.

Due to collision and nodes' movement, some forwarding candidates may fail to receive the packet forwarded by the next hop node or higher priority candidate, so that a certain amount of duplicate relaying would occur. If the forwarding candidate adopts the same forwarding scenario as the next hop node, which means it also calculates

a candidate list, then the propagation area of a packet will cover the entire circle comprising the destination as the centre and the radius can be as large as the distance between the source and the destination. To limit such duplicate relaying, 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. With the use of ID cache, duplicate packets will be dropped soon and would not propagate any further.

3 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.

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 neighbour that makes positive progress towards the real destination, it will change the forwarding mode back to normal greedy forwarding.

4 ACCOUNTING FOR MALICIOUS BEHAVIOUR

There are two types of MANETs: open and closed [10]. An open MANET comprises of different users, having different goals, sharing their resources to achieve global connectivity, as in civilian applications. This is different from closed MANETs where the nodes are all controlled by a common authority, have the same goals, and work toward the benefit of the group as a whole. Open environment of a MANET may lead to misbehaving nodes. Misbehaving nodes come into existence in a network due to several reasons: (a) Mobile hosts lack adequate physical protection (due to the open communication medium), making them prone to be captured and compromised; (b) Usually mobile hosts are resource constrained computing devices. Performing network functions consumes significant energy of participating nodes, as communication is relatively costly.

Non-cooperative actions of misbehaviour are usually termed as selfishness. Selfish nodes are unwilling to spend their precious resources for operations that do not directly benefit them. Selfish nodes use the network for their own communication, but simply refuse to cooperate in forwarding packets for other nodes in order to save battery power. A selfish node would thus utilize the benefits provided by the resources of other nodes, but will not make available its own resources to help others.

4.1 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. 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.

4.2 Solution to minimize black hole attacks

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. Secure POR overcomes the packet dropping problem by finding the alternate route and transmission.

Each node keeps track of neighbours' reliability according to its "personal" experience while transferring data.

Whenever a node communicates with another node in the network, it estimates the reliability of the neighbour node involved in relaying its packets. Specifically, it maintains a table of sent packets, storing also the identity of the next hop that has been charged with forwarding the packet toward the destination. Then its reliability is estimated according to the delivery result. If the source node receives a TCP acknowledgment, then all the intermediate nodes have correctly forwarded the packet, and hence the reliability of the neighbour node is positively updated. Otherwise, some node on the path misbehaved, and the neighbour's reliability decreases. Reliability estimates are useful to choose the best route for packet forwarding. Whenever multiple paths are available, the route with the highest success probability is desired.

5 SIMULATION AND RESULTS

To evaluate the performance of POR, we simulate the algorithm in NS-2.34 and compared it with AODV. The following parameters are used for performance comparison:

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). From Fig.2, it is clear that the Packet delivery ratio of the POR is better with respect to AODV.

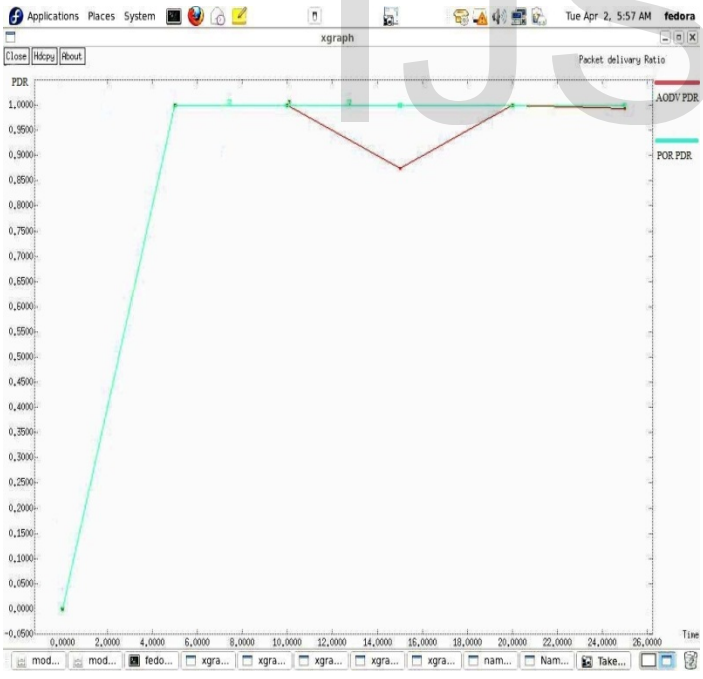


Fig 2: PDR Comparison Graph.

Throughput: is the average rate of successful message delivery over a communication channel. Fig 3 shows POR has high throughput compared to AODV.

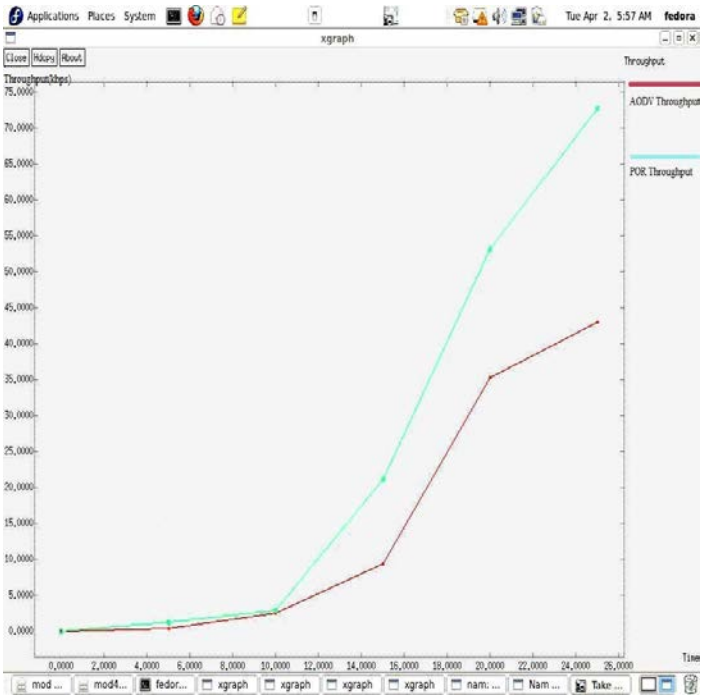


Figure 3: Throughput Comparison Graph

End-to-end delay: The average end-to-end delay is evaluated. POR has lower delay compared with AODV as shown in Fig.4.

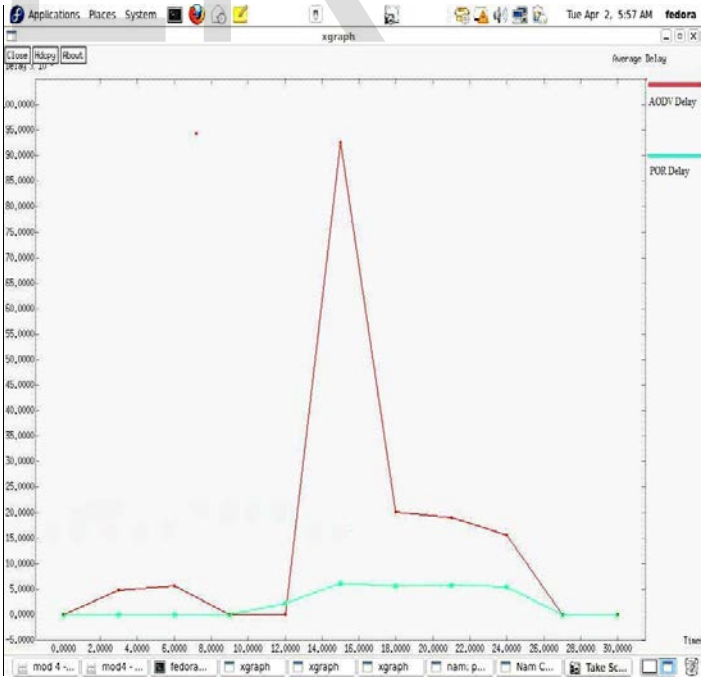
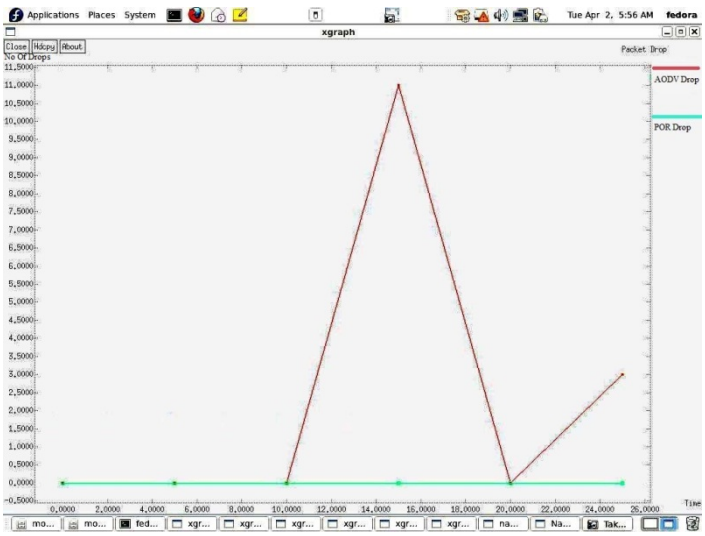


Figure 4: End to End Delay Comparison Graph

Packet Drop: The packet drop of POR and AODV are compared and POR has less packet drop compared to AODV as shown in Fig.5



.

Figure 5: Packet drop Comparison Graph

6 CONCLUSION

In this paper, we proposed a position based opportunistic routing protocol and void handling mechanism based on virtual destination, to solve the problem of reliable data delivery in highly dynamic mobile ad hoc networks. 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 POR protocol with security. In case of communication hole, a Virtual Destination-based Void Handling (VDVH) scheme is further proposed to work together with POR. Through simulation, we further confirm the effectiveness and efficiency of POR; high packet delivery ratio is achieved while the delay and duplication are the lowest.

ACKNOWLEDGMENT

The authors would like to thank the management, and Faculty Members, of Department of Electronics and Communication Engineering, Younus College of Engineering and Technology, Kollam for many insightful discussions and the facilities extended for completing the task.

REFERENCES

[1] J. Macker and S. Corson, "Mobile Ad Hoc Networks (MANET)," IETF WG Charter., http://www.ietf.org/html.charters/manet-charter.html, 1997.

[2] Charles Perkins, "Ad Hoc On Demand Distance Vector (AODV) routing", Internet-Draft, draft-ietf-manet-aodv-00.txt, November 1997.

[3] J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," Proc. ACM MobiCom, pp. 85-97, 1998.

[4] 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.

[5] 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.

[6] B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," Proc. ACM MobiCom, pp. 243- 254, 2000.

[7] S. Biswas and R. Morris, "EXOR: Opportunistic Multi-Hop Routing for Wireless Networks," Proc. ACM SIGCOMM, pp. 133-144, 2005.

[8] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading Structure for Randomness in Wireless Opportunistic Routing," Proc. ACM SIGCOMM, pp. 169-180, 2007.

[9] Shengbo Yang, Chai Kiat Yeo, and Bu Sung Lee, "Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks" IEEE Transactions on Mobile Computing, vol. 11, no. 1, january 2012

[10] H. Miranda and L. Rodrigues, "Preventing Selfishness in Open Mobile Ad Hoc Networks", Proc. of the Seventh CaberNet Radicals Workshop, October 2002.