Computer Networks 129 (2017) 232–250

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

# Distributed hole-bypassing protocol in WSNs with constant stretch and load balancing

Phi Le Nguyen[a], Yusheng Ji[a,b,*], Zhi Liu[c], Huy Vu[d], Khanh-Van Nguyen[d]

[a] Department of Informatics, SOKENDAI (The Graduate University for Advanced Studies), 2-1-2 Hitotsubashi, Chiyoda-ku, 101–8430, Tokyo, Japan
[b] National Institute of Informatics, Tokyo, Japan
[c] Global Information and Telecommunication Institute (GITI), Waseda University, Tokyo, Japan
[d] School of Information and Communication Technology, Hanoi University of Science and Technology, Hanoi, Vietnam

ARTICLE INFO

*Article history:*
Received 22 December 2016
Revised 12 September 2017
Accepted 3 October 2017
Available online 4 October 2017

*Keywords:*
Wireless sensor network
Geographic routing
Routing hole
Constant stretch
Load balance

ABSTRACT

Geographic routing has been widely used in wireless sensor networks because of its simplicity and efficiency resulting from its local and stateless nature. However, when subjected to routing holes (i.e., regions without sensor nodes that have communication capability), geographic routing suffers from the so-called *local minimum phenomenon*, where packets are stopped at the hole boundary. This local minimum phenomenon results in problems of *load imbalance* (i.e., a higher traffic intensity around the hole boundary) and *routing path enlargement* due to the long hole detour paths. Although several protocols have been proposed to address these issues, the load imbalance problem has not been solved thoroughly, and none of the existing protocols can solve both of these problems. In this article, we propose a distributed hole-bypassing routing protocol named ACOBA (**A**daptive forbidden area-based **CO**nstant stretch and load **BA**lancing), which can solve the load imbalance problem thoroughly while ensuring the constant stretch property of the routing path. Our theoretical analysis proves that the routing path stretch of the proposed protocol can be controlled to be as small as $1+\epsilon$ (for any predefined $\epsilon > 0$), and the simulation experiments show that our protocol strongly outperforms state-of-the-art protocols in terms of load balancing.



## 1. Introduction

In recent years, wireless sensor networks (WSNs) have been intensively investigated due to their potential in various practical applications [1–3]. Several characteristics of WSNs, such as the limited energy supply, available storage and computational capacity of the sensor nodes[1], distinguish them from other traditional networks as well as pose many challenges to the design of routing protocols.

Geographic routing [4], which works in a distributed manner and exploits the local geographical information of sensor nodes, is widely accepted in WSNs due to its simplicity and efficiency. This type of routing typically assumes that a) each network node knows its own and its neighbors' positions and that b) the source of a message knows the destination's position. Such a routing protocol typically starts with a greedy strategy whereby each node chooses the next hop to be the neighboring node closest to the destination. Geographic routing performs well in networks without routing holes; however, with the occurrence of holes [2], this routing protocol suffers from a serious drawback called the *local minimum phenomenon* [5], i.e., the forwarding process is stopped at the hole boundary because there is no neighboring node closer to the destination than the current node. The traditional scheme for bypassing the hole is to switch off the usual greedy forwarding mode and instead, manage to route packets along the hole boundary [6,7]. However, this approach suffers from the following problems:

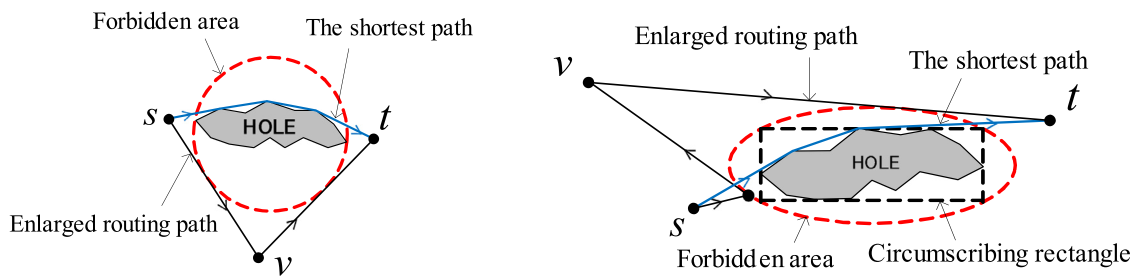
- *Load imbalance*: As a lot of packets will be sent along the hole boundary, the boundary nodes are imposed a heavier traffic than the other nodes. Therefore, the boundary nodes are depleted of energy quickly, and the hole is consequently enlarged.

* Corresponding author.
*E-mail addresses:* nguyenle@nii.ac.jp (P.L. Nguyen), kei@nii.ac.jp (Y. Ji), liuzhi@aoni.waseda.jp (Z. Liu), vannk@soict.hust.edu.vn (K.-V. Nguyen).

[1] In this article, the words node, sensor and sensor node are used interchangeably.

[2] Holes are formed either due to the presence of some geographical obstacles or because of the failure of sensor nodes due to various reasons such as battery depletion or the node being destroyed by external forces (e.g., by fire or earthquake).

https://doi.org/10.1016/j.comnet.2017.10.001
1389-1286/




(a) The forbidden area is a circle ([9]).

(b) The forbidden area is an ellipse ([11]).

**Fig. 1.** Examples of routing path enlargement due to the difference between the hole and the forbidden area.

- *Routing path enlargement*: The path length can grow as much as $\Omega(c^2)$[3] when holes are present, where $c$ is the optimal path length [8].

To address these two problems, several methods have been proposed, wherein a common approach is to approximate the hole by a simple shape. This shape is often a minimum cover of the hole, and is considered as a special *forbidden area* (as we call it) from which the packets are made to stay away. The information of this forbidden area is disseminated to the surrounding area to establish a hole awareness. This hole awareness is then utilized to discover detour routes. In some proposals, the authors use the forbidden area that has a certain selected and simple shape, e.g., a circle [9], a hexagon [10], an ellipse [11] or a quadrilateral [12]. Although these approaches can decrease traffic around the hole boundary, they may create traffic congestion around the perimeter of the forbidden area and thus cannot solve the load imbalance problem thoroughly. Moreover, the routing path enlargement problem remains unsolved because the difference between this forbidden area and the original hole can be quite large. Fig. 1 illustrates the worst cases when the forbidden areas are in the shape of a circle or an ellipse. In a recent approach addressing the path enlargement problem [13,14], a hole is compactly described by a simple polygon, i.e., the smallest convex polygon covering the hole. Although this approach can obtain a constant stretch, it still suffers from the load imbalance problem due to the traffic concentration around the convex polygon. Moreover, this approach may result in extra resource overhead caused by disseminating and storing information of the convex polygon.

In this paper, we propose a novel approach[4] for addressing routing hole. To the best of our knowledge, this is the first approach targeting and solving both load imbalance and routing path enlargement problems simultaneously. The basic idea is to use an adaptive forbidden area, which varies for each packet, instead of only one fixed forbidden area for all packets. These forbidden areas are determined based on *core polygons* (i.e., compact representations of the hole). On the one hand, the diversity of the forbidden areas helps to avoid traffic congestion surrounding the hole and furthermore balances the traffic load over the network. On the other hand, the size of the forbidden area is adjusted to guarantee that the stretch of the routing path (i.e., the ratio between the length of the real routing path and the shortest routing path) does not exceed a predefined threshold. The contributions of this article are as follows:

- We propose a strategy to construct an adaptive forbidden area which can guarantee the constant stretch of the routing paths while maintaining the load balance over the network. We also propose a distributed protocol to determine such forbidden area.
- We propose a distributed geographic routing protocol that generates dynamic routing paths with the stretch upper bounded by a constant. This constant can be controlled to be as small as $1+\epsilon$ ($\epsilon$ is a predefined positive number, which we call the *stretch factor*). The variation of the routing paths ensures the load balance over the network.
- We present an insightful analysis to prove the $(1+\epsilon)$-constant stretch property of our routing protocol.
- We conduct extensive simulations to evaluate the effectiveness of the proposed protocol as well as the impact of the parameters.

The remainder of the article is organized as follows. Section 2 introduces the network model and definitions. We propose the routing protocol in Section 3. Section 4 theoretically analyzes the performance of the protocol, and Section 5 evaluates the protocol using simulations. We further discuss our proposed protocol in Section 6. Section 7 describes additional related works and Section 8 concludes the article.

## 2. Network model and definitions

In this section, we first introduce the network model and then provide notations and definitions used throughout this article.

### 2.1. Network model

We assume that each node knows its position (using GPS or other positioning services [16]) and its 1-hop neighbors (through the neighbor notification packets); in addition, the source node knows the position of the destination node. In this article, we consider networks with only one hole. For theoretical analysis, we make a reasonable assumption that the considered network is sufficiently dense such that there are sensors everywhere apart from the considered hole. Given such an ideal situation, we can model the *geographical greedy routing path* between two given nodes $s$ and $t$ (in the dense area) as *the Euclidean line connecting s and t*. Fig. 2 illustrates such an example. In this figure, $s_1t_1$ does not intersect the hole; the packets from $s_1$ can be greedily directed straightforward toward $t_1$, and thus, this greedy routing path can be modeled by the segment $s_1t_1$. In contrast, $s_2t_2$ intersects the hole, and thus, the packets from $s_2$ are greedily forwarded to $v$ before arriving at $t_2$. Therefore, this routing path from $s_2$ to $t_2$ can be modeled by the broken line $s_2vt_2$.

[3] $\Omega(f(n))$ means that for large enough $n$, $\Omega(f(n)) \geq f(n)$ for some constant $k$.

[4] The initial idea of this approach was presented in our previous work [15], which received the best paper award at ISSNIP'14. However, the existing protocol suffers from some problems which will be described in Section 7.