West Chester University
Digital Commons @ West Chester University

Computer Science

College of Arts & Sciences

2009

A Straightforward Path Routing in Wireless Ad Hoc Sensor Networks

Zhen Jiang
West Chester University of Pennsylvania, zjiang@wcupa.edu

Junchao Ma
Hong Kong Polytechnic University

Wei Lou
Hong Kong Polytechnic University

Jie Wu
Florida Atlantic University

Recommended Citation

Jiang, Z., Ma, J., Lou, W., & Wu, J. (2009). A Straightforward Path Routing in Wireless Ad Hoc Sensor Networks. *29th IEEE International Conference on Distributed Computing Systems Workshops, 2009*, 103-108. http://dx.doi.org/10.1109/ICDCSW.2009.47

A Straightforward Path Routing in Wireless Ad Hoc Sensor Networks [*]

Zhen Jiang
Computer Sci. Dept.
West Chester Univ.
West Chester, PA 19383, USA

Junchao Ma, Wei Lou
Department of Computing
Hong Kong Polytechnic Univ.
Kowloon, Hong Kong

Jie Wu
Computer Sci. & Eng.
Florida Atlantic Univ.
Boca Raton, FL 33431, USA

Abstract

Building a "Straightforward" path in wireless ad hoc sensor networks (WASNs) not only avoids wasting energy in detours, but also incurs less interference in other transmissions when fewer nodes are involved in the transmission. This plays an important role in recent WASN applications that require a streaming service to deliver large amount of data. In this paper, we extend our early work on the straightforward path routing in WASNs in the presence of the "local minima", where the routing is blocked due to the lack of available forwarding successors. We bring some new insights of the safety information model for a forwarding routing that is limited in the request zone. A new routing is proposed to make a more intelligent decision in greedy advance and achieve more straightforward paths. The experimental results show substantial improvements of our approach compared with the best result known to date.

Keywords: *Distributed algorithm, information model, routing, wireless ad-hoc sensor networks.*

1 Introduction

Geographic greedy forwarding (GF routing) [6], as a simple, efficient and scalable strategy, is the most promising routing scheme in wireless ad-hoc sensor networks (WASNs). In such a multi-hop unicasting, the path from the source to the destination is determined at each intermediate node in a fully-distributed manner by selecting its successor in the forwarding. The packet advances greedily along a *straightforward* path hop by hop. Not only can it avoid wasting energy in detours, but also less interference occurs in other transmissions when fewer nodes are involved in the transmission. This plays an important role in recent WASN applications that require a steaming service to deliver large amount of data.

An important challenge often faced in GF routing is the "local minimum phenomenon" [1] where the forwarding process is blocked at a node called *stuck node*. The occurrence of block can be caused by not only the "deployment hole" such as sparse deployment and physical obstacles, but also many dynamic factors, including node failures, signal fading, communication jamming, power exhaustion, interference, and node mobility [1, 10, 11].

To mitigate the local minimum issue, existing routings adopt a perimeter routing phase [2] where the packet is routed by the "right-hand rule" counter-clockwise along a face of the planar graph that represents the same connectivity as the original network, until it reaches a node that is closer to the destination than that stuck node. Then, the routing returns to the greedy advance phase. However, without enough information of the entire blocking area, a long detour path may be needed in the perimeter routing, compared with the shortest path to the destination.

In our early work [7], the safety information model is provided for the forwarding (also called LGF routing) that is limited within the request zone in LAR scheme 1 in [8]. A straightforward path can be achieved if and only if safe nodes are used. The other nodes are called unsafe. In this paper, we improve such a safety information based LGF routing (SLGF routing) by providing a more straightforward path in the phases of safe forwarding and perimeter routing, and further reducing the need for the perimeter routing phase.

The contributions are threefold. (a) The connected unsafe nodes constitute an unsafe area and its shape can be estimated as a rectangular region. Considering the relative locations of the destination and unsafe areas, the whole forwarding zone is divided into the critical and forbidden regions (see Fig. 1 (b)). The access of forbidden region will be avoided when the destination is inside the critical region. (b) Instead of applying the enforced routing phase to enter an unsafe area, which will directly lead to a perimeter routing phase, the routing uses other types of safe nodes as the backup to route around the unsafe area until a safe forwarding path is found. Such a backup path can also be used to

[*] This work was supported in part by NSF grants CNS 0422762, CNS 0434533, CNS 0531410, CNS 0626240, and CCF 0840891. Contact E-mail: zjiang@wcupa.edu

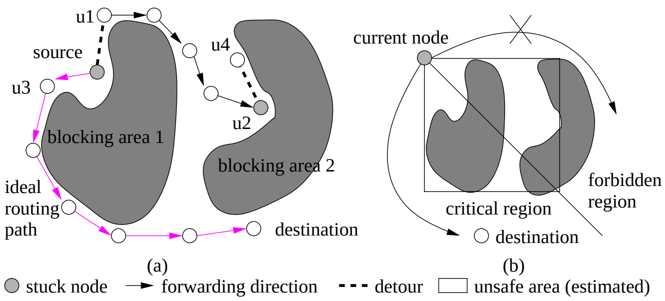


Figure 1. (a) Detour problem by intertwined local minima. (b) Illustration of the critical and forbidden region.

connect the unsafe source with a safe forwarding path to the destination. (c) The perimeter routing, if it is needed, will be limited within a rectangular unsafe area to avoid many unnecessary trials.

The remainder of this paper is organized as follows: Section 2 provides some background information. Section 3 introduces the LGF routing. Then, the safety information model that determines the availability of each node is discussed. The estimated shape information and its distributed construction process, including information collection, distribution, and storage are also introduced. Section 4 proposes the new safety information based routing. In Section 5, the experimental results are provided to show the performance improvement of our new routing compared with the best results known to date. Section 6 concludes the paper and provides directions for future research.

2 Related Work

In [3], some stuck nodes are identified as “dead ends”. By removing the interference of holes, the detour in the perimeter routing phase will be more efficient. In [4], a local protocol produces short-cuts for the perimeter routing to bypass the holes. However, both routings cannot avoid the occurrence of every local minimum.

Recent work has focused on the use of the area that contains the stuck nodes. In [5], a process called BOUNDHOLE is initiated to form a closed circle (also called the boundary). However, the block problem of the local minimum cannot be solved completely by limiting the solution along its boundary self. Consider a scenario in Fig. 1 (a) where the source s wishes to send packets to the destination d. s is a stuck node. A perimeter routing will be conducted to reach u_1. After the routing leaves away from the blocking area, it will encounter the second blocking area and be blocked at node u_2; that is, another perimeter routing phase is needed. However, when the routing detours to u_3 at s in another direction, it will not be affected by the second blocking area due to the repulsive force along the boundary of the first blocking area. Thus, the mutual impact of blocking areas should be detected early and help the routing to select a shorter path in the global view.

However, this is very difficult to achieve when no global information can be used in multi-hop systems. Many existing methods (e.g., [9]) ignores the fact that the node availability is relative when the source and destination change their relative locations. Imagine that the information needed at s in the above case will be unnecessary when the routing is reversed from the destination to the source, due to the repulsive force along the blocking areas. As a result, the information is not precise enough for every case and needs to re-constitute every time. It will be more challenge to achieve a simple local description at each intermediate node that correctly infers such a global eligible condition for any possible routing path.

In our early work [7], the safety level model is provided for LGF routing. For a given network configuration, the safe/unsafe status of each node is deterministic and unique. The connected unsafe nodes will form an unsafe area with the consideration of the mutual impact of blocking areas. A straightforward path can be achieved if and only if safe nodes are used. This is a balance point of tradeoff between the structure regularity of node status and the flexibility of routing adaptivity. However, when a routing is initiated at an unsafe source or has an unsafe destination, the perimeter routing without the safety information is adopted. A more intelligent routing is needed for determining when and how the perimeter routing phase is conducted.

3 Safety Information Model

With the assumption that all the sensors have the same communication range, a WASN can be represented by a simple undirected graph $G = (V, E)$, where V is a set of vertices including all the nodes and E is a set of undirected edges, each of which indicates two nodes are within the communication range of each other. $N(u)$ denotes the set of neighboring nodes of node u. Each node u has the location (x_u, y_u), simply denoted by $L(u)$. $\mid L(u)-L(v) \mid$ is the distance between two nodes u and v. $s(x_s, y_s)$ and $d(x_d, y_d)$ are the source and the destination nodes. $[x_1 : x_2, y_1 : y_2]$ represents a rectangle with four corners (x_1, y_1), (x_1, y_2), (x_2, y_2), and (x_2, y_1).

In this paper, all the routing schemes are presented via their forwarding node selection at an intermediate node $u(x_u, y_u)$. Rectangle $[x_u : x_d, y_u : y_d]$ has both u and d at the opposite corners. It is also called the request zone of node u in LAR scheme 1 in [8]. The request zones with respect to d in quadrants I, II, III, and IV are of types 1, 2,

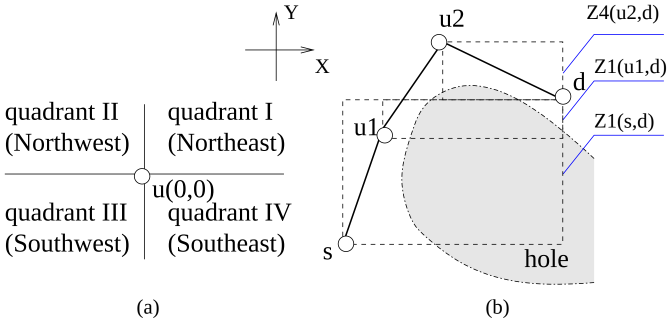


Figure 2. Definition of different types of request zones.

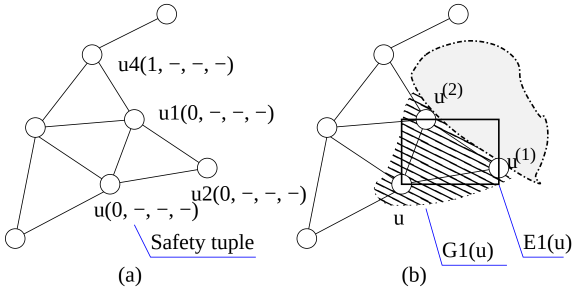


Figure 3. Labeling process for type-1 unsafe nodes ("-" stands for safe/unsafe statuses of other types). (a) stabilized safety information, and (b) $GF_1(u)$ & $E_1(u)$.

3, and 4, denoted by $Z_i(u, d)$ $(1 \leq i \leq 4)$. Respectively, each corresponding quadrant is called a type-i *forwarding zone*, denoted by $Q_i(u)$. A greedy advance within $Z_i(u, d)$ is called the type-i forwarding. Note that the forwarding for one packet may experience different types of request zones, when the relative position of d to u changes and d locates in different types of request zones (see in Fig. 2 (b)). To simplify the discussion, we describe all the schemes in a synchronous, round-based system. All the schemes presented in this paper can be extended easily to an asynchronous round based system.

As one of many traditional geographic greedy routings using "right-hand rule" policy [2] in the perimeter routing phase, the limited geographic greedy routing, denoted by LGF, selects the forwarding successor candidates within the request zone at the current node u. The successor node selection in its perimeter routing phase is implemented by simply rotating the ray ud counter-clockwise until the first untried node $v \in N(u)$ is hit by the ray. The details of the LGF are shown in Algo. 1.

Algorithm 1 (LGF routing) [7]: Determine the successor v at the current node u.

1. If $d \in N(u)$, $v = d$.
2. Determine the request zone $Z_k(u, d)$ $(1 \leq k \leq 4)$ according to $L(u)$ and $L(d)$.
3. select $v \in Z_k(u, d) \cap N(u)$.
4. If such a v does not exist, send the packet in the perimeter routing by the "right-hand rule" policy [2].

In LGF routing, say type-i, the perimeter routing phase starts when the current node u has no successor candidate inside Q_i; that is, the local minimum occurs. In the safety information model, the nodes are labeled as *unsafe nodes* if using them and only using them will cause a local minimum. Otherwise, the node is called *safe*. Due to the types of forwarding zones, there are four different types of safe/unsafe statuses for each node u, denoted by $S_i(u)$. The definition of safe/unsafe status of each type and the corresponding labeling process are shown as follows.

Definition 1 (labeling process): *Initially, each healthy node u sets its status $S_i(u)$ to 1 $(1 \leq i \leq 4)$ where "1" (or "0") stands for the safe (or unsafe) status. Any status, say $S_i(u)$, will change to unsafe if there is no type-i safe neighbor in the type-i forwarding zone; that is, $\forall v \in N(u) \cap Q_i(u), S_i(v) = 0$. The connected unsafe nodes constitute an unsafe area.*

According to Definition 1, a change of safe status of node u may also affect its neighbors' safety information and contribute further changes. The local minimum and all nearby connected unsafe nodes form a so-called *unsafe area*. According to the type of unsafe nodes contained, four types of unsafe areas form respectively. We assume that all of the communication actions occur inside the *interest area*. This area is an inner part of the deployment area encircled by the edge of networks, which can easily be built by the hull algorithm. In our labeling process, each edge node will always keep its status tuple as (1, 1, 1, 1). Thus, the edge of interest area will not affect the label of nodes inside.

A sample of the labeling process is shown in Fig. 3 (a). Initially, all nodes will set their type-1 statuses as safe $(S_1 = 1)$. In the first round, nodes u_1 and u_2 will change their statuses to unsafe $(S_1(u_1) = S_1(u_2) = 0)$. In the second round, this unsafe status change will cause the change of the $S_1(u)$. u_1 and u_2 are stuck nodes. u is not a stuck node but it is one of those nodes that their type-1 forwarding successors are all stuck nodes. A straightforward path should avoid using either of these kinds of unsafe nodes according to the following theorem.

Theorem 1 [7]: *Any LGF routing can be blocked by a local minimum if and only if one type-i unsafe node is used.*

The *greedy region* $G_i(u)$ includes all the type-i unsafe nodes that can be reached from u by a type-i forwarding. For any node $v \in G_i(u)$, we can always find a path $v_0(=u)$, v_1, v_2, $\cdots$, $v_n(=v)$, such that v_i $(0 \leq i \leq n-1)$ is type-i unsafe and $v_{i+1} \in Q_i(v_i)$. A sample of $G_1(u)$ is shown in Fig. 3 (b). Rotate a ray from u scanning $G_i(u)$, counter-clockwisely. We denote that $u^{(1)}$ and $u^{(2)}$ are the farthest nodes that can be reached on the first and the last greedy forwarding paths. When the routing reaches node u, $u^{(1)}$ or $u^{(2)}$ can be used as the bound to detour around the hole. Therefore, from the view of node u, the shape of unsafe area H can be estimated as $H \cup [x_u : x_{u^{(1)}}, y_u : y_{u^{(2)}}]$. Furthermore, for a type-i forwarding routing, the shape of unsafe area can simply be represented by $E_i(u)$: $[x_u : x_{u^{(1)}}, y_u : y_{u^{(2)}}]$.

Individually, each unsafe node u will have its own estimated shape information of the related unsafe area. To collect and distribute such information, we have the following implementation. To simplify the discussion, we focus on type-1 unsafe nodes and E_1. When u has no neighbor in $Q_1(u)$, $u^{(1)} = u^{(2)} = u$. For the rest of cases, the location information of $u^{(1)}$ and $u^{(2)}$ is collected as well as the propagation of unsafe status. Each node w along that type-1 forwarding path from u to $u^{(1)}$ will have $w^{(1)} = u^{(1)}$. Node u can collect the location information of $u^{(1)}$ from its neighbor along that path, i.e., the first type-1 unsafe neighbor hit by a ray from u when scanning $Q_1(u)$ in counter-clockwise order. Similarly, we have a path from u to $u^{(2)}$ for the update of $u^{(2)}$ at u. Fig. 3 (b) shows the type-1 forwarding region of the unsafe node u and the corresponding farthest reachable nodes $u^{(1)}$ and $u^{(2)}$. Then, the shape of the unsafe area in the Northeast is estimated as $E_1(u)$: $[x_u : x_{u^{(1)}}, y_u : y_{u^{(2)}}]$. In the following theorem, we show that the convex rectangle $E_i(u)$ is an accurate description for the routing at u.

Theorem 2 [7]: *The type-i forwarding from node u in LGF routing will be blocked iff any node inside the estimated type-i unsafe area $E_i(u)$ $[x_u : x_{u^{(1)}}, y_u : y_{u^{(2)}}]$ is used.*

Algo. 2 shows the details of the construction process. In such a process, the safety status and the estimated shape information are collected and distributed via information exchanges among neighbors. Such an exchange is implemented by broadcasting such information of a node that newly changes its safety status to all its neighbors.

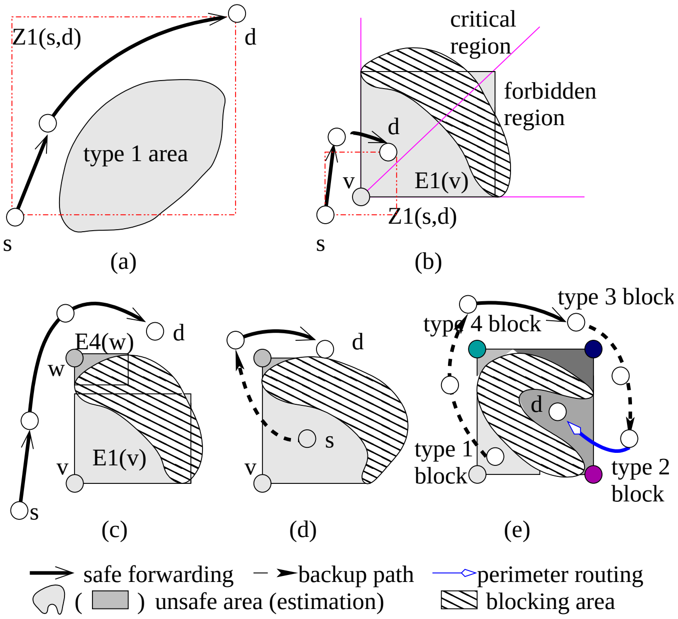


Figure 4. Samples of SLGF2 routing.

Algorithm 2 [7]: Information Construction.

1. Each healthy node is initially labeled as a safe node.
2. For each safe node u, change one of its status to unsafe, say S_i, if there is no type-i safe neighbor within $Q_i(u)$.
3. For an unsafe node, say type-i unsafe, set $u^{(1)} = u^{(2)} = u$ if $N(u) \cap Q_i(u) = \phi$. Otherwise, $u^{(1)} = v_1^{(1)}$ and $u^{(2)} = v_2^{(2)}$, where v_1 and v_2 are the first and the last type-i unsafe neighbors hit by a ray from u when scanning $Q_i(u)$ in counter-clockwise order.
4. Repeat steps 2 and 3 until no safe node changes its status.

4 Information based Routing (SLGF2)

Safe forwarding phase. Basically, at the current node u, a neighbor $v \in N(u)$ that is safe to the destination (i.e., $S_{\Bbbk}(v) > 0$) is always preferred. k and $\Bbbk$ denote the types of the request zones at u and v. Note that k and $\Bbbk$ are not necessarily the same. Regardless of the safety status of the source s, when s has a safe successor to initiate the $SLGF2$ routing, that safety status guarantees all the greedy advances along the routing path based on Theorems 1. When the destination d is type-k' safe ($k' = (\Bbbk + 2)\ Mod\, 4, 1 \leq k' \leq 4$), a straightforward path is achieved. Samples of this safe forwarding from s to d can be seen in Fig. 4 (a), (b), and (c).

Backup path routing phase. When u is safe in one of four types but not in the type of its request zone (i.e., $S_k(u) = 0 \wedge S_i(u) > 0$, $i \neq k$), the routing from u can use the type-i forwarding to approach to the edge of that type-k unsafe area and then leave away from such an area. The $SLGF2$ routing is extended with a guided backup path to reach an intermediate node so that the safe forwarding can continue (see Fig. 4 (d)). The number of detours is in proportional of the perimeter of the unsafe area. Due to the limited size of each unsafe area, the length of the routing path can be controlled.

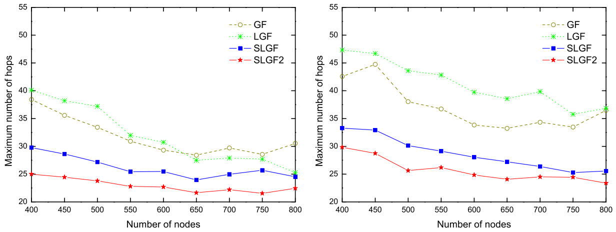
Perimeter routing phase. When the source or the destination has the safety tuple $(0,0,0,0)$, the network may have disconnected. In a cautious way, the above safe forwarding will experience all four types of request zones (see Fig. 4 (e)) and then apply the perimeter routing in the area that covers all four E areas.

When u can collect an unsafe area estimation from its unsafe neighbor v, u is neighboring such an unsafe area. For the routing at u, the successor selection will prefer to those candidates that are not in the critical region of $E_i(v)$ while the destination is in the forbidden region. According to $E_i(v) : [x_v : x_{v^{(1)}}, y_v : y_{v^{(2)}}]$, $Q_i(v)$ is divided by the ray $(x_v, y_v)(x_{v^{(1)}}, y_{v^{(2)}})$ into two parts. The region with d is called *critical region* and the other is called *forbidden region* (see Fig. 4 (b)). Such a selection will help routing avoid unnecessary detours around the edge of $E_i(v)$. Because the destination can be located in either of these two parts, the node selection will be in either side of blocking of v; that is, the routing routes around $E_i(v)$ by either "left-hand rule" or "right-hand rule". It is implement in a superseding rule on the candidates selected in all the above phases, called the "either-hand rule". Note that in the backup path routing phase, once a certain hand-rule is applied, the routing will keep using the same hand-rule until it escapes from the unsafe area and finds a safe forwarding. This will avoid the oscillation in node selection. Similarly, once the perimeter routing is initiated, the routing will stick with the same hand-rule until the destination is reached.

With the safety information, our routing can predict the success greedy advances ahead and avoid wasting time and channel resources. In summary, the routing will use the estimated shape information stored at the unsafe nodes to conduct the routing phases in the following order: (1) forward to a node that is safe to the destination (also called safe forwarding), (2) forwarding to a different type of safe node until a safe forwarding path can be found (also called backup path forwarding), and (3) perimeter routing. Moreover, for each of these three cases, the relative location of the destination and the successor is considered in a superseding rule to avoid extra detours around the edge of estimated unsafe area. The details of SLGF2 routing are shown in Algo. 3.

Algorithm 3 ($SLGF2$ routing): Determine the successor of node u (including node s) with respect to $N(u)$.

1. Apply steps 1) and 2) of Algo. 1.
2. **Safe forwarding**. Select $v \in N(u) \cap Z_k(u,d)$, where the forwarding from v to d is safe with respect to request zone $Z_{\Bbbk}(v,d)$.
3. **Either-hand rule (Superseding rule)**. In the above step, the successor selection will prefer to those candidates that are not in the forbidden region of any unsafe area while d is inside the critical region.
4. **Backup path forwarding**. Select $v \in N(u)$ by the "either-hand rule" such that $\exists S_i(v) > 0$ and stick with the same hand-rule, until the forwarding from v to d is safe with respect to request zone $Z_{\Bbbk}(v,d)$.
5. **Perimeter routing**. Route by the "either-hand rule" and stick with the same hand-rule until the destination is reached.



(a) Under IA model (b) under FA model

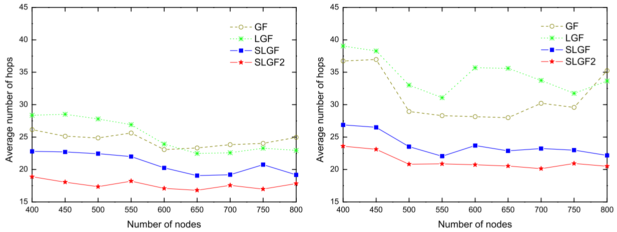
Figure 5. Maximum number of hops of a GF, LGF, SLGF, SLGF2 routing.

5 Experimental Results

In this section, we study the performance of the proposed information model and routing algorithms, using a simulator built in C++. The performance metrics used in the evaluation are the hops and length of routing path. Note that the construction cost of safety information has been proved to be the minimum in [7].

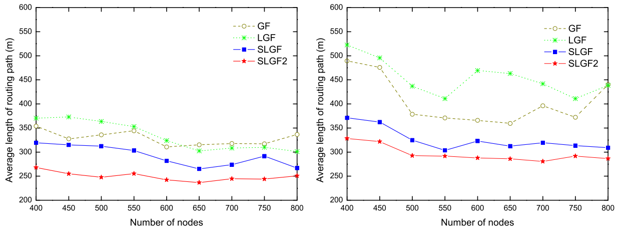
In the simulations, nodes with a transmission radius of 20 meters are deployed to cover an interest area of 200m × 200m, under different deployment models. First, the nodes will be deployed uniformly. This is ideal model (denoted by IA), in which the hole is only caused by a sparse deployment. Usually, the size of a hole is very small. Secondly, we randomly set some forbidden areas inside interest area, where no nodes can be deployed. The forbidden areas, which may be irregular, are constructed to study the impact of larger holes on the proposed algorithms. Such a model is denoted by FA. We assume that the destination and the source are randomly selected in the interest area, including both safe sources and unsafe sources. Before we test the routing performance in routing time, within the interest area, boundary information [5] is constructed for GF routings, and safety information and estimated shape information are constructed for our SLGF and SLGF2 routing. Then, we test the networks when the number of nodes in the interest area is varied from 400 to 800 in increments of 50. For each case, 100 networks are randomly generated, and the average routing performance over all of these randomly sampled networks is reported.

Fig. 5 shows the upper bound of the number of hops of routing path. Respectively, Fig. 6 shows the average



(a) Under IA model (b) under FA model

Figure 6. Average number of hops of a GF, LGF, SLGF, SLGF2 routing.



(a) Under IA model (b) under FA model

Figure 7. Average length of a GF, LGF, SLGF, SLGF2 routing.

number of hops of routing path. LGF routing may experience more perimeter routing phases than GF routing, because its forwarding adaptivity is limited and it will experience more blocking cases that have no forwarding node to use. With the safety information, the routing can predict the holes ahead and avoid being blocked. In this way, both information based routings SLGF and SLGF2 can keep the forwarding direction in many cases and require the fewest number of hops in detour. Moreover, with our extension in utilizing the estimated shape information, the SLGF2 routing can improve the performance by reducing a great number of detours in its perimeter routing phase. Fig. 7 shows the corresponding length of entire routing path on average. These results prove the new routing under our safety information model can always achieve shorter path and conserve more energy used in data transmission.

6 Conclusion

This paper extends our early work on safety information in WASNs and further illustrates the use of regular structure. With the estimated shape information of unsafe area, it improves the routing performance by reducing a great number of detours and path length while still keeping the cost of information construction to the minimum. In our future work, we will extend our approach and search for a new balance point to increase the routing adaptivity so that fewer perimeter routing phases are needed and the routing path will be more straightforward and shorter. Also, we will conduct a further study on more accurate information for unsafe areas so that shorter paths can be achieved.

References

[1] N. Ahmed, S. Kanhere, and S. Jha. The holes problem in wireless sensor networks: A survey. *ACM Sigmobile Mobile Computing and Communication Review*, 9(2):4–18, 2005.

[2] P. Bose, P. Morin, and I. Stojmenovic. Routing with guaranteed delivery in ad hoc wireless networks. *Proc. of the 3rd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, pages 48–55, 1999.

[3] S. Chen, G. Fan, and J. Cui. Avoid "void" in geographic routing for data aggregation in sensor networks. *International Journal of Ad Hoc and Ubiquitous Computing*, 1(4):168–178, 2006.

[4] T. Dimitrious and I. Krontiris. GRAViTy: Geographic routing around voids in sensor networks. *International Journal of Pervasive Computing and Communications*, 2(4):351–361, 2006.

[5] Q. Fang, J. Gao, and L. Guibas. Locating and bypassing routing holes in sensor networks. *Proc. of the 23rd IEEE INFOCOM*, pages 2458–2468, 2004.

[6] S. Gasagni, I. Chlamtac, V. Syrotiuk, and B. Woodward. A distance routing effect algorithm for mobility (DREAM). *Proc. of the 4th ACM/IEEE MOBICOM*, pages 76–84, 1998.

[7] Z. Jiang, J. Ma, W. Lou, and J. Wu. An information model for geographic greedy forwarding in wireless ad-hoc sensor networks. *Proc. of the 27th IEEE INFOCOM*, pages 825–833, 2008.

[8] Y. Ko and N. Vaidya. Location-aided routing (LAR) in mobile ad hoc networks. *Proc. of the 4th ACM/IEEE MOBICOM*, pages 66–75, 1998.

[9] M. Li and Y. Liu. Rendered path: Range-free localization in anisotropic sensor networks with holes. *Proc. of the 13th ACM/IEEE MOBICOM*, pages 51–62, 2007.

[10] K. Liu, N. Abu-Ghazaleh, and K. Kang. Location verification and trust management for resilient geographic routing. *Journal of Parallel and Distributed Computing*, 62(2):215–228, 2007.

[11] S. Olariu and I. Stojmenovic. Design guidelines for maximizing lifetime and avoiding energy holes in sensor networks with uniform distribution and uniform reporting. *Proc. of the 25th IEEE INFOCOM*, 2006.