Secured POR for Flooding Attack Prevention in Extremely Dynamic Ad Hoc Networks

R. Kanaga Sundar*, J. Joe Paul**, M. Krishna Kumar*** & Lissa Laser****

*PG Scholar, Department of Electronics & Communication Engineering, Chandy College of Engineering, Thoothukudi, Tamilnadu, INDIA. E-Mail:kanagasundar@ymail.com
**Assistant Professor, Department of Department of Electronics & Communication Engineering, Chandy College of Engineering, Thoothukudi, Tamilnadu, INDIA. E-Mail: jeanvilavan@gmail.com
***Assistant Professor, Department of Department of Electronics & Communication Engineering, Chandy College of Engineering, Thoothukudi, Tamilnadu, INDIA. E-Mail: krishna18innet@gmail.com
****PG Scholar, Department of Department of Electronics & Communication Engineering, Chandy College of Engineering, Thoothukudi, Tamilnadu, INDIA. E-Mail: lisalaser90@gmail.com

***Abstract*—**To address the problem of flood attacks and communication hole in large scale networks, a Secured Position-based Opportunistic Routing (SPOR) protocol which exploits stateless property of geographic routing as well as the cooperation between the nodes is proposed in this paper. When a data packet is transmitted, the neighbour nodes that have overheard the transmission will serve as forwarding candidates, and take their best efforts to forward the packet if it is not relayed by the specific best forwarder within a certain amount of time. Also a new trust approach based on the extent of friendship between the nodes is proposed which makes the nodes to co-operate and prevent flooding attacks in an ad hoc environment. The problem of communication hole can be greatly reduced using Virtual Destination-based Void Handling (VDVH) scheme working along with POR. The performance of this trust algorithm along with POR achieves excellent performance even under high node mobility with acceptable overhead and the VDVH scheme reduces hole problem.

***Keywords*—**AODV; Flooding; Geographic Routing; MANETs; Mobile Ad Hoc Network; Opportunistic Forwarding; Reliable Data Delivery; Trust Estimation; Void Handling.

***Abbreviations*—**Ad Hoc On-Demand Distant Vector (AODV); Geographic Routing (GR); Mobile Ad Hoc Network (MANET).

I. INTRODUCTION

MANET is gaining momentum because of its infrastructure-less, multihop transmission. Due to its error prone wireless channel and the dynamic network topology, reliable data delivery still remains as an issue in highly varying mobile environments. Long-established topology-based routing protocols such as DSDV, AODV, DSR are quite vulnerable to node mobility [Broch et al., 1998]. The main cause of such vulnerability is predetermining an end-to-end route before data transmission. It is very intricate to sustain a deterministic route in case of highly varying network topology. Moreover the recovery and detection procedures are energy and time consuming. Geographic Routing (GR) utilizes location information for forwarding the data packets in a hop-by-hop routing fashion [Mauve et al., 2001]. Greedy forwarding can be used to pick up the next hop forwarder with the largest positive advancement towards the destination. Void handling mechanism is activated to detect communication voids [Chen & Varshney, 2007]. The location-aided opportunistic routing, which was proposed recently directly uses location information for forwarding the packets [Son et al., 2004]. Anyhow, it still focuses on network throughput rather than exploiting opportunistic forwarding. A novel Position-based Opportunistic Routing (POR) protocol was proposed, in which suppose if the best forwarder does not forward the packets, then the subordinate nodes which will be copying the duplicate message will be forwarding it to the intended recipient [Shengbo Yang et al., 2012]. The Position based Opportunistic routing suggests that some of the neighbour nodes that have overheard the transmission can serve as forwarding candidates, and take turn to forward the packet if it is not relayed by the specific best forwarder within a certain period of time [Shengbo Yang et al., 2012A]. The trust approach suggests a new trust estimator based on the extent of friendship between the nodes which makes the nodes to co-operate and prevent flooding attacks in an ad hoc

environment [Revathi Venkataraman et al., 2000]. By using distributed antennas, we can provide the powerful benefits of space diversity without the need for physical arrays that can be applicable to any wireless setting, including cellular or ad hoc networks [Laneman et al., 2004]. The Multihop Cellular Network (MCN) incorporates the flexibility of ad hoc networks into traditional cellular networks [Chong et al., 2007]. The exact expressions for outage probabilities and outage capacities of three proactive cooperative diversity schemes were derived that select the best relay from a set of relays to forward the information [Woradit et al., 2009]. A distributed relay-selection scheme must have considered other parameters such as power control and application-layer QoS in wireless cooperative networks [Wei et al., 2010]. A Capacity-Optimized COoperative (COCO) topology control scheme considers both upper layer network capacity and physical layer relay selections [Guan et al., 2011]. Fisheye State Routing introduces the notion of multi-level fisheye scope to reduce routing update overhead in large networks [Ganesh, 2013]. The shortage of security features in POR makes them the major concern of interests if deployed in large scale environments. On certain occasions, the malicious node may get involved in a flooding attack by sending unwanted messages to different destinations, making a neighbouring victim node to drain its resources. Our proposal is to add security features in Position based Opportunistic Routing protocol.

The rest of this paper is organized as follows: in Section II, Secured Position Based Opportunistic Protocol is presented. Section III contains Virtual Destination Void Handling Scheme is explained. In Section IV, extensive performance evaluations of Trust algorithm in POR are analyzed. Finally, in Section V, conclusions are given and relevant works done on resisting flooding attacks.

II. POSITION BASED OPPORTUNISTIC ROUTING

The working methodology of POR is centered on geographic routing and opportunistic forwarding. The nodes are well aware of their own location and their neighbour's position. One-hop beacon or piggyback in the data packet's header is exchanged for finding neighbour location. Location registration and lookup service mapping node addresses to locations can be assumed. The location of the destination can be informed by low bit rate, but long range radios, which can be executed as periodic beacon, as well as by replies when requested by the source. When a source node wants to communicate with the destination node, it gets the destination's location first and then attaches itself to the packet header. Because of the movement of the destination node, the multihop path may deviate from its original location of the final destination and a packet would be lost even though it has been delivered to the neighbourhood of destination. During every hop the forwarding node will verify its neighbour list to check whether the destination is within its transmission range. After verifying, the sender node will be transmitting the packet based on the destination location prediction scheme. The problems caused due to path divergence can be avoided by checking the destination before greedy forwarding processes. In traditional opportunistic forwarding, to make a packet received by multiple candidates, either IP broadcast or an integration of routing and MAC protocol is used. The first one is vulnerable to MAC collision due to the lack of collision avoidance, while the latter one needs complex coordination making hard for implementation. We are using a similar scheme like the MAC multicast mode in POR. The best forwarder which is leading than the other nodes towards the destination will be the next hop. Proper usage of RTS/CTS/DATA/ACK can greatly reduce the collision and similarly all the remaining nodes within the transmission range of the sender can eavesdrop on the packet successfully with higher probability due to medium reservation. Each of the packets can be identified by source IP address, and the corresponding sequence number. The packet that waits in the packet list will be sent after a certain resting period or it might get discarded.

2.1. Selection and Prioritization of Forwarding Candidates

Selection and prioritization of the forwarding candidates has always been one of the vital problems in POR. The nodes that are found in the forwarding area will get a chance for taking the backup for nodes. Determining the forwarding area is done by both the sender and the next hop node. Moreover, it has to satisfy the following conditions:

1) The node that makes positive progress toward the destination.

2) The distance to the next hop node must not exceed half of the transmission range of a wireless node (i.e., R=2)

Depending upon the requisite number of backup nodes, some of them can be selected as forwarding candidates. The priority of the forwarding candidate is certain by its distance to the destination. The closer it is to the destination, the higher priority it will get. Every time a node transmits or forwards a packet, it selects the next hop forwarder in addition to the forwarding candidates among its neighbours. The next hop and the applicant list include the forwarder list. The applicant list will be attached to the packet header and updated hop by hop. Only the nodes specified in the candidate list can act as forwarding candidates. The node in the candidate list which has the lower index will be the highest priority node.

2.2. Selection and Prioritization of Forwarding Candidates

All the nodes in the MANET can be categorized as friends, acquaintances or strangers based on their relationships with their neighbouring nodes. All nodes will be strangers to each other during network initiation. To evaluate the trust level of its neighbouring nodes we use the trust estimator in each node.

The trust level will be a function of several parameters like length of the association, ratio of the number of packets forwarded successfully by the neighbour to the total number

of packets sent to that neighbour, ratio of number of packets received intact from the neighbour to the total number of received packets from that node, average time taken to respond to a route request etc. Consequently, the neighbours are classified into friends (most trusted), acquaintances (trusted) and strangers (not trusted).The relationship of a node i to its neighbour node j in a MANET can be any of the following types.

A. Node i being stranger (S) to neighbour node j

If node i has never sent or received messages to or from node j then their trust levels between each other will be very low. Every new node entering an ad hoc network will be a stranger to all its neighbours. There is a high probability for new stranger nodes showing their malicious behaviour.

B. Node i being an acquaintance (A) to neighbour node j

Node i have already sent or received few messages from node j. Their mutual trust level that has been created between the two nodes shall be neither too low nor too high to rely on it.

The likelihoods of malicious behaviour have to be observed.

C. Node i is a friend (F) to neighbour node j

Note i has already sent and received many messages to and from node j. Their relationship shows the trust levels that are reasonably high. The probability of misbehaving nodes might be considerably less. The above relationships are figured by each node and a friendship table is maintained for the neighbours. During route discovery phase of the DSR protocol, the extended system also computes the aggregate trust along different paths to the destination by the "path semiring" algorithm as proposed in Shengbo Yang et al., 2012A.

Based on this, the most trusted path between the source and the destination is found out before establishing the data transfer. The separation of the neighbouring nodes into friends, acquaintances and strangers is the consequence of the direct evaluation of trust. To avoid RREQ flooding, the threshold level can be maintained for the maximum number of RREQ packets a node can receive from its neighbours. The threshold values for DATA flooding can be set as per the requirements of the application software.

III. VIRTUAL DESTINATION BASED VOID HANDLING

For enhancing the sturdiness of POR in the network where nodes are not uniformly distributed as well as large holes might coexist, a corresponding void handling mechanism based on virtual destination is proposed.

3.1. Trigger Node

We have to decide which node should involve in packet forwarding switch from greedy mode to void handling mode. In most of the existing geographic routing protocols, the mode change happens at the void node. As soon as the void warning is received, the trigger node will switch the packet delivery from greedy mode to void handling mode and choose better next hops to forward the packet. Anyhow, if the void node happens to be the source node, packet forwarding mode will be acted as void handling at that node without other selection.

3.2. Virtual Destination

The advantage of greedy forwarding cannot be achieved during the void handling process as the path that is used to go around the hole is usually not optimal. The strength of the multicast-style routing cannot be misused. For enabling the opportunistic forwarding in void handling, which shows that even in dealing with voids, we can still retransmit the packet in an opportunistic routing .Virtual destinations can be located at the circumference with the trigger node as centre ,but the radius of the circle is set at a value that is large enough. They will guide the direction of packet delivery during void handling. By using the virtual destination, the potential forwarding area is significantly extended. Our mechanism cannot handle all kinds of communication voids. However, it is effective in most situations. When the communication hole has a very strange shape, a reposition scheme has been proposed to smooth the edge of the hole. VDVH has the potential to deal with all kinds of communication voids.

3.3. Switching Back to Greedy Forwarding

The most fundamental problem in void handling is when and how to switch back to the normal greedy forwarding. To prevent the deviating packet too far from the right direction or even missing the chance to switch back to normal greedy forwarding, the candidates with a higher priority is relayed. The progress toward the virtual destination made of these nodes is multiplied by a coefficient called scaling parameter which is set as 0.75 in our experiment. As soon as we have forwarded a packet to route around the communication void for more than two hops (including two hops), the forwarder has to check whether there is any potential candidate that is able to switch back. If yes, then that node has to be selected as the next hop, but the mode will be in still void handling. Only if the receiver finds that its position is nearer to the real destination than the void node, then it will change the forwarding mode back to normal greedy forwarding.

IV. SIMULATION ANALYSIS

The simulations are carried out in network simulator (ns-2) & we have to assign the parameters like:

Testing area: 1000m * 1000m

No of nodes: 40r

MAC layer: IEEE 802.11

In this all the nodes were assigned and the hello packets are sent between them, to make them ready for communication purpose. Source node and destination node were initialized first and the router searches the path using

efficient protocol for transmitting data. The throughput ratio for E-POR protocols are simulated here which is shown in fig 1 and it has high throughput ratio compared to other proactive protocols.

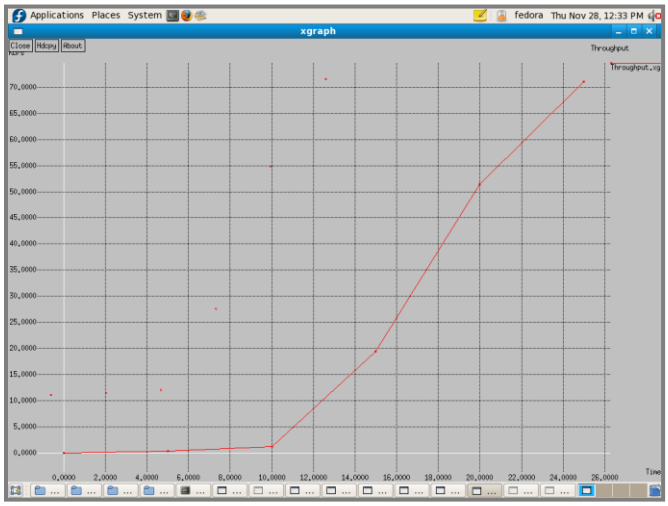

Figure 1: Throughput Ratio

This protocol ensures high packet delivery rate, It is not possible to receive all packets in destination from the source node due to error prone wireless channel, low signal strength etc. , the proposed protocol has efficient packet delivery ratio compared to AODV, AOMDV protocol etc. This concept is shown in fig 2.

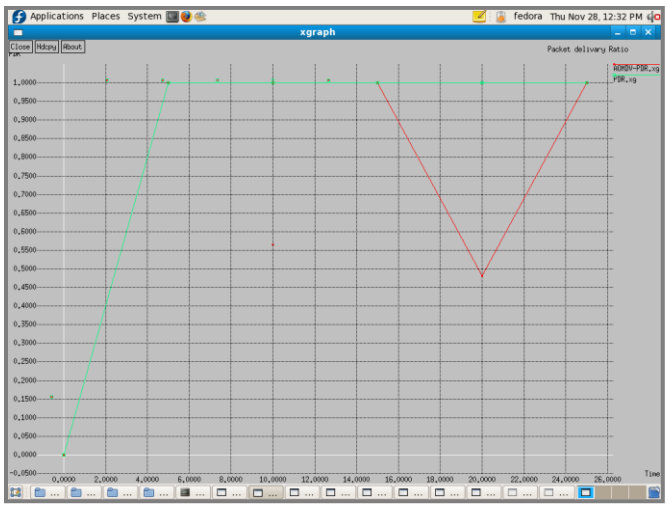

Figure 2: Packet Delivery Ratio

In this figure performance of POR and S-POR protocols is calculated and it is concluded that POR is time consuming and energy consuming. S- POR decreases the packet loss and it is better than the POR, in S-POR packet loss is reduced and duplicate relaying packets also reduces the POR performance. S-POR protocol uses multi-interface for mobile nodes, the nodes that communicate with each other. In less time data packet will be reach at destination. At the same time communication voids can also be avoided and single packet can be delivered to multiple neighbors. The packet loss ratio is shown in fig 3.

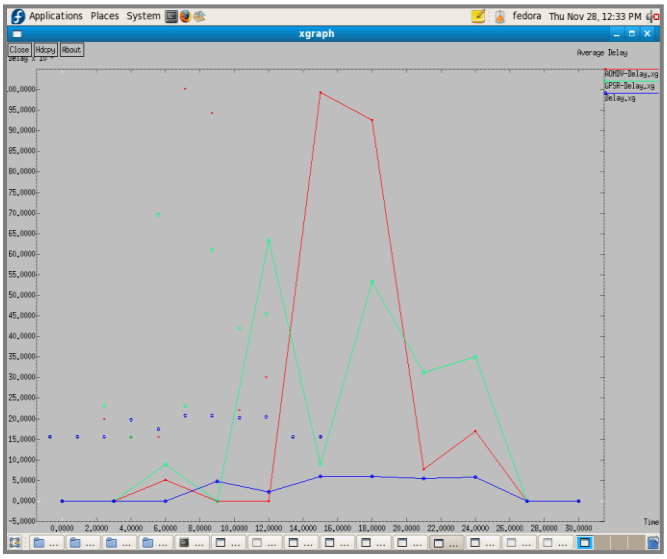

Figure 3: Packet Loss Ratio

V. CONCLUSION

A proposal for effectively preventing flooding attack and hole problem using Secured Position-based Opportunistic Routing (SPOR) for MANET is discussed. In addition with selecting the next hop, several forwarding candidates can also be selected during link breaks. Using such a natural air-backup, broken link routes can be easily recovered in timely manner. Our simulations, further confirm the effectiveness and efficiency of POR: high packet delivery ratio is achieved while the delay and duplication are the lowest. By regulating the direction of data flow and by using the greedy forwarding algorithm brought about by opportunistic routing efficient results can still be achieved while handling communication voids. Along with the opportunistic routing we also address the security issues and trust establishment schemes.

REFERENCES

[1] J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu & J. Jetcheva (1998), "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," *Proceedings of 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Pp. 85–97.

[2] M. Mauve, A. Widmer & H. Hartenstein (2001), "A Survey on Position-based Routing in Mobile Ad Hoc Networks," *IEEE Network*, Vol. 15, No. 6, Pp. 30–39.

[3] D. Chen & P. Varshney (2007), "A Survey of Void Handling Techniques for Geographic Routing in Wireless Networks", *IEEE Communications Surveys and Tutorials*, Vol. 9, No. 1, Pp. 50–67.

[4] D. Son, A. Helmy & B. Krishnamachari (2004), "The Effect of Mobility Induced Location Errors on Geographic Routing in Mobile Ad Hoc Sensor Networks: Analysis and Improvement using Mobility Prediction", *IEEE Transactions on Mobile Computing*, Vol. 3, No. 3, Pp. 233– 245.

[5] Shengbo Yang, Chai Kiat Yeo & Bu Sung Lee (2012), "Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, Vol. 11, No. 1, Pp. 111–124.

[6] Shengbo Yang, Chai Kiat Yeo & Bu Sung Lee (2012A), "Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, Vol. 11, No. 1, Pp. 111–124.

[7] Revathi Venkataraman, M. Pushpalatha & T. Rama Rao (2000), "Performance Analysis of Flooding Attack Prevention Algorithm in MANETs", *World Academy of Science, Engineering and Technology*, Vol. 56, Pp. 458–461.

[8] J. Laneman, D. Tse & G. Wornell (2004), "Cooperative Diversity in Wireless Networks: Efficient protocols and Outage Behavior", *IEEE Transactions on Information Theory*, Vol. 50, No. 12, Pp. 3062–3080.

[9] P.H.J. Chong, Fumiyuki Adachi, S. Hamalainen & V. Leung (2007), "Technologies in Multihop Cellular Network", *IEEE Communications Magazine*, Vol. 45, No. 9, Pp. 64–65.

[10] K. Woradit, T.Q.S. Quek, W. Suwansantisuk, H. Wymeersch, Lunchakorn Wuttisittikulkij & M.Z. Win (2009), "Outage Behaviour of Selective Relaying Schemes", *IEEE Transactions on Wireless Communications*, Vol. 8, No. 8, Pp. 3890–3895.

[11] Y. Wei, F.R. Yu & M. Song (2010), "Distributed Optimal Relay Selection in Wireless Cooperative Networks with Finite-State Markov Channels", *IEEE Transactions on Vehicular Technology*, Vol. 59, Pp. 2149–2158.

[12] Q. Guan, F.R. Yu, Shengming Jiang & V.C.M. Leung (2011), "Capacity-Optimized Topology Control for MANETs with Cooperative Communications", *IEEE Transactions on Wireless Communications*, Vol. 10, Pp. 21.

[13] S. Ganesh (2013), "Reliable Data Delivery in Mobile Ad-Hoc Network using Fisheye State Routing", *International Journal of Computer Trends and Technology*, Vol. 4, No. 2, Pp. 148–152.

R. Kanagasundar got his B.E degree in the field of Electronics & Communication from Mohamad Sathak Engineering College, Kilakarai. He is currently pursuing Master's Degree in the field of Applied Electronics from Chandy college of Engineering, Thoothukudi.

J. Joe Paul got his B.E degree in the field of Electronics & Communication from R.V.S College of Engineering and Technology, Dindigul. He obtained his Master's Degree in the field of Networks Engineering from Kalasalingam University, Srivilliputhur. Presently he is pursuing his career as an Assistant Professor at Chandy College of Engineering, Thoothukudi.

M. Krishna Kumar got his B.E degree in the field of Electronics & Communication from Noorul Islam College of Engineering, Nagercoil. He obtained his Master's Degree in the field of Communication Systems from Mepco Schlenk Engineering College, Sivakasi. Presently he is pursuing his career as an Assistant Professor at Chandy College of Engineering, Thoothukudi. He is a life time Associate Member of IETE. He has published papers in many international journals & conferences.

Lissa Laser got her B.E degree in the field of Electronics & Communication from Dr. G. U Pope Engineering College, Tuticorin. She is currently pursuing Master's Degree in the field of Applied Electronics from Chandy college of Engineering, Thoothukudi**.**