# Fault Tolerant Greedy Perimeter Stateless Routing in Wireless Network

Jyotsana Jaiswal
National Institute of Technology Rourkela
Rourkela, Odisha, India
jyotsanaa.jaiswal@gmail.com

Pabitra Mohan Khilar
National Institute of Technology Rourkela
Rourkela, Odisha, India
pmkhilar@nitrkl.ac.in

## ABSTRACT

Routing in wireless network is a key research area. This paper proposes a fault tolerant greedy perimeter stateless routing protocol (FGPSR) suitable for wireless network with minimal routing overhead. FGPSR has four main phases-Fault testing, Planarization, Greedy forwarding and Perimeter forwarding. First, fault testing phase provides all nodes with their fault free neighbour positions periodically. The next phase, planarization is a prerequisite process for perimeter forwarding phase which removes crossing edges. Routing starts with Greedy forwarding, each node forwards packets to the neighbour which minimizes the distance to the destination in each step. Greedy forwarding can lead into a dead end or void, where there is no neighbour closer to the destination. In that case perimeter forwarding helps to recover and finds a path to another node, where greedy forwarding can resume. The probability of finding a route between source destination node pairs is very high. FGPSR establishes fault free paths between various wireless node pairs. The protocol has been analyzed and validated through simulation. The result shows that the number of path established in FGPSR are more than GPSR.

## Categories and Subject Descriptors

C.2.2 [**Computer-Communication Networks**]: Network Protocols—*Routing protocols*; C.4 [**Performance of Systems**]: *Fault tolerance.*

## General Terms

Experimentation.

## Keywords

Wireless Network, Geographic Routing, Fault tolerance, GPSR, Planarization.

## 1. INTRODUCTION


*ICCCS'11* February 12-14, 2011, Rourkela, Odisha, India


Routing in wireless networks is a key research area since last three decades. Routing establishes paths between different wireless connected nodes. Since last few decades, Geographic routing (GR) has gained significant attention for wireless networks. The major advantage of GR over classical approaches is that each node only needs to know the location of itself and its neighbours. Thus, only a small amount of routing state is required at each node for its functioning. However in traditional routing protocols for wireless networks (e.g. AODV [7], DSDV [8]), nodes usually have to keep significant amount of routing information. In geographic routing, each node is identified by a set of coordinates and packets are forwarded greedily, i.e., each node picks as next hop the neighbour that is closest to the destination in the coordinate space. The geographic coordinates for each nodes are obtained using special devices such as GPS. However, GR itself suffers from few feedback. Firstly, greedy routing over geographic cordinates may not be optimal due to unawareness of connectivity information of the underlying network. Secondly message may get stuck in local minimum condition (a node does not have neighbor closer to the destination) for sparse networks. To deal with above stated local minimum problem, perimeter routing can be used which route around the perimeter of a face in a planar sub graph of the network until greedy routing can be resumed. The probability of finding a route between source destination node pairs is very high, provided the nodes are aware of own locations and there is a distributed algorithm to compute a connected planar sub graph of the network.

The routers used in wireless networks are subjected to various kind of faults such as crash fault, transient fault etc. The occurrence of faults affects the routing process. Fault diagnosis is of increasing importance in applications where it is critical to maintain flawless routing. In routing when fault tolerance is applied it helps in controlling the overhead which is there due to faulty node and thus helps in considering the reliable routes. The paper is organized as follows: The introduction is addressed in Section 1. The background and related works are summarized in Section 2. The proposed protocol design is discussed in detail in Section 3. The performance of our network protocol is evaluated in Section 4. The conclusion is presented in Section 5.

## 2. BACKGROUND AND RELATED WORK

Fault tolerant routing is an important area of research. The authors, Xue and Nahrstedt [9] proposed the popular end-to-end estimation based fault-tolerant routing algorithm $E^2FT$. The authors, Oommen and Misra also proposed a

weak-estimation based learning approach for assessing better routing paths. Additionally, the foraging behavior of swarms of naturally occurring ants has inspired researchers to solve different complex engineering problems. It has given rise to the theory of ant colony optimization(ACO) [4]. ACO has been used in the past to solve different network routing problems e.g., AntNet [3], ARA [2]. Even with the complete knowledge of faulty nodes, the fault-tolerant routing problem can be formulated as a packet delivery rate constrained, overhead-optimization problem. The authors, Xue and Nahrstedt [9] proved the designing of an effective and efficient fault-tolerant routing algorithm as NP-complete.

An ordered classification of fault is given below: 1. Fail-Stop Fault, 2. Crash Fault, 3. Omission Fault, 4. Timing Fault, 5. Incorrect Computation Fault and 6. Byzantine Fault. Though, a number of geographic routing protocols exists in the literature, none of them have addressed the fault tolerance issue in their protocols [6]. In this work, a fault tolerant geographic routing protocol has been proposed.

# 3. MODELING AND PROPOSED PROTOCOL

## 3.1 System Model and Fault Model

### *3.1.1 System Model*

The system is composed of $n$ hosts (nodes), with unique identifiers that communicate via a packet radio network. The assumption has been made that the entire nodes have similar computing and storage resources. A set of nodes with circular radio range $r$, can be seen as a graph: each node is a vertex, and edge $(n, m)$ exists between nodes $n$ and $m$ if the distance between $n$ and $m$, $d(n, m) \leq r$. Graphs whose edges are dictated by a threshold distance between vertices are termed unit disk graphs. The transmission range of each node is assumed to be 250 meters. The nodes are initially placed uniformly at random in a rectangular region 1000×1000 and the number of nodes considered are 50. 20 connection are taken at a time. The topology of the multihop packet radio network can be described by a directed graph $G_t = (V, L_t)$, where $V$ is the set of mobiles and $L_t$ is the set of logical links. Finally, the sources can determine the approximate locations of destinations, to mark packets they originate with their destination's location.

### *3.1.2 Fault Model*

Each node in the wireless networks can be in one of two states: faulty or fault-free. Faults are permanent, i.e. a faulty node remains faulty until it is repaired and/or replaced. Faults can be either hard or soft. When a unit is hard-faulted, it is unable to communicate with the rest of the system. In a wireless network, a unit can be hard-faulted either because it is crashed or due to battery depletion. Soft faults are subtle, since a soft-faulted node continues to operate and to communicate with the other node in the system although with altered specifications i.e., the faulty nodes may produce some random results instead of expected results. In this work, both hard-faulted and soft-faulted nodes in static wireless networks has been considered.

The proposed routing protocol uses the testing model given in Table 1. As shown in the test model, five cases are observed. First case, the status of the tester node and tested node are both fault free then test result is zero. This means that there is match between the expected result of the tester node and the actual result returned by the tested node. Second case, the tester node is fault free and the tested node is soft faulty then test result is 1. This means there is a mismatch between the expected result and actual result. Third case, the tester node is fault free or soft faulty and the tested node is hard faulty then test result is NULL because a hard faulty node can receive a beacon test message but cannot send reply to it. Fourth case, the tester node is soft faulty and tested node is soft faulty or fault free then test result is 1. Here also there is mismatch between the expected result and actual result. Fifth case, the tester node is hard faulty and tested node is also faulty (soft or hard) or fault free then test result is NULL because a hard faulty node cannot send a beacon test message.

When the test result is 0, the node is considered as fault free, otherwise faulty. The test model given in Table 1 is used to select fault free nodes while establishing the paths between the nodes pair.

**Table 1: Test model**

| Status of Tester node | Status of Tested node | Test Result |
|---|---|---|
| Fault free | Fault free | 0 |
| Fault free | Soft faulty | 1 |
| Fault free | Hard faulty | NULL |
| Soft faulty | Hard faulty | NULL |
| Soft faulty | Soft faulty | 1 |
| Soft faulty | Fault free | 1 |
| Hard faulty | Soft faulty | NULL |
| Hard faulty | Hard faulty | NULL |
| Hard faulty | Fault free | NULL |

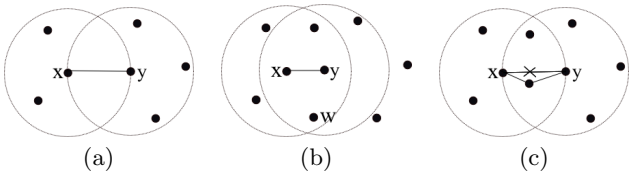


**Figure 1: The RNG graph: (a) Edge exit between (x,y), (b) Edge exist between (x,y) and (c) Alternate path exist between (x,y)**

## 3.2 Fault Testing Phase

A fault testing phase provides all nodes with their fault free neighbours' positions periodically. Each tester node transmits a beacon-test message to the broadcast MAC address containing its own identifier (e.g. IP address), position and test task. Each tester node knows the result of the test task. When the neighbouring node receives the beacon-test message they unicast the reply message. The reply message contains the result of the test task, their own IP address and position. In this phase, each tester node checks whether the neighbouring nodes present are fault free or faulty (i.e., soft or hard) by comparing the result of test task using the test model given in Table 1. In this phase each node maintains the location of all fault free nodes in their range. After this planarization phase starts.

## 3.3 Planarization Phase

Planarization is a prerequisite process for FGPSR as the right-hand rule does not work properly on full connected graphs with crossing edge. The right hand rule is an important part of perimeter forwarding phase. The planarization algorithm should run in a distributed fashion by each node in the network. The Relative Neighbourhood Graph (RNG) and Gabriel Graph (GG) are two planar graph known since long in varied disciplines [1]. An algorithm for removing edges from the graph that are not part of the RNG or GG would yield a network with no crossing links. RNG planarization has been considered in this paper. One important property to be taken care during this phase is that removing edges from the graph to reduce it to the RNG must not disconnect the graph. Figure 1 shows the rule for constructing the RNG for various cases: a) An edge $(x, y)$ exists if there is no existent node(s) present in the intersection of transmission range of both nodes $x$ and $y$. b) An edge $(x, y)$ exists between nodes $x$ and $y$ if the distance between them, $d(x, y)$ is less than or equal to the distance between every other node(s) $w$ as shown in Figure 1 (b). In equation form:

$$\forall w \neq u, v : d(x, y) \leq [d(x, w) + d(y, w)] \quad (1)$$

c) An edge $(x, y)$ is only eliminated from the graph when there exist node(s) in the intersection of transmission range of $x$ and $y$, and the distance between them, $d(x, y)$ is greater than the distance between every other node. Then an alternate path through a nearest node is constructed between $x$ and $y$ that exist in the intersection of range $x$ and $y$.

## 3.4 Greedy Forwarding Phase

After planarization phase all nodes maintain two neighbouring tables. First table (also known as original table) stores address and location of original neighbours based on transmission range which is used by greedy forwarding phase. Second table (also known as planarized table) stores the address and locations of the single hop transmission range neighbours based on planarization which is used by perimeter forwarding phase. In FGPSR, source node knows their destination's location. As a result, a forwarding node uses first neighbour table in choosing next hop. The locally optimal choice of next hop is the neighbour geographically closest to the destination. Forwarding in this manner follows successively closer geographic hops, until the destination is reached. An example of greedy next-hop choice is shown in Figure 2 (a). The greedy forwarding comes with one attendant drawback. A simple example of such a topology is shown in Figure 2 (b). Here, $a$ is closer to $e$ than all its neighbours. Though a path $(a \rightarrow b \rightarrow c \rightarrow d \rightarrow e)$ exists to e but $a$ will not choose to forward to $e$ using greedy forwarding because $a$ is local minimum in its proximity to e. Therefore, perimeter forwarding mechanism must be used to forward packets in this situations.

## 3.5 Perimeter Forwarding

Perimeter forwarding uses right hand rule as described below:

### 3.5.1 *Right Hand Rule*

The right-hand rule for traversing a graph is shown in Figure 3 (a). This rule states that when arriving at node $b$ from node $a$, the next edge traversed is the next one sequentially counterclockwise about $b$ from edge $(a, b)$. On graphs with

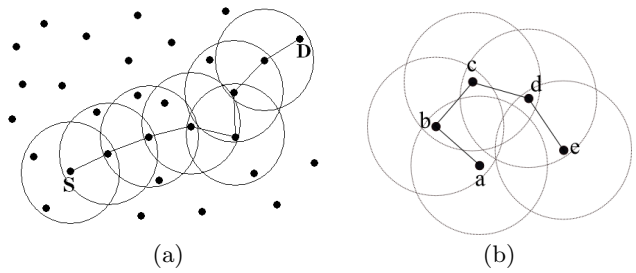


**Figure 2: (a) Greedy forwarding and (b) Local minima condition**

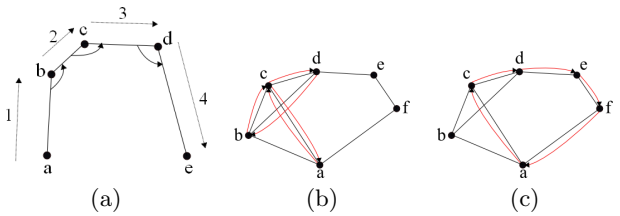


**Figure 3: (a) Right Hand Rule (RHR), (b) RHR with crossing edge, (c) RHR without crossing edge**

edges that cross, the right-hand rule may take a degenerate tour of edges that does not trace the correct path as shown in figure 3 (b). Now on removing the crossing edges right hand rule traces the correct path (Figure 3 (c)). In this context planarization comes into picture.

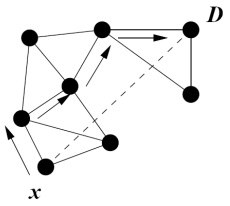


**Figure 4: Perimeter forwarding example**

### 3.5.2 *Perimeter Forwarding*

FGPSR combines fault testing phase, greedy forwarding phase on the full network graph and perimeter forwarding phase on the planarized network graph where greedy forwarding fails. The packet header fields used in FGPSR for perimeter-mode forwarding is shown in Table 2. FGPSR packet headers include a flag field indicating whether the packet is in greedy mode or perimeter mode. All data packets are marked initially at their source as greedy-mode. Upon receiving a greedy-mode packet for forwarding, a node searches its original neighbour table for the neighbour that is geographically closest to the destination and forwards the packet to that neighbour. When no neighbour is closer, the node marks the packet into perimeter mode.

FGPSR forwards perimeter-mode packets using planarized table. As shown in figure 4 when a packet enters perimeter mode at node $x$ bound for node D, the first node for perimeter forwarding is chosen by the following process. First, the line is projected from $x$ to all neighbors present in planarized table. Second, angle is measured between positive

**Table 2: FGPSR packet header fields used in perimeter mode forwarding (adapted from [5])**

| Field | Function |
|---|---|
| D | Destination Location |
| $L_p$ | Location Packet Entered Perimeter Mode |
| $L_f$ | Point on $\overline{xD}$ Packet Entered Current Face |
| $e_0$ | First Edge Traversed on Current Face |
| M | Packet Mode: Greedy or Perimeter |

$x$ axis taking node $x$ as origin and the lines projected to all the neighbours. Then that neighbour is chosen which makes a minimum angle with positive axis in counterclockwise direction with node $x$. FGPSR forwards the packet on progressively closer faces of the planar graph, each of which is crossed by the line $\overline{xD}$. On each face, the traversal uses the right-hand rule to reach an edge that crosses line $\overline{xD}$. At that edge, the traversal moves to the adjacent face crossed by $\overline{xD}$ as depicted in Figure 4. When a packet enters perimeter mode, FGPSR records in the packet the location $L_p$, the site where greedy forwarding failed. This location is used at subsequent hops to determine whether the packet can be returned to greedy mode. Each time FGPSR forwards a packet onto a new face, it records in $L_f$ the point on $\overline{xD}$ shared between the previous and new faces. Finally, FGPSR records $e_0$, the first edge a packet crosses on a new face, in the packet. Upon receiving a perimeter-mode packet for forwarding, FGPSR first compares the location $L_p$ in a perimeter-mode packet with the forwarding nodes location. FGPSR returns a packet to greedy mode if the distance from the forwarding node or its original table neighbours to D is less than that from $L_p$ to D. Perimeter forwarding is only intended to recover from a local minima; once the packet reaches a location closer than where greedy forwarding previously failed for that packet, the packet can continue greedy progress toward the destination. There are two cases to consider: either x and D are connected by the graph, or they are not. When x and D are connected by the graph, traversing the face bordering x in counterclockwise direction must lead to a point y at which $\overline{xD}$ intersects the far side of the face and reaches the destination D. When D is not reachable, FGPSR notices the repetition of forwarding on the edge $e_0$ stored in the packet, and correctly drops the packet, as the destination is unreachable.

# 4. SIMULATIONS AND RESULTS

Figure 5 shows the simulation result for the 1000×1000-sized networks of node 50. For traffic source 20 traffic flow originated by 20 sending nodes has been considered. As shown in fig 5, FGPSR provides higher number of path between source and destination out of the total number of path (i.e., 20) than GPSR due to the fact that GPSR does not check the faulty node which causes long detouring paths and sometime may not establish path to the destination.

# 5. CONCLUSIONS

In this paper, fault tolerant GPSR routing algorithm has been proposed. FGPSR and GPSR have been simulated for the 1000×1000-sized static networks of 50 node. 20 traffic flow originated by 20 sending nodes has been considered. The result carried out shows that FGPSR provides higher

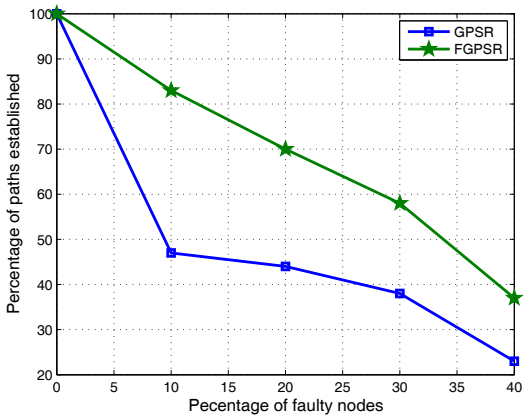


**Figure 5: GPSR vs FGPSR**

no. of path between source and destination out of the total no. of paths (i.e., 20) than GPSR due to the fact that GPSR does not check the faulty node which causes long detouring paths and may not establish path to the destination.

# 6. REFERENCES


[1] P. K. Agarwal and J. Matauˇsek. Relative neighborhood graphs in three dimensions. In *SODA '92: Proceedings of the third annual ACM-SIAM symposium on Discrete algorithms*, pages 58–65, Philadelphia, PA, USA, 1992. Society for Industrial and Applied Mathematics.

[2] I. Bouazizi. Ara - the ant-colony based routing algorithm for manets. In *ICPPW '02: Proceedings of the 2002 International Conference on Parallel Processing Workshops*, page 79, Washington, DC, USA, 2002. IEEE Computer Society.

[3] G. Di Caro and M. Dorigo. Antnet: distributed stigmergetic control for communications networks. *J. Artif. Int. Res.*, 9(1):317–365, 1998.

[4] M. Dorigo, G. Di Caro, and L. M. Gambardella. Ant algorithms for discrete optimization. *Artif. Life*, 5(2):137–172, 1999.

[5] B. Karp and H. T. Kung. Gpsr: greedy perimeter stateless routing for wireless networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254, New York, NY, USA, 2000. ACM.

[6] J. Lin and G.-S. Kuo. A novel location-fault-tolerant geographic routing scheme for wireless ad hoc networks. In *Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd*, pages 1092 – 1096, Melbourne, Vic, 2006. IEEE Computer Society.

[7] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (aodv) routing, 2003.

[8] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. *SIGCOMM Comput. Commun. Rev.*, 24(4):234–244, 1994.

[9] Y. Xue and K. Nahrstedt. Fault tolerant routing in mobile ad hoc networks. In *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, pages 1174 – 1179 vol.2, New Orleans, LA, USA, 2003. IEEE Computer Society.