WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. **00**: 1–13 (2008)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/wcm.0000

Path Quality Detection Algorithms for Near Optimal Geographic Routing in Sensor Networks with Obstacles *Wireless Communications and Mobile Computing*

Luminita Moraru [†] [1] [*], Pierre Leone[1], Sotiris Nikoletseas[2] and Jose Rolim[1]

[1]*University of Geneva, 1211 Geneva 4, Switzerland*
[2] *University of Patras and CTI, 26500 Patras, Greece*

Summary

Geographic routing scales well in sensor networks, mainly due to its stateless nature. Most of the algorithms in this area are concerned with guaranteeing a path toward the destination in the context of any network topology, while the optimality of the path is of little interest. In this paper we are presenting a novel geographic routing algorithm with obstacle avoidance properties. It aims at finding the optimal path from a source to a destination when some areas of the network are unavailable for routing due to low local density or obstacle presence. It locally and gradually with time (but, as we show, quite fast) evaluates and updates the quality of the previously used paths and ignores non optimal paths for further routing. By means of extensive simulations, we are comparing its performance to existing state of the art protocols, showing that it performs much better in terms of path length and hop count thus minimizing latency, overall traffic and energy consumption. Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: Geographic Routing, QoS Routing, Obstacle Avoidance, Communication Void, Optimal Path, Sensor Networks

1. Introduction

Computing the shortest path between two nodes in a graph is a well studied problem in graph theory [1]. For the geometric domain, where the path is built based on the geographical position of the destination and of one hop neighbors, it exists as well a plethora of solutions and applications [2]. We will consider the behavior of path finding algorithms in the case when there are obstacles and local irregularities in the initial network configuration. Because of the severe limitations of sensor network devices and the lack of global network knowledge, our purpose is to find in a distributed manner the shortest possible obstacle avoidance path between two points using only local geographical information.

The simplest form of geographic routing, greedy, chooses for forwarding the neighbor closest to the destination. The main drawback: the local maximum phenomenon - there is no neighbor closer to the destination than the current node. This situation appears often when there is an obstacle or a hole in the network, in low density network areas and even in the case of medium densities. Perimeter routing solves the problem of stuck nodes by using the right hand rule to route around the perimeter, until it can switch

[*]Correspondence to: University of Geneva, 1211 Geneva 4, Switzerland Email: moraru@cui.unige.ch
[†]Research partially founded by the Swiss SER Contract No. C05.0030 and FP6-015964 AEOLUS

Prepared using wcmauth.cls *[Version: 2007/01/09 v1.00]*

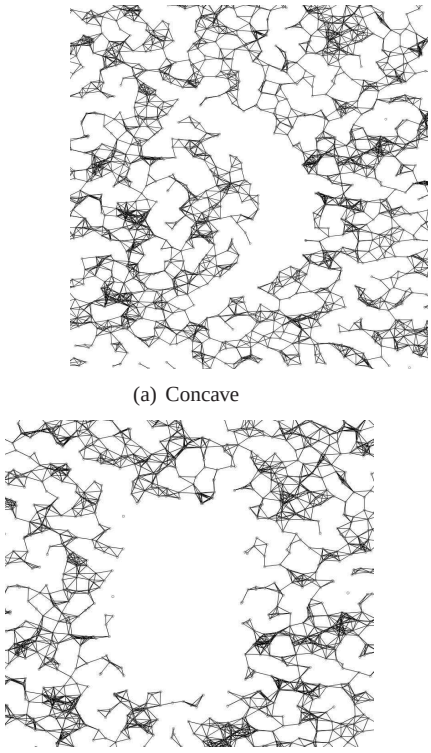
back to the greedy routing. But these paths are not optimal in terms of length, and in fact can be quite long and thus inefficient. Additionally, it cannot guarantee delivery for any shape of the obstacle, i.e it fails in the presence of some hard obstacles. Although several solutions have been proposed for routing around the holes, they represent a trade off between optimal path routing and network topology maintenance traffic.

Our approach We are proposing a mechanism for finding optimal paths, without extra maintenance traffic. It is a heuristic forwarding strategy, thus it uses the information about the previous forwarding tasks in order to make a decision. The novelty consists in considering not only the topology of the nodes, but also their previous behavior, in order to make a decision.

The usage of previous behavior for the prediction of the behavior of a node is a technique used in reputation mechanisms. The current reputation mechanisms are used to evaluate the willingness of a node to execute collaborative tasks in the network. We aim at using previous behavior to evaluate the ability of a node to forward messages on an efficient path in terms of specific cost metrics important for the sensor networks. Based on previous routing decisions, the algorithm will identify and avoid non optimal paths. The optimal path is defined as the shortest path between a node and the destination. In terms of routing decisions, we consider that the decision is optimal if greedy routing is used. If a node uses perimeter routing, then it is evaluated as a non-optimal path.

A node's rank is built based on the ratio between optimal and non optimal routing decisions. A path that contains nodes in perimeter routing will have a bad reputation, thus it is less efficient. We consider that each node is aware of the reputation of its neighbors. When a node is in greedy mode, it selects a neighbor for forwarding from the list of nodes with good reputation.

The quality of an obstacle avoidance mechanism is defined by several criteria. The quantity of information used to build the path is one of the most important ones, since it influences the communication overhead, thus the overall energy consumption and even the feasibility of the approach. We are considering the case of distributed, low complexity, low overhead, and guaranteed delivery routing protocols. Since most of the low overhead techniques do not guarantee delivery, we limit the interest in existing void handling techniques to only one category: planar graph based. Planar graph traversal algorithms provide guaranteed delivery with medium overhead, using only local information. Then, they forward messages on a planar graph extracted from the initial graph.



(a) Concave

(b) Convex

Fig. 1. Communication Voids

The effectiveness of obstacle avoidance problem is determined as well by the structure of the network and of the obstacles. In the particular case of planar graph based void handling techniques, most of the protocols fail in avoiding concave obstacles (see Fig 1(a)). Even if we consider the case of convex obstacles (see Fig 1(b)), difficulties in finding an efficient path are raised by the stateless constraint: nodes should exploit only local information.

In this context, we are introducing a technique for path length convergence to near the optimal one. This method exploits the particularities of sensor networks in order to avoid adding any communication overhead. While using only one hop location information and maintaining the computational complexity low, it provides a near optimal path in routing with obstacle avoidance, and converges relatively fast to this state. A preliminary version of the research in this paper has appeared in [37].

The paper is organized as follows: section 2 introduces the state of the art in geographic routing algorithms. Section 3 discusses the building blocks of

DOI: 10.1002/wcm

our algorithm - network communication model, object avoidance algorithms and path evaluation methods. The following section shows the modifications made to the existing protocols, to consider path quality and proposes three different evaluation methods for quality. Section 5 contains the experimental results and the last sections contains the conclusions.

2. State of the art / comparison

We address the problem of finding near optimal paths for geographic routing with obstacles avoidance. Although several obstacle avoidance techniques for geographic routing were proposed so far, most of them are concerned only with finding some path (usually a quite long one) when greedy forwarding is not possible. Moreover, the constraints like the stateless nature of geographic routing, are in contrast to the quantity of data needed to make a decision. Thus, they provide a trade off between efficiency, effectiveness on one side and complexity, communication overhead on the other side.

By default, all geographic routing algorithms are using greedy forwarding strategy. Several greedy routing techniques have been proposed in the relevant state of the art. In [8], [33], [32], [3] the authors propose greedy forwarding schemes that each time selects the next hop sensor making best possible progress toward the destination of data, in terms of different metrics. The analysis and simulations show that while [3] behaves very well in dense networks, its performance drops in sparse networks and networks with routing holes and obstacle.

When greedy fails, the algorithms enters in a recovery mode, used until greedy is again possible. We will present only the techniques that guarantee the delivery of the data, since we consider effectiveness as a mandatory requirement. The solutions are divided in the following categories[5]: planar graph based, cost based, geometric, flood based, hybrid, spanning tree based.

Planar graph traversal techniques [6], [7], [26], [25] are used since they were proved to guarantee delivery if a path exists. Planar graph based obstacle avoidance strategies use greedy as long as a node has a neighbor closer to the destination. Otherwise, one of existing planar graph traversal algorithms [9], [10], [11] is used. Since the representation of the network is not always a planar graph, this class of strategies needs to use a distributed planarization algorithm. This can be done at the network level, in the network setup phase, or it can be done on demand, only for the set of nodes where greedy forwarding cannot be used. The performances of these strategies depend on two factors: the performances of graph traversal algorithm and of the distributed planarization algorithm [29], [31], [30]. Thus most of the algorithms are concerned with improving the planar graph traversal algorithms. The optimality of the path is not considered. The gain in path length (compared with path chosen when complete network topology knowledge is available) becomes significant when obstacles are present and it is proportional with the size of the obstacle. Our approach is different: while keeping both the greedy and planar graph based strategies, our algorithm progressively marks and avoids the non-optimal paths.

Geometric obstacle avoidance is proposed in [12]. It uses the geometric properties of a node to determine if a message can be stuck at that node. An algorithm is developed to find holes in the network, defined as areas of the network bounded by the stuck nodes. The disadvantage of this technique is the high complexity of the detection of the holes. Additionally, it does not guarantee delivery when the destination is inside the hole.

Cost based approach [13] consists in assigning a cost to each node, proportional to the distance to the destination. When greedy forwarding fails, a node will forward a packet to a neighbor with a lower cost than itself. Although the complexity and the overhead of the algorithm is rather medium, it does not choose optimal paths.

Flooding based techniques [14],[15] are using broadcast to forward the message, once a packet is stuck. Although the complexity is low, the overhead is high. Although they guarantee delivery, path optimality is not a concern. An alternative to flooding is multicast. [4] proposes a redundant multipath delivery scheme that uses probabilistic choices to achieve good trade-off between efficiency and cost; while this method indeed copes well in sparse networks, it fails to bypass obstacles.

Hybrid techniques use at least two obstacle avoidance techniques. The motivation is the improved efficiency of the path and the guaranteed delivery of the message, and they are used when only one of the two techniques is not enough to achieve these requirements. The disadvantage is the increased overall complexity. [16] is a protocol combining greedy routing and adaptation of the transmission range to bypass obstacles. Indeed, the protocol manages to ”jump over” obstacles, but the routing path created is not optimal and the energy cost can become high, [17] proposes a variation of the right hand rule

DOI: 10.1002/wcm

and manages to bypass even hard obstacles. The paths it creates are quite efficient but not optimal.

Spanning tree based techniques build a spanning tree when a message is stuck at a node. In [28] they are forwarded using flooding, while in [27] the locations covered by subtrees are aggregated using convex hulls to decide which direction in the tree is closer to the destination.

3. The building blocks of our approach

3.1. Network model

We consider the case of a static network, where the entire network traffic is oriented to and from the base station. The network model is a graph $G = (V, E)$, where V represents the set of nodes and $E \subseteq V^2$ represents the set of edges. The distance between nodes is the Euclidean distance, and the path length is the sum of the distances between the intermediary hops. The two issues related with the graph representation of a network is link detection and graph planarisation method.

The information about the presence of the one hop neighbors is obtained by the means of short beacon messages, called *hello* messages [19]. Sent with maximum signal strength, hello messages are used to detect the neighbors of a node in the network. They are used both to advertise the presence of a node and its physical location.

The classical representation for network is the unit disk graph model - it makes the assumption that an edge $e \subset E$ exists only if the distance between nodes is below a certain limit. This model was proved to be inaccurate [34]. A better representation is the realistic physical layer model [35], [36] - a message is received with a probability depending on the distance between nodes. The performances of our protocol in terms of path gain is independent of the model used. The physical layer model has a direct impact on the routing protocol performance, but not on the optimization method.

The alternative we use for the planar graph building is the crossed link detection protocol algorithm, CLDP, proposed in [29]. The algorithm is used for graph planarisation and is proved to incur moderate overhead, to converge quickly and to choose low loss paths. Another advantage of this protocol is the robustness to arbitrary localization error.

By exploiting the existence of *hello* messages, each node maintains an accurate image of the path rating of each neighbor. Nodes can locally send information about the optimality status, by adding this information to the content of the *hello* messages. If the messages are sent periodically, this additional information is transmitted with only one additional bit, added at the end of the *hello* message. A second alternative for optimality status dissemination is to send an update message each time the state is changed. The trade off in choosing one of these methods is between convergence time and the overhead. If the algorithm waits until the beacon is send, then the convergence time is delayed, otherwise, more overhead is added into the network. Other factors to consider when choosing the dissemination method are the number of nodes marked as non optimal and the number of state switches of each node, since both influence directly the overhead added in the network when reactive updates are used.

In order for communication to succeed, it is necessary to map a node's ID to its location (Each transmission needs the coordinates of the destination). We are assuming the availability of a distributed location service, responsible for determining the position of the destination. GLS, as described in [18], is a suitable solution. In GLS, the mappings are stored in location servers. The main mechanisms are the querying of a node's location and the selection of the location servers. Both are based on a predefined identifier ordering and on a predefined geographic hierarchy.

We assume that all sensors are willing to collaborate, and we do not investigate security aspects. We assume as well that sensors are not being malicious or attacked. This assumption is made since routing and security are seen as two different concerns in sensor network, and existing security mechanisms [20], [21] are built with generality in mind: they are independent of the underlying communication protocols. We are only using the same mathematical tools of the trust/reputation concept in our setting. High trust in our routing case means ability to route messages efficiently around obstacles.

3.2. Planar graph based object avoidance

As discussed above, perimeter routing is the most suitable routing technique for object avoidance when greedy fails. Thus, our algorithm will use two routing modes: greedy routing and face routing. They are concerned with selecting the next relay node. We consider that the current relay, P_1 knows its geographical coordinates, the coordinates of the

DOI: 10.1002/wcm

previous node, of the destination D and of all its one hop neighbors N_i. In greedy forwarding, the choice of the next relay is a local optimum decision: the selected neighbor is the one closer to the destination. In Fig. 2, the first three transmissions are in greedy mode.

Faced with an obstacle, a node will switch to perimeter routing and the next hop will be represented by the first node counterclockwise from P_1D line. This heuristic will continue until the message reaches an edge crossing the P_1D line. At this point it will switch to another face. The purpose is to route the message around faces progressively closer to the destination. The node will return to greedy when the current node is closer to the destination than the node where perimeter routing started. In Fig. 2, P_3 is closer to D than P_1, therefore the algorithm will switch to greedy. Perimeter routing works only on planar graphs with no crossing edges.

Our purpose is to avoid the paths where the messages will fall into face routing.

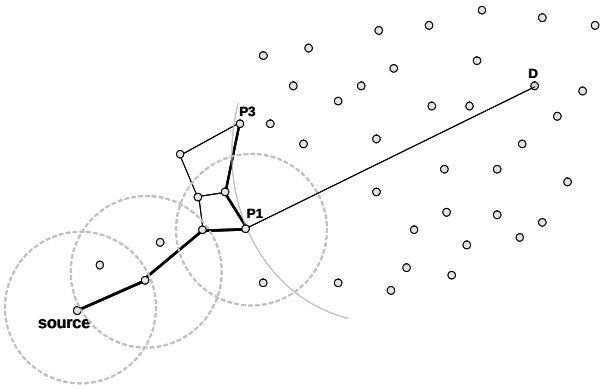


Fig. 2. Planar graph based routing

3.3. Reputation - Path ranking Analogy

Reputation systems are enforced in collaborative environments and are used to help predicting the behavior of an entity based on the previous experience with that entity. Each interaction is evaluated in terms of only two possibile results: positive or a negative. Therefore, their behavior can be modeled as a statistical process with binary events. The information obtained from the previous interactions is inferred, the outcome of future interactions is predicted and based on this prediction, a decision is made about interacting with it or not.

An example is beta reputation system [22], that uses beta probability density function to build reputation ratings. Reputation, defined as the opinion of an entity about another, is represented as a probabilistic distribution.

Trust is the expectation of an entity about the actions of the other. It is obtained by taking the statistical expectation of the probability distribution representing the reputation. If α is the number of positive outcomes and β is the number of negative outcomes, then the expected value of beta distribution is:

$$E(p) = \frac{\alpha}{\alpha + \beta}$$

Based on the trust value, an entity will decide if it will cooperate or not. A threshold is set and compared with the expected value. If the expected value is under the threshold, then the node will not cooperate.

$$behavior = \begin{cases} \text{cooperate} & \text{if E(p)} > \text{Threshold} \\ \text{not cooperate} & \text{if E(p)} < \text{Threshold} \end{cases}$$

We take the mathematical tools used by beta reputation system, but we give a different meaning. We are interested in evaluating optimality / non optimality of a path passing through a certain node. The advantages of this method are the simplicity of implementation in practical applications and the strong statistical background. Simplicity of implementation is important in sensor networks which are scarce in computational and energy related resources. The statistical background will provide robustness to the evaluation mechanism.

We are using the same model of binary events. Each node can choose from two routing decisions; one of them is evaluated as optimal, thus it will represent a positive outcome; the other is evaluated as non-optimal, and it will represent a negative outcome. Each node will choose the next forwarding neighbor based both on the suitability with the selection method and on its expected behavior.

In a system where the willingness to cooperate is evaluated, it seems reasonable that the trust is computed by the neighbors. But when the frequency of the used routing methods has to be evaluated, the node can make the decision by itself. Thus, the estimation of the routing method optimality can be made at the node level. Furthermore, the evaluation made at the neighbors' level will increase the network traffic.

4. Algorithms

The purpose of the algorithm is to obtain a gradual convergence to the optimal path. We intend to obtain

DOI: 10.1002/wcm

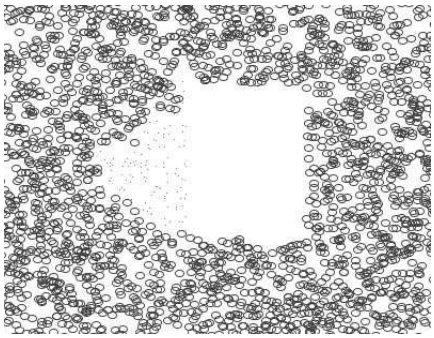


Fig. 3. Untrustworthness region for convex void

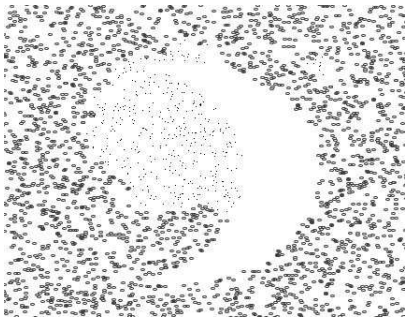


Fig. 4. Untrustworthness region for concave void

minimal path lengths by dynamically evaluating the frequency of every routing method used by a node and assigning further routing tasks based on this evaluation.

As mentioned before, geographical routing uses greedy method to choose the next neighbor. When greedy fails, another strategy - rescue mode - is enforced. We are choosing as the rescue mode strategy a planar graph based traversal algorithm to route around obstacles. We are making this decision considering the guaranteed delivery and the stateless nature of this class of protocols. Greedy routing will be considered as good quality routing method, while face routing will be evaluated as a poor quality one.

The protocol gradually evaluates the performance of a path, detecting dynamically the nodes around holes, and progressively redefining the routing paths. Each node is evaluating itself and it is spreading locally information about its performance. Once the non optimal nodes are detected and advertised, each node in greedy routing mode will avoid to choose non optimal neighbors for forwarding, thus redirecting the message outside the non optimal area.

The shape of the non optimal area is presented in Fig. 3, for convex obstacles, and Fig. 4, for concave ones. Both figures represent intermediary stages during the convergence process. The black areas represent nodes marked as optimal, while the gray area contains non optimal nodes. The edge of the non-trusted area represents the path that the messages originated at the left side of the obstacle will follow. The upper area of the void for the concave shape is marked faster, since the messages are routed only counterclockwise around the obstacle.

The evaluation of a node as non optimal depends on the relative position between the source, object and destination. The point of incidence with the object influences the number of hops a message is routed with perimeter, since the message will exit perimeter only when it finds a node closer to the destination then the perimeter entry point. This is also the reason why a small area of nodes above the concave object is marked.

Further, we will present a new routing protocol which will take into account the optimality of a node for choosing the next relay and several non optimality detection methods, outlining there advantages and disadvantages.

4.1. Routing

Algorithm 1 describes our routing protocol. It checks first what is the current routing mode. If the message is in the perimeter mode, there are two possible situations: the current node is closer to the destination than the perimeter entry point and the routing mode is switched to greedy, otherwise the current node will forward the message counterclockwise to the next neighbor on the face of the planar graph.

If the message is in the greedy mode, it will select next relay between the optimal neighbors. If greedy fails in finding the next relay, the perimeter mode is enabled. Based on the routing mode used, the optimality of the current node is updated.

The modifications to the behavior of the routing protocol are as follows. First a selection of candidates for greedy routing is made: only nodes that are closer to the destination than the current node and that are marked as optimal are included. The reason is that, even if they could represent a local optimum, since afterward they use perimeter routing, they are nodes on non-optimal paths. The condition to enter perimeter routing remains unchanged. When a message enters the perimeter mode, it will choose the first neighbor counterclockwise, with the line between the source

DOI: 10.1002/wcm

Algorithm 1 Trust based routing strategy

```
if routing_mode is "perimeter" then
  if is_closer(this, entry_point) then
    routing_mode ← greedy
  end if
end if
if routing_mode is "perimeter" then
  next ← get_next_hop("perimeter", neighs)
else
  selected_neighs ← filter(neighs)
  next ← get_next_hop("greedy", selected_neighs)

  if ! ∃ next then
    next ← get_next_hop("perimeter", neighs)
  end if
end if
update_optimality(routing_mode)
```

and the destination as a reference. Perimeter routing selection of the next hop remains unchanged as well.

With this configuration in mind, the behavior of the algorithm is similar to the classical perimeter routing algorithms for both the marked and unmarked area. We define the border as the area composed of nodes with neighbors in both marked and unmarked areas. The only difference is represented by the behavior at the border: by giving priority first to the optimal nodes, the messages will be routed around the marked area. But this behavior is possible only when the nodes at the border have greedy optimal neighbors toward the destination. Otherwise, The node will enter into the marked area, without any significant improvement on the routing path.

The second change in the routing algorithm aims at improving the path, even when the border nodes have no greedy optimal neighbors toward the destination. When the perimeter entry point chooses the next relay, it will check first the status of its neighbors. If it has both optimal and non optimal neighbors, it will select an optimal neighbor to continue routing. Since the probability that a node on a current face is closer to the destination than the current node is high, the node will switch to greedy with high probability. Therefore the message is kept on the border, advancing toward the destination in greedy or perimeter mode.

Further we will address the second important issue of the algorithm. We will sketch three different classes of optimality evaluation methods, that achieve different compromises between the efficiency and the cost of the solution achieved.

4.2. Last step based evaluation

First method (Last Step Trust), described in Algorithm 2, is to build a reputation based only on evaluation of the last interaction. Each time a node is used as a relay, it will evaluate the quality of the path and it will set the *optimality* value to 1 if greedy is used and 0 otherwise.

The advantage of this method is its simplicity, no computing effort is necessary.

Algorithm 2 Last step trust update

```
if routing_mode is "perimeter" then
  trust ← 0
else
  trust ← 1
end if
```

The disadvantage is the increased number of transmissions needed to notify the neighbors about the state changes. Additionally, the convergence time can be be quite long, especially for the border nodes. The usage of perimeter or greedy at a specific node depends as well on the position of the perimeter entry point, therefore of the source. The state of a node could change often at the border between the nodes for which the obstacle intersects the direct line between the source and the destination and the other nodes.

4.3. Bayesian interference based evaluation

Second method (Entire History Evaluation), as described in Algorithm 3, is to use two counters to evaluate the interactions. Each time the greedy routing is used, the counter for positive interactions, is increased. Each time perimeter routing is used, the counter for negative interactions is increased.

We will use Bayesian probability for interference. If g represents the number of messages sent by greedy and p the number of messages sent by perimeter, then the performance is calculated by the formula $g/(p+g)$ and represents the expected value, a number between 0 and 1. The *optimality* is determined by comparison between the *expected* value and a specific *THRESHOLD*. Initially all nodes are assigned the rating of 1.

In the context of stationary traffic, this method offers a robust evaluation and faster convergence to a stable state than the evaluation in one step. Additionally, the current state reflects the the behavior of the network, the traffic density distribution. Another factor that influences both the convergence time and the number of nodes marked as non optimal is the

DOI: 10.1002/wcm

Algorithm 3 Bayesian computation trust update

if $routing\_mode$ is "$perimeter$" **then**
  $increment\ positive\ counter$
else
  $increment\ negative\ counter$
end if
$recompute\ reputation$
if $reputation \geq THRESHOLD$ **then**
  $trust \leftarrow 0$
else
  $trust \leftarrow 1$
end if

threshold value. The lower the threshold is, the longer the convergence time and the marked number of non optimal nodes is.

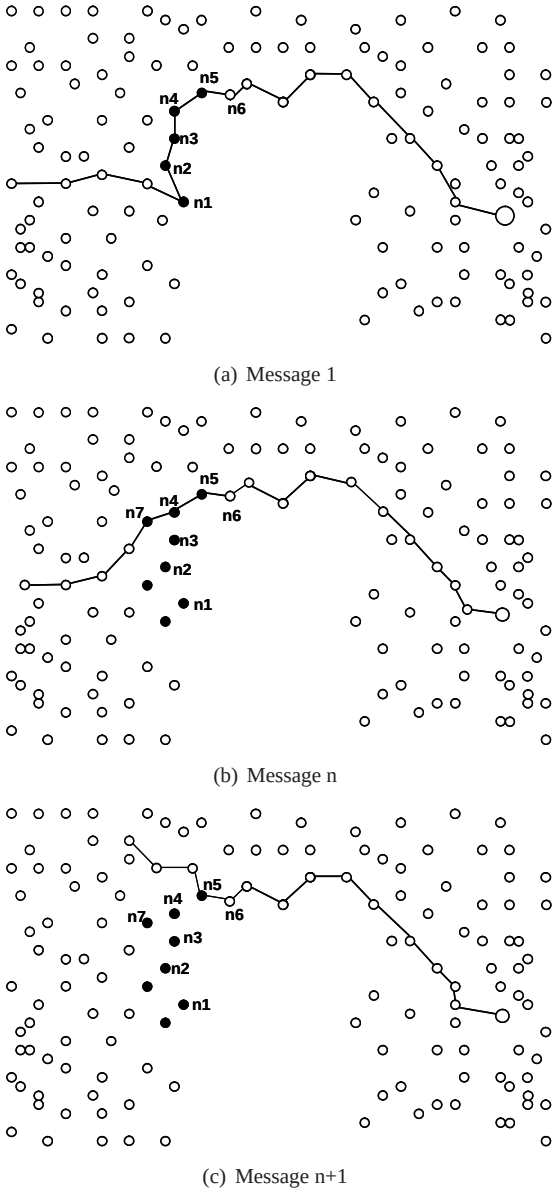
Algorithm 4 Bayesian with inference trust update

$R_d \leftarrow compute\ direct\ reputation$
for $each\ neighbor\ i$ **do**
  $R_i \leftarrow get\ reputation$
end for
$R \leftarrow (1 - WEIGHT) * R_d + WEIGHT * R_i$
if $R \geq THRESHOLD$ **then**
  $trust \leftarrow 0$
else
  $trust \leftarrow 1$
end if

4.4. Bayesian interference with propagation based evaluation

The third algorithm (Bayesian with Propagation) uses neighbors optimality in building the optimality of each node. We are using the same method as the previous described reputation system uses to combine feedback from multiple sources. The method is presented in Algorithm 4. R is the optimality of a node, R_d is the optimality value obtained as a result of the own decisions and R_i is the optimality inferred from that of the neighbors.

The weighting factor, *WEIGHT*, is a measure of the influence of the neighbors. It improves the convergence time of the algorithm, since the non optimal nodes in the vicinity of an already detected area will be marked faster. The value of the weighting factor is a trade off between the convergence time and the number of nodes detected. It has to be small enough, such that the influence of the node own behavior is more significant than the influence of the neighbors.



(a) Message 1

(b) Message n

(c) Message n+1

Fig. 5. Message path

4.5. Example

Figure 5(a) represents the path of the first message. When the message arrives at node $n1$, it switches to perimeter, since node $n1$ does not have any greedy neighbors toward the destination. The message is forwarded in perimeter mode until $n6$ which is closer

DOI: 10.1002/wcm

	n1			n2			n3			n4			n5			n6		
	+	-	R	+	-	R	+	-	R	+	-	R	+	-	R	+	-	R
M_1	0	1	NO	0	1	NO	0	1	NO	0	1	NO	0	1	NO	1	0	O
M_{n-1}	0	5	NO	0	7	NO	0	9	NO	0	9	NO	0	9	NO	9	0	O
M_n	0	5	NO	0	7	NO	0	9	NO	0	10	NO	1	9	NO	10	0	O
M_{n+1}	0	5	NO	0	7	NO	0	9	NO	0	10	NO	2	9	NO	11	0	O

Table I. Optimality indicators

to the destination than the perimeter entry point, therefore it switches to greedy. The negative counter is increased to one for the nodes $n1 - n5$, which are marked as non-optimal.

We will further present the behavior of the network and the detection of the non optimal nodes. Table I represents at each step the positive and negative counters, and the optimality value for each node.

We consider few other messages sent from the same source in Fig. 5(a), having as a result the marked area in Fig. 5(b). Fig. 5(b) represents the path of a message that avoids the marked area, choosing a path close to optimal. Node $n7$ has no optimal greedy neighbors toward the destination, therefore its negative counter is increased. Similar for $n4$. $n5$ is closer to the destination than $n4$, therefore it will switch to greedy, and its positive counter is increased.

The last step, Fig. 5(c), shows the path of a message with a different source than the previous ones. The node $n8$ has no optimal neighbors closer to the destination than itself, therefore its negative counter will increase and it will start routing in perimeter. $n5$ is closer to the destination than $n8$, and it has optimal greedy neighbors, therefore it will increase the positive counter and route in greedy mode.

5. Simulations

5.1. Network configuration

We will evaluate experimentally the performances of the algorithms mentioned above. The network configuration used is as follows. The size of the network is 50x50 units, with the number of nodes varying between 2800 and 6700, therefore the density range is between 15 and 35. We are choosing rather high densities, in order to minimize the number and the impact of the communication voids. This way, the alteration of routing performances are mainly caused by the behavior of the protocol around the object.

Two types of obstacles in the network topology are tested. The first one is a convex shape, a rectangle with the size of 10x20 units. The second type is a concave object, with the shape of a half moon, with the radius of the generator of 10.

The transmission radius of a node has 2 units, thus the ratio between the obstacle size and the transmission range is 5, therefore the obstacles are quite large.

The traffic in the network is generated in an area of size 3x3 units. The destinations are located in a 3x3 units square area on the other side of the obstacle reported to the source. The reason for this configuration is to have an evaluation of the worse case influence of the obstacles on the traffic.

The results are presented as the median of 50 experiments, after the convergence of the network. For each experiment, a message is sent into the network at each step. If the number of non optimal nodes remains constant after 300 steps, the algorithm is considered convergent, and the performance of the first message routed in the network after convergence is measured. For each experiment we are changing the network configuration: the position of the nodes and the links between the nodes.

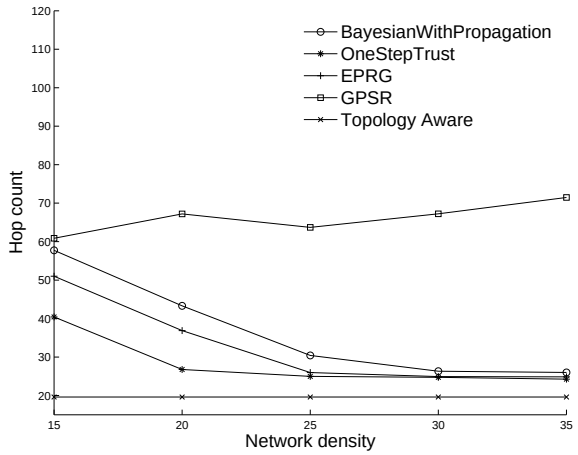
5.2. Performance evaluation

We are evaluating the performances of our three protocols: Last Step Trust, Entire History Evaluation, and Bayesian With Propagation. The comparison is made based on criteria like the path quality and the time to convergence.

We are concerned with building algorithms close to the optimal path. We define the optimal as the euclidean path. Thus, we will compare the quality of the path with the one generated by a topology aware greedy strategy. In the case of obstacles, the optimal path will have as intermediary destinations the extremities of the obstacle.Each intermediary reference is chosen as the closest extremity to the line between the current node and the destination. The optimal hop count is measured as the ratio between the euclidean distance and the communication range.

The second reference for comparison is the greedy perimeter stateless routing, as the state of the art

DOI: 10.1002/wcm



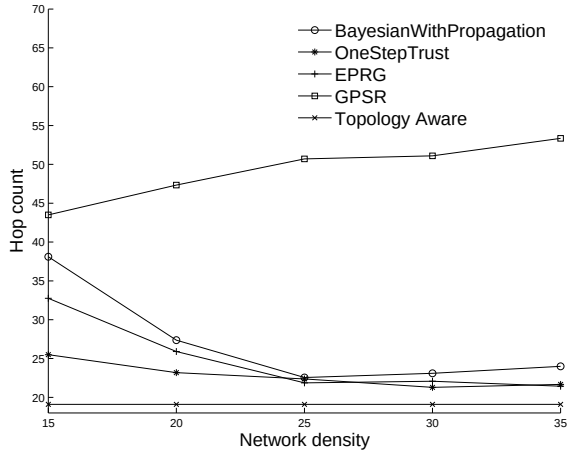
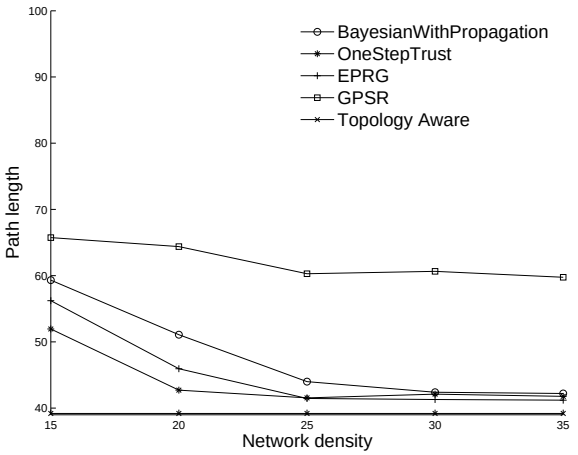


Fig. 6. Hop distance after convergence



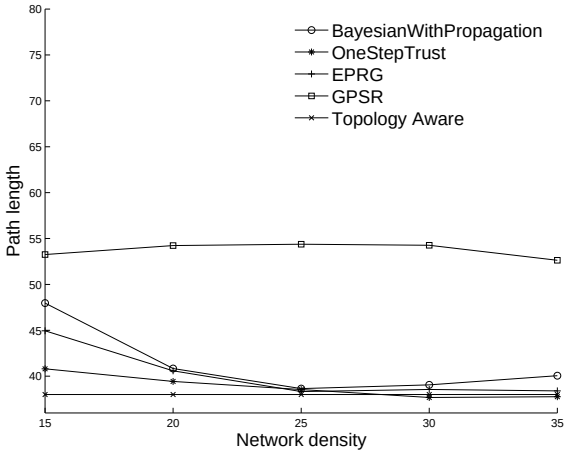


Fig. 7. Path length after convergence

in planar graph traversal based routing protocols. The planar graph traversal algorithm is convex face routing: a node walks on faces progressively closer to the destination.

5.2.1. *Hop count*

First simulation results, Fig. 6 present the average hop distance in the vicinity of the obstacle, as an estimator of the latency of the message. The first image represents the measurements for the convex obstacle, while the second represents the measurements for the concave one. The x axis represents the network size, measured in number of nodes. The y axis represents the average number of hops traversed by the message.

Greedy perimeter stateless routing introduces a latency of more than 200% in the vicinity of the obstacle. For convex obstacles, all the trust based algorithms are introducing at most 50% of latency for the highest densities. For lower densities, the One Step Evaluation has the best performance, while Bayesian With Propagation algorithm is closed to Greedy Perimeter Stateless Routing.

For concave obstacle, the gain in hop distance compared to GPSR is even higher. This is due to the effort of attaining the node closest to the destination inside the convex shape, added to the perimeter routing along the obstacle. For highest densities, the increase in hop count compared with the ideal case is 25% for ranking mechanisms, while for Greedy perimeter stateless routing is 200%. For lower densities, One Step evaluation mechanism has the closest to optimal performances.

Another observation is that GPSR does not have a liniar dependence on the network density.This can also be observed in [23] for GPSR and other suggested algorithms, the performance of the algorithms are sensitive to the density due the the impact of this

DOI: 10.1002/wcm

parameter on the planarization process. Thus, the explanation resides in the number of perimeter routing decisions. Actually, one can claim that as the network density is not high enough, voids cause difficulties to GPSR. As the network density increases, voids disappear and the total hop count decreases. Indeed, numerical experiment tends to confirm this since trust based algorithm avoid using perimeter routing and do not show similar behavior.

The final remark is that our class of algorithms have a behavior closer to the optimum when the network size increases.

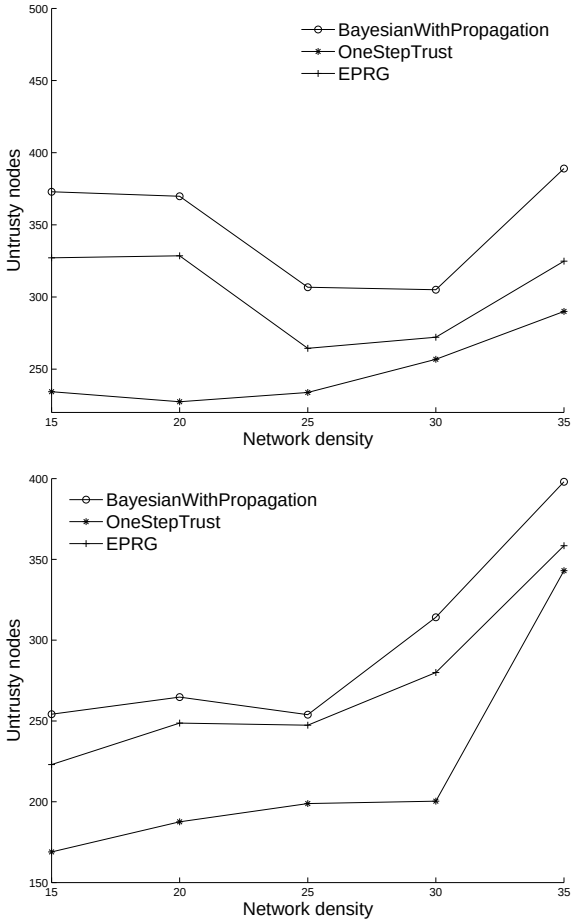


Fig. 8. Untrustworthy nodes before convergence

5.2.2. *Path Length*

The second criterion for path quality is the path length, evaluated as a sum of all intermediary euclidean distances. This parameter is important for energy consumption evaluation, since energy is more or less

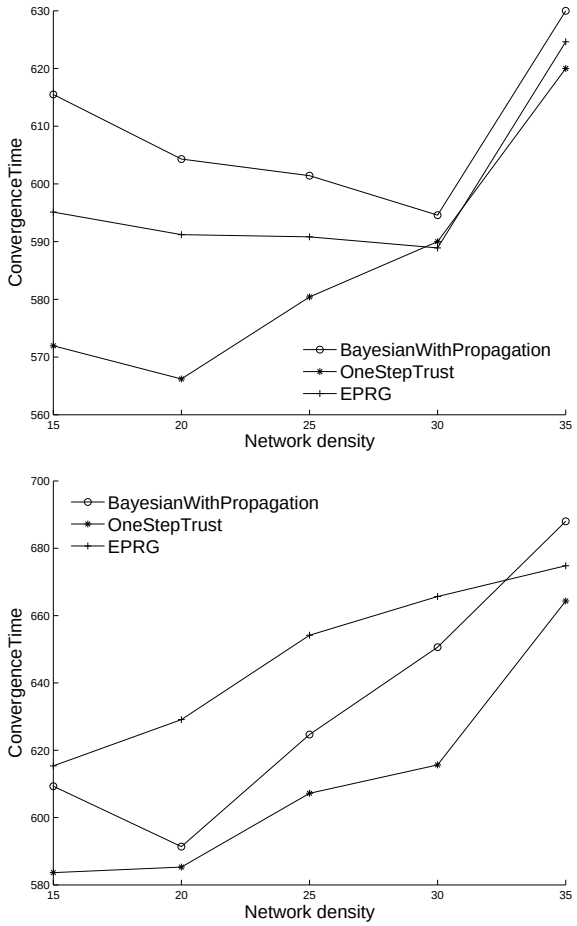


Fig. 9. Convergence time for ranking algorithms

proportional to the sum of squares of distances. Of course, to take advantage of the performance of trust based algorithms one still have to tune the energy of transmission accordingly to the physical conditions. Fig. 7 shows the median of the path length obtained by each of the algorithms. The x axis represents again the size of the network. One Step has better results than all the other algorithms in the same class. For high densities, all the ranking based algorithm have smaller average path length and their behaviors are similar. The path length decreases as the density of the network is increasing. Notably, for densities higher than 20, they are less sensitive to the particularities of the network's topology and the average path length is almost constant, as the density increases. However, the density of the network has a smaller impact on the ranking based algorithms than on GPSR.

DOI: 10.1002/wcm

5.2.3. Convergence time

The convergence time, Fig. 9 is also evaluated for different reputation algorithms. The convergence condition is a constant value for the number of untrustworthy nodes. If the network configuration is static then our algorithm is convergent.

While for lower densities, the performance of the three algorithms is different, they start to have the similar performances for high densities. Additionally, for high densities, the convergence time increases significantly.

The Bayesian with Interference algorithm has the highest convergence time. A decrease of convergence time was expected, since the state of the non optimal nodes influences the detection time for their neighbors.

5.2.4. Marked area size

In Fig. 8 we notice an increase of number of non optimal nodes with the density. There are two factors that influence the The influence of neighbors' reputation will increase the number of untrustworthy nodes. This is explained by the fact that some of the nodes at the edge of the untrustworthy area are having a small difference between the optimal and non-optimal routing decisions. If the number of non optimal neighbors is significantly higher than of optimal ones, than they can determine a change in the state of the node.

6. Conclusions

We presented a class of algorithms, heuristic based, to significantly improve the behavior of the geographic routing with obstacle avoidance protocols. It aims at providing optimal routing, by using a path ranking scheme, build with a reputation like mechanism. As the simulations show, the algorithms achieve better performances than the greedy perimeter stateless routing, the reference protocol. The performances come after the paths converge to an optimum, thus the convergence time is an important factor, and again, our algorithms converge quite fast. The quality of the path is not the only comparison criterion for the geographic routing algorithms. The overhead and the complexity of the algorithm are also important factors that we considered and the proposed mechanisms comply with both requirements.

One concern is raised by the propagation of the information about the optimality level of each node. Our ranking based model is close to the classical distributed trust building mechanisms, but still there is an important difference. Usually, the trust is build locally and distributedly by the neighbors. But, in our algorithm each node builds its own ranking, since it is a measure of the quality of the path and not a measure of the willingness to cooperate. The main advantages of this method is that it minimizes the network traffic and optimize convergence time. If a node computes its own optimality level, which is limited (for Entire History Evaluation and Last Step Evaluation) to only two values: 0 or 1, the information shared with the neighbors needs only one additional bit in order to be transmitted.

Another concern is the behavioral pathologies, identified in [24], and the unit disk model as its main source, reason why we chose a different planarization method, CLDP. With respect to this aspect, Entire History Evaluation strategy has the advantage of having smaller number of transitions (compared with Last Step Trust for example).

Future work will further investigate the properties (e.g. generality) of the algorithms. The strategy is build considering only a single fixed destination. We are interested to investigate its behavior and adapt it to both the case of mobile nodes and of multiple base stations. In this case one trust value is not enough, since the optimality of the path depends on the relative position of the destination and the obstacle. Further investigations can be done when the base station is mobile or the network configuration is dynamic.

Another assumption was that the nodes are cooperative. Further work could deal with the security/fault tolerance of the algorithm and the impact of non collaborative entities in the network.

A lot of interest has been shown to energy balanced algorithms. Of course as long as data aggregation is used, this is not an mandatory demand, but the conformance with network lifetime maximization techniques remains an interesting study direction as well.

References

1. Ahuja, R.K., Magnanti, T.L., Orlin, J.B.: Network Flows: Theory, Algorithms, and Applications. Prentice Hall, Englewood Cliffs, NJ (1993)
2. Sack, J.R., Urrutia, J.: Handbook of computational geometry. North-Holland Publishing Co., Amsterdam, The Netherlands, The Netherlands (2000)
3. Chatzigiannakis, I., Nikoletseas, S., Spirakis, P.G.: Efficient and robust protocols for local detection and propagation in smart dust networks. Special Issue on Algorithmic Solutions for Wireless,Mobile, Ad Hoc and Sensor Networks, ACM/Baltzer Mobile Networks and Applications(MONET) Journal **10**(1-2) (2005) 133–149

DOI: 10.1002/wcm

4. Chatzigiannakis, I., Dimitriou, T., Nikoletseas, S., Spirakis, P.: A probabilistic algorithm for efficient and robust data propagation in smart dust networks. Ad-Hoc Networks Journal **4**(5) (2006)
5. Chen, D., Varshney, P.: A survey of void handling techniques for geographic routing in wireless networks. Communications Surveys and Tutorials, IEEE (2007) 50–67
6. Karp, B., Kung, H.T.: GPSR: greedy perimeter stateless routing for wireless networks. In: Mobile Computing and Networking. (2000) 243–254
7. Heissenbüttel, M., Braun, T., Bernoulli, T., Wälchli, M.: BLR: Beacon-less routing algorithm for mobile ad-hoc networks (2003)
8. Kranakis, E., Singh, H., Urrutia, J.: Compass routing on geometric networks. In: Proc. 11 th Canadian Conference on Computational Geometry, Vancouver (1999) 51–54
9. Urrutia, J.: Routing with guaranteed delivery in geometric and wireless networks. (2002) 393–406
10. Kuhn, F., Wattenhofer, R., Zollinger, A.: Worst-Case Optimal and Average-Case Efficient Geometric Ad-Hoc Routing. In: Proc. 4^{th} ACM Int. Symposium on Mobile Ad-Hoc Networking and Computing (MobiHoc). (2003)
11. Kuhn, F., Wattenhofer, R., Zhang, Y., Zollinger, A.: Geometric ad-hoc routing: Of theory and practice (2003)
12. Fang, Q., Gao, J., Guibas, L.J.: Locating and bypassing holes in sensor networks. Mob. Netw. Appl. **11**(2) (2006) 187–200
13. Chen, S.: (Avoid void in geographic routing for data aggregation in sensor networks)
14. Stojmenovic, I., Lin, X.: Loop-free hybrid single-path/flooding routing algorithms with guaranteed delivery for wireless networks. IEEE Trans. Parallel Distrib. Syst. **12**(10) (2001) 1023–1032
15. Jain, R., Puri, A., Sengupta, R.: Geographical routing using partial information for wireless ad hoc networks (1999)
16. Boukerche, A., Chatzigiannakis, I., Nikoletseas, S.E.: A new energy efficient and fault-tolerant protocol for data propagation in smart dust networks using varying transmission range. Computer Communications (COMCOM) Journal **29**(4) (2006) 477–489
17. Nikoletseas, S., Powell, O.: Simple and efficient geographic routing around obstacles for wireless sensor networks. In: Proceedings of the 6th International Workshop on Efficient and Experimental Algorithms (WEA), Lecture Notes in Computer Science (LNCS), Springer-Verlag (2007) 161–174
18. Li, J., Jannotti, J., Couto, D.S.J.D., Karger, D.R., Morris, R.: A scalable location service for geographic ad hoc routing. In: MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, New York, NY, USA, ACM Press (2000) 120–130
19. Stojmenovic, I.: Handbook of Sensor Networks: Algorithms and Architectures. John Wiley and Sons, Inc (2005)
20. Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E.: Spins: security protocols for sensor networks. Wirel. Netw. **8**(5) (2002) 521–534
21. Ganeriwal, S., Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. In: SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, New York, NY, USA, ACM Press (2004) 66–77
22. Ismail, R., Josang, A.: The beta reputation system. In: Proceedings of the 15th Bled Conference on Electronic Commerce. (2002)
23. Leong, B., Mitra, S., Liskov, B.: Path vector face routing: Geographic routing with local face information. In: ICNP '05: Proceedings of the 13TH IEEE International Conference on Network Protocols (ICNP'05), Washington, DC, USA, IEEE Computer Society (2005) 147–158
24. Kim, Y.J., Govindan, R., Karp, B., Shenker, S.: Geographic routing made practical. In: NSDI'05: Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation, Berkeley, CA, USA, USENIX Association (2005) 16–16
25. Susanta Datta and Ivan Stojmenovic and Jie Wu: Internal Node and Shortcut Based Routing with Guaranteed Delivery in Wireless Networks. In Proceedings of the 21st international Conference on Distributed Computing Systems (April 16 - 19, 2001). ICDCSW. IEEE Computer Society, Washington, DC, 461.
26. Bose, P., Morin, P., Stojmenovic', I., and Urrutia, J. Routing with guaranteed delivery in ad hoc wireless networks. Wirel. Netw. 7, 6 (Nov. 2001), 609-616. DOI= http://dx.doi.org/10.1023/A:1012319418150
27. Leong, B., Liskov, B., and Morris, R. Geographic routing without planarization. In Proceedings of the 3rd Conference on 3rd Symposium on Networked Systems Design & Implementation - Volume 3 (San Jose, CA, May 08 - 10, 2006). USENIX Association, Berkeley, CA, 25-25.
28. S. Radhakrishnan, N. S. V. Rao G. Racherla, C. N. Sekharan, and S. G. Batsell, DST - a routing protocol for ad hoc networks using distributed spanning trees, IEEE Wireless Communications and Networking Conference, pp. 100–104, 1999.
29. Kim, Y., Govindan, R., Karp, B., and Shenker, S. Geographic routing made practical. In Proceedings of the 2nd Conference on Symposium on Networked Systems Design & Implementation - Volume 2 (May 02 - 04, 2005). USENIX Association, Berkeley, CA, 217-230.
30. G. Toussaint. Some unsolved problems on proximity graphs In D. W. Dearholt and F. Harary, editors, Proceedings of the First Workshop on Proximity Graphs. Memoranda in Computer and Cognitive Science MCCS-91-224. Computing research laboratory, New Mexico State University, Las Cruces, 1991.
31. K. Ruben Gabriel and Robert R. Sokal A New Statistical Approach to Geographic Variation Analysis Systematic Zoology, Vol. 18, No. 3 (Sep., 1969), pp. 259-278
32. Takagi, H.; Kleinrock, L. Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals IEEE Transactions on Communications. Volume 32, Issue 3, Mar 1984 Page(s): 246 - 257
33. G.G. Finn. Routing and addressing problems in large metropolitan-scale internetworks. Technical Report ISI/RR-87-180, Information Science Institute, March 1987
34. Schmitz, R., Torrent-Moreno, M., Hartenstein, H., and Effelsberg, W. The Imapct of Wireless Radio Fluctuations on Ad Hoc Network Performance. In Proceedings of the 29th Annual IEEE international Conference on Local Computer Networks (November 16 - 18, 2004). LCN. IEEE Computer Society, Washington, DC, 594-601. DOI= http://dx.doi.org/10.1109/LCN.2004.125
35. I. Stojmenovic, A. Nayak, J. Kuruvila, F. Ovalle-Martinez and E. Villanueva-Pena Physical layer impact on the design and performance of routing and broadcasting protocols in ad hoc and sensor networks Computer Communications, Volume 28, Issue 10, 16 June 2005, Pages 1138-1151
36. Nadeem, T.; Agrawala, A. IEEE 802.11 fragmentation-aware energy-efficient ad-hoc routing protocols IEEE International Conference on Mobile Ad-hoc and Sensor Systems, 25-27 Oct. 2004 Page(s): 90 - 103
37. Moraru, L., Leone, P., Nikoletseas, S., and Rolim, J. D. Near optimal geographic routing with obstacle avoidance in wireless sensor networks by fast-converging trust-based algorithms Proceedings of the 3rd ACM Workshop on QoS and Security For Wireless and Mobile Networks (Chania, Crete Island, Greece, October 22 - 22, 2007). Q2SWinet '07. ACM, New York, NY, 31-38.

DOI: 10.1002/wcm