

Security Based Reliable Data Delivery For Dynamic Mobile Ad Hoc Networks

Mr.R.Vinoth Kumar¹

PG Scholar¹

Department of CSE

Anna University Regional centre

Coimbatore, India

Mr.T.Parameshwaran²

Assistant Professor²

Department of CSE

Anna University Regional centre

Coimbatore, India

Abstract - Routing is a challenging task in dynamic topologies. The speed data delivery is the important problem. In a communication on the wireless dynamic network has addressed the problem of data delivery in a reliable and timely manner. The reliable communication is based on node mobility. Due to the reason of large scale network it addresses many problems in network. The Position based Opportunistic Routing (POR) protocol is used in existing, which provides the stateless property of geographic routing and it uses the broadcasting mechanism for data transfer. This protocol is reduced the latency of local route recovery and it is provided forward relay candidates. It is additionally combine together with Virtual Destination based Void Handling (VDVH) scheme, which provides an excellent performance. To improve the performance of reliable routing, the existing approach is added with security mechanism. The Trust based Security mechanism is used. It provides highly reliable data delivery with security in dynamic mobile ad hoc networks.

Index Terms - Geographic Routing, Opportunistic Routing, Reliable data delivery, Void Handling, Trust based Security, Mobile Ad Hoc Network

I. INTRODUCTION

In MANETs, establishing a reliable data delivery is more difficult. Each node in the network is tied on the basis of dynamic topology. Due to the reason of dynamic topology with high mobility nodes, there is many problems occur regarding reliable communication. MANETs has many challenged environments with high mobility nodes. Many protocols are introduced to derive the reliable data delivery in highly dynamic topology. The topology based traditional routing protocols are proposed for node mobility and end-to-end delay of route. The route discovery and data recovery are time and energy consuming in MANETs. Thus it is very difficult to find a route for reliable communication. A long time reconstruction of the route is creating transmission interruption while data delivery.

Geographic routing (GR) uses nodes current location information to forward data packet, in a single hop

routing. Greedy forwarding is used to select the next forwarder node in the network. It is used to find a path for data delivery. Void Handling mechanism is used here. Greedy forwarding is the basic terminology of void handling mechanism. In multicast routing it is difficult to lead multiple receptions. An opportunistic routing is ensuring the transmission with multiple routes backup based on nodes priority. Opportunistic routing is the approach of link-state topology database to select and prioritize the forwarding nodes. The location based opportunistic routing is provides an information to guide packet forwarding. But the position based opportunistic routing is providing information about several forwarding candidates. The packet receiving is using MAC interception with time slots manner. If the best forwarder route does not forward the packet in a particular time slot, the suboptimal candidates is handles the packet delivery in locally formed order based on nodes priority. POR protocol is very efficient for data delivery and highly robust. To improve the performance of the mobile ad hoc network, POR protocol is added with security mechanism. The trust based security mechanism is used to deliver packets with high confidentiality.

II. RELATED WORK

Reliable data delivery is an important factor in MANETs. To increase the robustness of system is commonly reduce the routing overhead of the network. The existing protocol provides some degree of redundancy. The broadcast nature of wireless network is transmits the data packets in a cooperative manner or opportunistic way. It provides the two categories of redundancy in the network. In multipath routing, it uses the end-to-end redundancy and hop-by-hop redundancy. In multipath routing is difficult to gather nodes, which creates communication hole among multiple paths. Existing protocols are widely based on three categories. 1) Using backup paths, 2) packet replication, 3) multipath delivery with reconstruction delivery using coding. This protocol provides high nodes

mobility, when some paths broken and it provides alternate path for reliable communication without failure. It has multiple backup paths for reliable communication in the network and increases the network throughput.

An opportunistic routing is widely increases the cooperative communication of the network. To improve the throughput of the network with security, the trust based security scheme is used as a proposed protocol. These protocols significantly increase the network throughput

III. PROBLEM IN EXISTING SYSTEM

Geographic Routing and Opportunistic Forwarding is used for design POR protocol. In position based routing the nodes are having aware on location information. It has one-hop beacon or piggyback for neighborhood information. The POR protocol is implemented in MAC protocol. It has IP based location broadcasting. In an opportunistic forwarding IP address is integrated with MAC protocol. It creates the communication over the network. In position based routing the complexity of MAC collision is created severe problem against data delivery reliability. It provides VDVH mechanism when communication hole occurs. When communication is broke in the network, it has rearrangements to configure route again. Then it provides exact reliable route in the network from source to destination. It provides high ratio packet delivery and reduce data packet loss rate. It is adoptable in single and multi flow cases. The security is the main issue in this routing problem. It does not ensure the secure data forwarding.

IV. PROPOSED SYSTEM

The proposed system Position based Opportunistic Routing (POR) mechanism is implemented in 802.11 MAC protocol Distributed Coordination function (DCF). In opportunistic route forwarding, the data is transmitted to multiple candidates, which are follows multicast forwarding. In a MAC interception is based on RTS/CTS/DATA/ACK. Initially POR protocol is selecting the nodes in the network. And it is assigns priority based on locations. Based on prioritization it chooses the forwarding candidates for data transfer. It selects the candidates using neighborhood list information. It is a one-hop neighborhood updating on demand routing. It has special limitations with duplicate relaying. The higher priority nodes are taking the responsibilities for opportunistic forwarding. The forwarding candidate has the propagation in radius factor as a circle formation. Then it is integrated with MAC interception. The RTS/CTS/DATA/ACK is specially designed for unicast communication, which can be adapted without any complex modification to MAC protocol and achieve multiple entries without losing the collision avoidance provided by IEEE 802.11. In-the-air backup concept is used here, which is significantly implements the

with security and reliability. POR and Trust based security protocol, is selectively choose a path for communication from source to destination. And it collectively provides the backup path with trust value with neighboring nodes. Each node in the network is choosing its neighbors based on trust value. Based on trust value factor it transmits the packets to its neighbors. Entirely it creates the secure reliable communication in wireless medium.

robustness of the routing protocol and mostly reduces the latency and duplicate data forwarding caused by local route repair among the network. In the case of communication hole occurs in the network it causes data forwarding breakages in the links of the network, for that a Virtual Destination-based Void Handling (VDVH) scheme in which follows the rules and merits of greedy forwarding and position based opportunistic routing can be achieved when handling communication voids. To improve the performance of network with security, the Trust based security mechanism is added with existing protocol. It provides the trust based value based on packet dropping ratio (PDR). The proposed protocol is significantly improves the reliability of the communication with security. The proposed scheme is highly improves the network performance.

V. SYSTEM IMPLEMENTATION

The Network topology formation is done by using MAC layer Distributed Coordination Function (DCF) in IEEE 802.11. Each node in the network should send hello packets to its next neighbor node which are in its communication range for update their topology. The Position-based Opportunistic Routing (POR) protocol has several forwarding candidates among the network links. It has been received using MAC interception in the data link layer. The data forwarding is based on particular time slots position. If the best forwarder node does not forward the packet in particular time slots, sub optimal candidates will take the forwarding work and forward the data packet based on locally formed order. Using this way, the candidates successfully forwarding data packets for a long time and the data transmission will not be destroyed and interrupted.

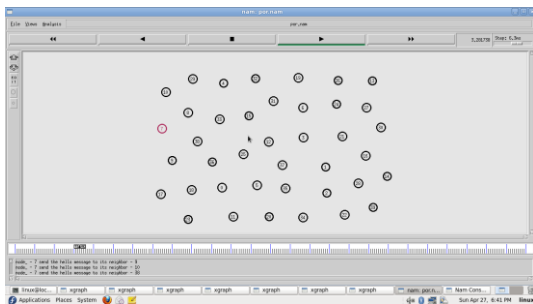
The design of POR is based on geographic routing and opportunistic forwarding. The nodes have the power of location awareness and the positions of their direct neighbors list for data forwarding positions. A one-hop beacon signal or piggyback is used to collect the nodes neighborhood location information, which is positioned in the data packet's header. The location registration and

lookup service which is used to map node addresses to locations is available, when for the position of the destination. It is using different kinds of location service. In this scenario, some efficient and reliable solution is available. For example, the location of the destination can be able to transmit by low bit rate but long range radios, which is implemented as a periodic beacon signal, as well as by replies while requested by the source in the links. When a source node desires to transmit a data packet, it gets the location information of the destination first and then attaches it to the packet header in the data link layer. Due to the reason of destination node's movement, the multi hop path may recognize from the true location of the final destination and a data packet can be dropped even if it has already been delivered to its destination.

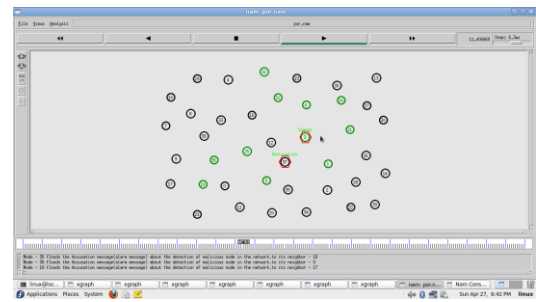
Each node in the network observes the behavior and information of its neighbors. It observes mobility of nodes; number of packets generated and number of nodes forwarded by the neighboring nodes, and listen the past activity of the node. The above parameters are used to determine which nodes are misbehaving in the network. Then, the observer node creates a table called Local Trust Table (LTT) that maintains a local trust value for each neighboring node estimated from these observations in the network communication. It is only using the trust value in LTT and it may not be an accurate measure to conclude that a node is a malicious one. Therefore, each node constructs a Neighbor Trust Table (NTT) in the total network link, which records the trust value for all nodes not only the neighbors but also the far ones. It updates the neighbor node trust value based on Packet Dropping Ratio (PDR). PDR value is calculated by using network threshold value. And it is highly improves the reliable communication with trusted nodes.

VI. RESULTS AND DISCUSSION

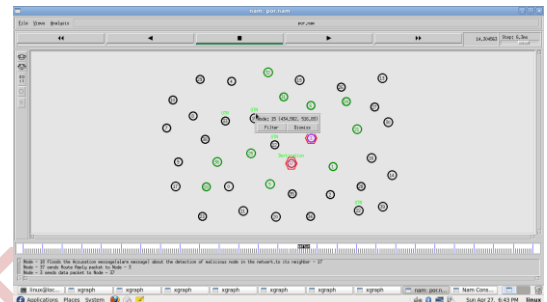
In network topology, nodes are grouped with random movements. And it has perfect neighbor node updates.



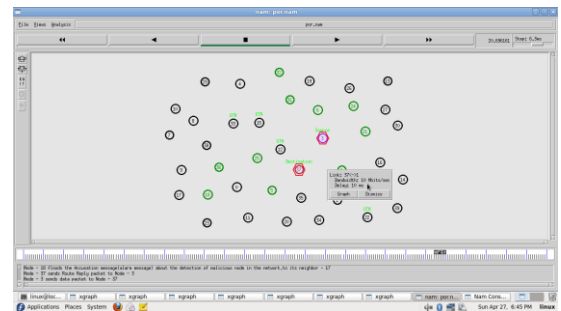
Among the group of nodes, the source and destination node has labeled.



In between the source and destination, the priority is positioned. Based on the nodes priority, the data has been transferred.



The Trust based security scheme is used to neglect the malicious node in the network.



It avoids the malicious nodes actions in the data forwarding time. In between the sender and destination, the nodes transmitting the data through trusted nodes. The trust value is stored in Local Trust Table (LTT). And it updates the neighbor node trust value and it transfers the data securely among the network.

VII. CONCLUSION AND FUTURE WORK

From the simulations, the given results address the problem of reliable data delivery in highly dynamic mobile ad hoc networks. Constantly changing network topology makes conventional problem in ad hoc routing protocols, which causes incapable of providing satisfactory performance. In the face of frequent link breakage due to

node mobility, substantial data packets may get lost, or experience to take longer time latency before restoration of network connectivity. By the use of opportunistic routing, then proposed MANET routing protocol POR with Trust based scheme is takes an advantage of the stateless property of geographic routing and broadcast nature of wireless medium. It selects the route based on broadcasting nature using data dissemination mechanism. It is significantly reduces the packet loss ratio and routing overhead with high security manner. It creates the packet delivery ratio with hop-by-hop and end-to-end redundancy. The proposed protocol is providing effective result than existing approaches.

VII. ACKNOWLEDGEMENT

It's my immense pleasure to thank my Guide and Mentor for his earnest efforts and incessant support throughout my project accomplishment.

REFERENCES

- [1] 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, pp. 111-124, January 2012.
- [2] A. Balasubramanian, R. Mahajan, A. Venkataramani, B.N. Levine, and J. Zahorjan, "Interactive WiFi Connectivity for Moving Vehicles," *Proc. ACM SIGCOMM*, pp. 47-428, 008.
- [3] S. Biswas and R. Morris, "EXOR: Opportunistic Multi-Hop Routing for Wireless Networks," *Proc. ACM SIGCOMM*, pp. 122-144, 2005.
- [4] 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.
- [5] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading Structure for Randomness in Wireless Opportunistic Routing," *Proc. ACM SIGCOMM*, pp. 169-180, 007.
- [6] 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.
- [7] David B. Johnson and David A. Maltz. "Dynamic source routing in ad hoc wireless networks". In *Mobile Computing*, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153-181. Kluwer Academic Publishers, 1996.
- [8] S. Das, H. Pucha, and Y. Hu, "Performance Comparison of Scalable Location Services for Geographic Ad Hoc Routing," *Proc. IEEE INFOCOM*, vol. , pp. 18-129, Mar. 2005.
- [9] Josh Broch David A. Maltz David B. Johnson Yih-Chun Hu and Jorjeta Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols", *Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, October 25-30, 1998,
- [10] B. Karp and H. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proc. of ACM MobiCom*, August 2000.
- [11] Martin Mauve and Jorg Widmer, "A Survey on Position-Based Routing in Mobile Ad Hoc Networks", *IEEE Network*, November/December 2001.
- [12] M. Mauve, J. Widmer, and H. Hartenstein, "A survey on position based routing in mobile ad hoc networks," *IEEE Network*, pp. 30-39, November/December 1999.
- [13] E. Rozner, J. Seshadri, Y. Mehta, and L. Qiu, "SOAR: Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh Networks," *IEEE Trans. Mobile Computing*, vol. 8, no. 1, pp. 16-1625, Dec. 009.
- [14] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading Structure for Randomness in Wireless Opportunistic Routing," *Proc. ACM SIGCOMM*, pp. 169-180, 007