



## GExOR: ExOR Routing Based on GPSR Implementation

Shehsa.A.Shukkoor

Shehsa.A.Shukkoor, M.tech student, Computer Science and Information Systems,  
Federal Institute of Science and Technology, Kerala, India.

---

**Abstract:** *Opportunistic routing has gained attention as it is considered as a promising direction for improving the performance of wireless networks. In opportunistic routing, intermediate nodes collaborate on packet forwarding in a localized and consistent manner. ExOR (Extremely Opportunistic Routing) is a widely used routing protocol in opportunistic networks. It improves routing performance by utilizing opportunistically success over unstable long-range links. The protocol called GExOR (Geographic Extremely Opportunistic Routing) is a combination of routing protocol and media access control for a wireless ad hoc network. The source node broadcasts the packet. Each node can determine its own location and that the source is aware of the location of the destination. With this information a message can be routed to the destination without knowledge of the network topology or a prior route discovery. RSA algorithm is used to provide security to GExOR protocol. The performance results show that GExOR outperforms existing routing protocols.*

**Keywords:** *ExOR, Opportunistic Routing, RSA algorithm, Broadcast Transmission, Wireless network, Adhoc networks.*

---

### 1. Introduction

Wireless networks have gained attention in recent years. Routing packets in wireless networks pose a great challenge because of the unreliability in the wireless links and the interferences in the wireless medium. In traditional wired routing, it will select a best path between the source and destination. Using a fixed neighbor it will forward a packet in each hop. But this strategy does not adapt well in dynamic environment. Traditional routing protocols are unable to operate in situations such as node mobility, node sparseness etc. Opportunistic Network is a network in which nodes may be fixed or mobile. It consists of wireless connected nodes all are within a communication range of 100-300 meters. The network topology may change due to node mobility or node activation and node deactivation. Opportunistic routing takes advantage of the broadcast nature and spatial diversity of the wireless medium. Any node that overhears transmission and is closer to the destination can participate in forwarding the packet. The core difference between traditional routing and opportunistic routing is that in opportunistic routing forwarding nodes can be selected from a group of recipients even after transmission. Since there is no predetermined path opportunistic routing can combine multiple weak links to create a reliable route. The forwarding capability of opportunistic routing reduces retransmission cost and also improves the throughput and energy efficiency. Opportunistic networks are typically wireless networks. Nodes are typically handheld devices carried by people. Nodes communicate directly with each other. They discover each other automatically and do not require any user intervention.

Multihop wireless networks have received great attention in past decade due to its low cost and without relying on existing infrastructure. Designing a protocol in such networks is a challenging issue. Since wireless networks is a time varying channel it is vulnerable to wireless channel propagation effects such as multi path fading there by results in fluctuations in signal strength. The quality of wireless link may change with transmission power, transmission range, path loss between the nodes etc. Since the wireless medium is broadcast in nature, the transmission of one link may interfere with other thereby causing unnecessary interferences. Traditional routing protocols of wireless networks operate like wired routing protocols there by abstracting the wireless links as wired links. These protocols can cope with the consistent behavior of the network. The lossy links in wireless networks may result in poor performance. In a wireless network when a packet is unicast to a specific next-hop node, all the neighbors within the communication range of sender can overhear the transmission. It is also possible that some neighbors received the packet while the next hope node didn't receive it. Opportunistic routing is based on this observation. Opportunistic routing integrates MAC and physical layers. The network layer sets up a list of available candidate nodes and sends it to the MAC layer. The MAC layer makes the final decision according to the node connectivity, channel conditions, reliability, etc. Opportunistic routing is based on broadcast transmission of packets. These transmissions increase the probability that at-least any relaying node receives the packet. In traditional routing source select one of the potential forwarders as next hop. It will send the packet as unicast to its neighbor. But in opportunistic routing source broadcasts the packet, so all of its neighbors will receive it. Amongst one which is closer to destination will again rebroadcast it. Therefore the loss probability associated with opportunistic routing is less as compared to traditional routing. In opportunistic routing even if one of the nodes fails the process continues until packet reaches destination. But it is not the case in traditional routing. Therefore the throughput and reliability in opportunistic routing is high as compared to traditional routing.

## **2. Related Works**

Delivery rate based routing protocols are those protocols in which the forwarding nodes are chosen based on the loss probabilities of the link from source to the destination. In [1] ExOR each node knows the loss rate in every wireless link. The ETX (Expected Transmitted Count) metric was brought into the picture to take into account the effects of lossy, asymmetric links in wireless networks. The source broadcasts the packet. Some subset of nodes will receive the packet. Among these nodes, the node which is closest to destination again broadcasts the packet. This chain continues until the packet reaches destination. In order to reduce communication between the nodes the ExOR protocol operates on batches. A unique batch ID and a forwarder list is selected. The source specifies the forwarder list in priority order based on the expected cost of delivering a packet from each node in the list to the destination. Every packet in a batch contains its sender's snapshot of the network scenario and it is known as batch map. Every receiving node maintains its own snapshot of the network scenario. When a node receives the packet it checks to see whether it is on forwarder list. If so, it checks the batch map. If the packet is not received by higher priority node, it will add the packet to its corresponding buffer. If the batch map indicates that 90% of packets have been sent, then remaining packets are sent through traditional routing.

[2] proposes an efficient Position based Opportunistic Routing(POR).when a data packet is sent out, the neighboring nodes will serve as forwarding candidates and forward the packets within certain period of time. Here the communication is maintained without being interrupted. The protocol can be deployed without complex modification to MAC protocol. If there is any communication hole Virtual Destination Void Handling (VDVH) scheme will perform greedy forwarding and opportunistic routing. In Position based opportunistic routing for robust data delivery in MANETs the location information of nodes can be obtained with GPS like equipment and neighbors coordinates are updated periodically. Before the source node sends packet to the destination node, it calculates the forwarder list according to the distance between neighbors and destination and inserts the list into the packet header. When the packet is sent out, the best forwarder is selected based on priority. The receiving node check its position in forwarder list. If there are n nodes it will wait for n timeslots. It will discard the packet if it is sent by other nodes before the dedicated time slot. The operation continues until the packet reaches the destination. The position based property makes this protocol robust and scalable. Duplicate reception of packets is avoided using an ID record by every node. A forwarding table is used instead of routing table. The protocol also uses a packet list which is used to keep the packet to wait for a certain time before forwarding and it is checked periodically.

[3] Proposes GPSR(Greedy Perimeter Stateless Routing).In GPSR each node keep states from neighbors and these states are used for data forwarding. The state of each node is obtained through GPS devices or others. Source node propagates data with the position of destination node. At first forwarding node performs greedy forwarding. The greedy routing first selects a node which is having shortest path towards destination. Then data is forwarded to the nearest node. There are cases in which nearest node towards destination cannot be found. In such cases forwarding node runs perimeter routing. It is based on planarized graphs such as Relative Neighborhood Graph(RNG) or Gabriel Graph(GG). When each node receives position from neighboring nodes, it makes a unit graph and determines RNG or GG. If greedy forwarding is not possible, it selects a neighboring node by right handed rule and forwards the data. [4]Geographic Random Forwarding is yet another protocol used in opportunistic networks. In GeRaF the source node transmits the packet. All listening nodes in the coverage area will receive the packet and will assess their priority to act as relay based on how close they are to the destination. A mechanism is necessary to determine which one is going to act as the relaying node.

## **3. Proposed System**

### **3.1 Problem Definition**

GExOR is an integrated routing and MAC protocol. It aims to increase the throughput of large unicast transfers in multi hop wireless networks. It is based on cooperative diversity routing. Traditional routing protocols are vulnerable to malicious node attacks. GExOR takes advantage of broadcast nature of wireless networks and opportunistic forwarding. In addition inherited from GPSR and ExOR, GExOR's packet delivery ratio and throughput is better than other protocols. The main objective is to add security to the GExOR protocol and there by protect the wireless network from attacks. RSA algorithm is used to secure the protocol. In this paper we have compared the performance of the routing protocols using the packet delivery ratio, control overhead, hop count, and end-to-end delay.

### **3.2 Geographic Extremely Opportunistic Routing(GExOR)**

The source node broadcasts the packet. GExOR operates on priority queues. In each packet source node includes a list of forwarders which is prioritized by closeness to the destination. Receiving nodes successfully buffer the packets and wait for the end of queue. When a source node S sends a packet to the destination node D, it prioritizes the forwarder list according to the distance between its neighbors and the destination, and inserts the list into the packet header. The neighbor who is nearer to the destination will have higher priority. After that, the packet is sent out, taking the best forwarder as the next hop. All nodes within the sender's one-hop coverage may receive the packet. The receiver checks its position in the forwarder list. Subsequent nodes will do the same operation until the packet reaches the destination. Unlike traditional Internet routing (DV, LS), in GExOR each node keep states from immediate neighbors and uses only those states for data forwarding. The state of each node is obtained from GPS like devices. Before sending the packet the source node S marks each packet with its destination location D and forwards the packet. So the forwarding node can take optimal greedy choice in choosing packet's next hop. The Greedy Forwarding firstly selects a node whose distance to a destination is less than distance from forwarding node to destination and shortest among all immediate neighbors.

Then, data are forwarded to it. There are some topologies in which distance to destination is greater than distance from forwarding node to destination, then greedy forwarding will fail and some other mechanisms must be used to forward packets.

Perimeter Forwarding uses right hand rule for traversing the network. If a network is depicted as a graph, then the rule states that when a packet arrives at a node  $n_1$  from a node  $n_2$ , the next edge traversed is the next one sequentially counter clockwise about  $n_1$  from edge  $(n_1, n_2)$ . The sequence of edges traversed by the right hand rule is known as Perimeter. Planar graphs are those graphs in which two edges will not cross each other. Consider a network with a set of nodes, each node has a radio which is identical and within a circular radio range  $r$  can be seen as a graph. In the graph each node is a vertex and edge  $fg$  exists between nodes  $f$  and  $g$  if the distance between  $f$  and  $g$ ,  $d(f, g) \leq r$ .

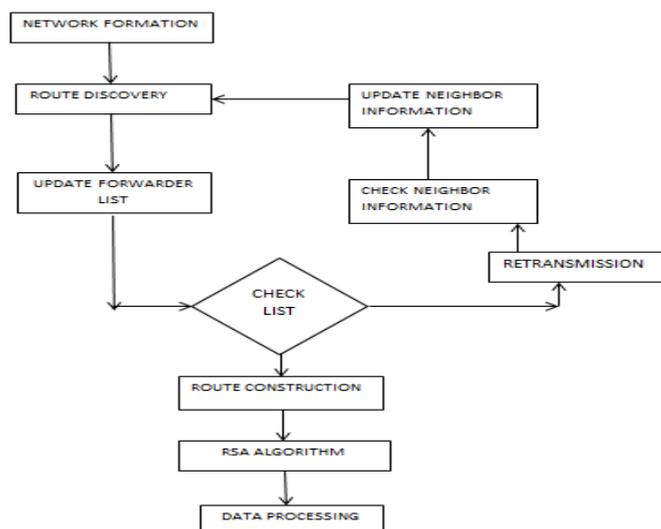
A unit graph is a graph whose edges are represented by a threshold distance between vertices. The perimeter routing is based on planarized graphs such as Relative Neighborhood Graph (RNG) or Gabriel Graph (GG). When each node receives position information from immediate nodes, it initially makes unit graph and then determine RNG or GG. During data forwarding in perimeter mode, if forwarding node run greedy routing, it returns to perimeter mode into greedy mode. RNG can be defined as An edge  $(fg)$  exists between vertices  $f$  and  $g$  if the distance between them,  $d(f, g)$ , is less than or equal to the distance between every other vertex  $h$ , and whichever of  $u$  and  $v$  is farther from  $h$ . GG can be defined as An edge  $fg$  exists between vertices  $f$  and  $g$  if no other vertex  $h$  is present within the circle whose diameter is  $fg$ . By applying RNG or GG, the graph is not disconnected. The edge  $fg$  is eliminated only if an edge  $h$  exists within the range of  $f$  and  $g$ . Each connected component in a network will not be disconnected by removing the edges not in RNG or GG.

Many of the routing protocols in wireless networks has been designed without considering the security aspects. Wireless networks are inherently vulnerable to attacks. The main objective of this paper is to add security to GExOR. To enhance security RSA algorithm is used. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who described the algorithm in 1977. RSA implements a public-key cryptosystem that allows secure communications and digital signatures. In RSA the encryption key is public and decryption key is private. The security rests in the part on the practical difficulty of factoring the product of two large prime numbers.

### 3. System Architecture

Opportunistic Routing protocols broadcast packets to multiple nodes with just one transmission. The receivers of the packet elect one of them as the next forwarder of this packet and others just discard the packet. The source broadcasts the packet. For this it forms the network which consists of set of nodes towards destination. It discovers the routes towards destination. While discovering the routes it also searches for the node which is closer towards destination. The forwarding-based scheme is used. In the forwarding-based approach, there is only single custodian for each message to help forwarding the message to destination. When the current custodian forwards the copy to an appropriate next-hop neighbor, these neighbors becomes the messages new custodian. The process is repeated until the message finally reaches its destination. This approach tries to reduce the buffer usages and the number of message transferred in the network. The nodes which are capable for forwarding are known as forwarding nodes.

Forwarding nodes may create a forwarding list and the nodes in the list may be ordered according to priority. The forwarder list is updated and source periodically checks whether forwarder is present or not. If nodes are not present then the packet is retransmitted. The source again checks the neighboring nodes and updates neighbor information. If the node is available, then the route towards destination is constructed. Among the forwarding candidates that receive the data packet, just one of them should be the relaying node for the current packet. If the receiving node is the higher priority than other nodes then it will process the data. RSA algorithm is used to provide security. It is best known and widely used public-key scheme based on exponentiation in a finite (Galois) field over integers modulo a prime. It uses large integers (eg: 1024 bits). It also provides high security due to cost of factoring large numbers.



3.1 System architecture of GExOR

#### 4. Implementation

To make GExOR robust on a mobile IEEE 802.11 network, the following significant choices are made in the implementation. The choices are:

**Packets are sent in batches:** The source begins by collecting a batch of packets all destined to the same host. The source chooses a unique batchID and selects a forwarder list. The source prepends an GExOR header to each packet of the batch, containing the batch ID and forwarder list. The batch map in each header indicates that the only source has received each packet.

**Planarization of the graph:** Both the RNG and GG planarizations depend on having current position information for a nodes current set of neighbors. Both planarizations are implemented in GExOR protocol. The results presented here use only the RNG. As nodes move, a planarization becomes stale, and less useful for accurate perimeter-mode packet forwarding.

**Integrated MAC and Routing Protocol:** Traditional routing protocols were designed for wired networks. These protocols do not take into account underlying wireless dynamics at MAC and PHY layer. GExOR is an integrated routing and MAC protocol. It routes packets by progressively forwarding them to closer to the sink. This also minimizes protocol overhead.

**Security:** RSA algorithm has been designed to add security to GExOR protocol. It is based on exponentiation in a finite (Galois) field over integers modulo a prime. It provides high security due to cost of factoring large numbers ie factorization takes  $O(e^{\log n \log \log n})$  operations which is very hard.

**Priority Queue:** Priority Queueing (PRIQ) assigns multiple queues to a network interface with each queue being given a priority level. A queue with a higher priority is always processed ahead of a queue with a lower priority. If two or more queues are assigned the same priority then they are processed in a round-robin fashion. We cannot define queues within queues. The root queue sets the total amount of band width available.

#### 5. Performance Evaluation

This section presents experimental results which show that GExOR delivers bulk data faster than traditional routing, for both long and short routes. It also examines some of the individual design decisions in the GExOR protocol, explores the consistency of GExOR's performance and identifies areas for improvement. GExOR is simulated in network simulator (2.29). There are 100 nodes dispersed over 200m X 200m area. GExOR protocol is compared against GPSR protocol on various network parameters. The results show that they achieve high performance, throughput, scalability and reliability.

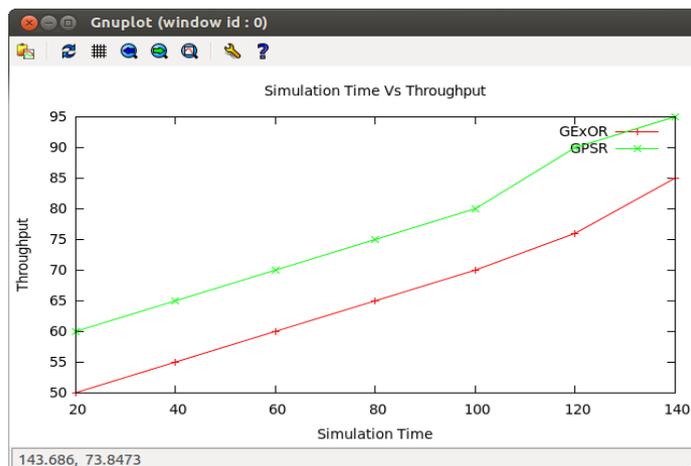


Fig 5.1 Time versus Throughput

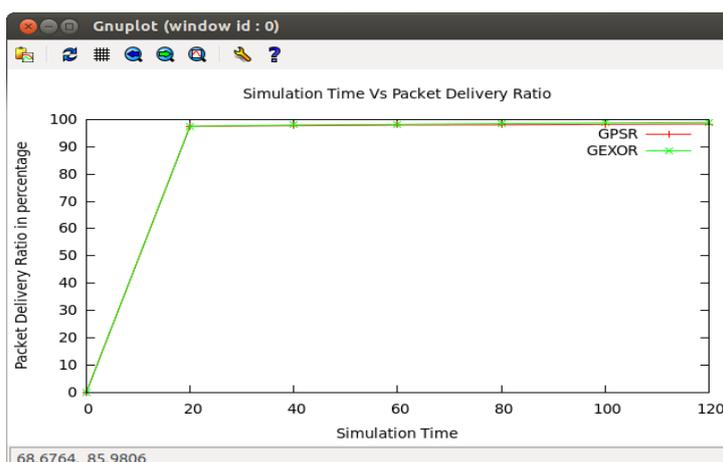


Fig 5.2 Packet delivery ratio versus simulation time

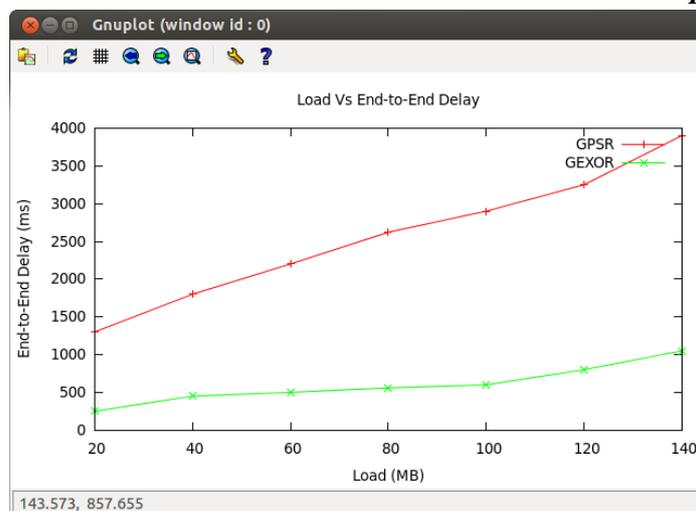


Fig 5.3 Load versus end to end delay

## 6. Conclusion

GEXOR, a routing algorithm that uses geography to achieve small per-node routing state, small routing protocol message complexity, and extremely robust packet delivery on densely deployed wireless networks. The proposed protocol GEXOR, an integrated routing and MAC protocol for multi-hop wireless networks in which the best of multiple receivers forwards each packet. GEXOR improves performance by taking advantage of long-distance but lossy links which would otherwise have been avoided by traditional routing protocols.

## References

- [1] S. Biswas, R. Morris, "Opportunistic Routing in Multi-Hop Wireless Networks", in Proc. of the Conference SIGCOMM, 2005.
- [2] Shengbo Yang, Chai Kiat Yeo, Bu Sung Lee, "Towards Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks"
- [3] Brad Karp, H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks"
- [4] M. Zorzi, R. R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks: energy and latency performance", IEEE Transactions on Mobile Computing, vol. 2, Issue 4, October 2003.
- [5] Zehua Wang, Yuanzhu Chen, Cheng Li, "CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks", IEEE Journal On Selected Areas In Communications, VOL. 30, NO. 2, February 2012.
- [6] A. Trivio-Cabrera, S. Caadas-Hurtado, "Survey on Opportunistic Routing in Multihop Wireless Networks", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 3, No. 2, August 2011.
- [7] Chung-Ming Huang, Kun-chan Lan and Chang-Zhou Tsai, "A Survey of Opportunistic Networks" 22nd International Conference on Advanced Information Networking and Applications - Workshops.