This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2008 proceedings.

Routing in Outer Space

Alessandro Mei and Julinda Stefa
Department of Computer Science
Sapienza University of Rome, Italy
Email: mei@di.uniroma1.it

***Abstract*—In this paper we consider security-related and energy-efficiency issues in multi-hop wireless networks. We start our work from the observation, known in the literature, that shortest path routing creates congested areas in multi-hop wireless networks. These areas are critical—they generate both security and energy efficiency issues. We attack these problems and set out routing in outer space, a new routing mechanism that transforms any shortest path routing protocol (or an approximated version of it) into a new protocol that, in case of uniform traffic, guarantees that every node of the network is responsible for relaying the same number of messages, on expectation. We can show that a network that uses routing in outer space does not have congested areas, does not have the associated security-related issues and does not encourage selfish positioning.**

***Index Terms*—Multi-hop wireless networks, routing, security, load-balancing, analysis, simulations.**

I. Introduction

During the past years the interest in multi-hop wireless networks has been growing significantly. One of the most representative and important examples of multi-hop wireless networks are wireless sensor networks where small devices equipped with a radio transmitter and a battery are deployed in a geographic area to monitor some desired property like temperature, pressure, or to build an emergency communication infrastructure, etc. (see [1] for a survey).

Due to the limited resources of the nodes, routing on a wireless sensor network is one of the most interesting and complex issues. A lot of work has been done and protocols that use minimal energy are more than valuable in this context. In [2], the authors analyze the impact of shortest path routing in a large multi-hop wireless network deployed onto a disk area and where a uniform traffic pattern is injected. They show that under these assumptions shortest path routing induces congested areas in the network, especially in the network center. The same problem holds for every two-dimensional convex surface. Our experiments show that, when using geographic routing [3] on a network deployed in a square, 25% of the messages are relayed by the nodes in a small central congested region whose area is 3% of the total area of the square.

Congested areas in a wireless sensor network give rise to important security-related issues: If a large number of messages are relayed by the nodes deployed in a relatively small congested region, then jamming becomes a vicious attack. A large geographical area is usually expensive to jam, but jamming a small congested region becomes feasible, cheaper, and effective. In the square, for example, it is enough to jam 3% of the network area to stop 25% of the messages. Moreover, if an attacker has the goal of getting control over as many communications as possible, then it is enough to control 3% of the network nodes to handle 25% of the messages. Note that these problems are not solved by trying to balance the load just locally, as done by a few protocols in the literature (like GEAR [4], for example)—these protocols are useful, they can be used in any case (in our protocols as well), and are efficient in smoothing the energy requirements among neighbors, while they can't do much against congested areas and they don't help to alleviate the above discussed security-related issues.

In this paper we do not consider mobility. However, in a world where energy is an issue and where the node itself can chose it's own position in order to maximize its own advantage, then no node would stay in the highly congested areas of the network. If the nodes are selfish, an uneven distribution of load in the network area leads to an irregular distribution of the nodes. Selfish behavior is a recent concern in the network community and it is rapidly gaining importance [3], [5], [6]. Most of these contributions show how to devise mechanisms such that selfish nodes can't help but truthfully execute the protocol. For the best of our knowledge, here we are raising a new concern that can be important in mobile networks or whenever the position of the node can be an independent and selfish choice.

There are also energy-efficiency issues: Aside from retransmissions, that are costly and, in congested areas, more frequent, the nodes have to relay a much larger number of messages. Therefore the nodes in these areas will die earlier than the other nodes in the network, exacerbating the problem for the neighbors that are still operational. In the long run, this results in holes in the network and in a faster, and less graceful, death of the system. Note that these problems are not solved by balancing the load just locally, as done by a few protocols in the literature (like GEAR [4], [7], for example)—these protocols are useful, they can be used in any case (in our protocols as well), and are efficient in smoothing the energy requirements among neighbors, while they can't do much against congested areas and they don't help to alleviate the above discussed security-related issues.

Solving these issues—security, energy-efficiency and tolerance to (a particular case of) selfish behavior—is an important and non-trivial problem. In this paper we attack this problem

The work presented in this paper was partially funded by the FP7 EU project "SENSEI, Integrating the Physical with the Digital World of the Network of the Future", Grant Agreement Number 215923, www.ict-sensei.org.

978-1-4244-2026-1/08/$25.00 © 2008 IEEE

and set out *routing in outer space*, a new routing mechanism that transforms any shortest path routing protocol (or an approximated version of it) into a new protocol that, in case of uniform traffic, guarantees that every node of the network is responsible for relaying the same number of messages, on expectation As a consequence, the message flow is distributed homogeneously over all the network.

We can show that a network that uses routing in outer space does not have congested areas, and thus does not have the security issues nor does encourage selfish positioning. Our claims are fully supported by experiments. Furthermore, with routing in outer space the load among network nodes is equally balanced. Hence, we are willing to think that this routing protocol brings also significant improvement in energy-efficiency issues.

The rest of the paper is organized as follows: In Section II we present the theoretical idea behind our work, we come up with routing in outer space and prove its mathematical properties; In Section III, after describing our node and network assumptions and our simulation environment, we discuss on on the practical issues related in implementing routing in outer space starting from geographic routing; lastly, we present an extensive set of experiments.

II. Routing in Outer Space

We model the multi-hop wireless network as a undirected graph $G = (V, E)$, where V is the set of the ad-hoc deployed nodes on the network area S and E is the set of edges. Formally, it is enough to assume that S is a metric space with distance d_S and that every node is a point on S. Given two nodes $u, v \in V$ deployed on S, we will denote the distance between their positions on the space with $d_S(u, v)$. The nodes have a transmission range r—two nodes $u, v \in V$ are connected by a wireless link $uv \in E$ if $d_S(u, v) \leq r$, that is, their distance is at most r. The common practice in the literature is to take a convex surface as S, usually a square, a rectangle, or a disk, with the usual Euclidean distance. In this paper we assume that the nodes know their position, either by being equipped with a GPS unit, or by using one of the many localization protocols that have been proposed (see [8] for a survey); and that they know the boundaries of the network area S, this is possible either by pre-loading this information on the nodes before deployment, or by using a protocol like the one in [9], [10].

We started from the observation that shortest path routing on the square, or even an approximate version of it, generates congested areas on the center of the network. We have already discussed that this is not desirable. The same problem is present on the rectangle, the disk, and any two dimensional convex deployment of the network, which is the common case in practice. Here, the idea is to relinquish shortest paths so as to get rid of congested areas, with the goal of improving security and tolerance to selfish behavior of the multi-hop wireless network. As the first step, we have to realize that there do exist metric spaces that do not present the problem. First, we need a formal definition of the key property of the metric space we are looking for.

Definition 1: Consider a multi-hop wireless network deployed on a space S. Fix a node u and choose its position on S arbitrarily. Then, deploy the other nodes of the network uniformly and independently at random. We will say that S is *symmetric* if, chosen two nodes v_1 and v_2 uniformly at random in the network, the probability that u is on the shortest path from v_1 to v_2 does not depend on its position.

Clearly, the disk is not a symmetric space as in the above definition. It has been clearly shown in [2]—if node u is on the center of the circle or nearby, the probability that u is traversed by a message routed along the shortest path from a random source node v_1 to a random destination v_2 is larger than that of a node away from the center of the network area. Clearly, the square has exactly the same problem. This claim is confirmed by our experiments: 25% of the shortest paths traverse a relatively small central disk whose area is 3% of the entire square.

To solve these problems, our idea is to map the network nodes onto a symmetric space (the *outer space*) through a mapping that preserves the initial network properties (such as distribution, number of nodes, and, with some limitations, distances between them). The second step is to route messages through the shortest paths as they are defined on the outer space. When the outer space and the corresponding mapping are clear from the context, we will call these paths the *outer space shortest paths*. Since the outer space is symmetric, we can actually prove that every node in the network has the same probability of being traversed by an outer space shortest path. Now, let's make a step back and proceed formally.

Let S be the original space where the network is deployed, and let T be the outer space, an abstract space we use to describe routes, both metric spaces with respective distances d_S and d_T. We are looking for a mapping function $\phi : S \mapsto T$ with the following properties:

1) if x is a point taken uniformly at random on S, then $\phi(x)$ is also taken uniformly at random on T;
2) for every $r > 0$, and every $u, v \in T$ where $u \neq v$, if $d_T(\phi(u), \phi(v)) \leq r$ then $d_S(u, v) \leq r$.

Property 1 guarantees that a uniform traffic on S is still a uniform traffic when mapped onto T through ϕ, and Property 2 says that paths on T are paths on S, when the nodes are mapped into T using ϕ. Later we will see why these properties are important.

Definition 2: A mapping $\phi : S \mapsto T$ is *fair* if it enjoys Properties 1 and 2.

Once such a fair mapping has been fixed, any message from node u to node v can be routed following a shortest path $\phi(u), \phi(w_1), \phi(w_2) \ldots, \phi(w_h), \phi(v)$ between the images of u and v and through some of the images of the nodes of the network under ϕ on space T. Being ϕ a fair mapping, the path $u, w_1, w_2, \ldots, w_h, v$ is a well defined path on S. Indeed, any two consecutive nodes in the shortest path on T are neighbors in S as well, thanks to Property 2. If T is *symmetric* as in Definition 1, the routing through ϕ would be well distributed

over T, since ϕ has Property 1. Hence, this path can be used to route messages on S, giving as a result a homogeneous distribution of the message flow over all the network.

Theorem 1: Let $\phi : S \mapsto T$ be a mapping from source metric space S to target metric space T. Assume that ϕ is fair and T is symmetric. Fixed a node $u \in S$, deployed the other nodes of the network uniformly at random, and taken a source $v_1 \in S$ and a destination $v_2 \in S$ uniformly at random, the probability that the outer space shortest path from v_1 to v_2 defined by ϕ traverses u is independent of the position of u on S.

The above theorem gives an important hint on how to build a routing protocol on a not symmetric network area, in such a way that the message flow is distributed homogeneously over all the network. What is needed is to determine a symmetric space (the outer space) and a fair mapping for it, and then to "transform" the shortest paths on the original network area into the corresponding outer space shortest paths.

We assume that the original network area is a square of side 1. An excellent candidate as a symmetric outer space is the torus. A *torus* is a 3-dimensional surface that we can model as $T = [0, t] \times [0, t]$. Let u_x and u_y be the coordinates of the position of node u on the torus. We can endow T with the following distance d_T:

$$d_T(u, v) = \sqrt{d_x^2 + d_y^2}, \text{ where} \tag{1}$$

$$d_x = \min\{|u_x - v_x|, t - |u_x - v_x|\}, \text{ and} \tag{2}$$

$$d_y = \min\{|u_y, v_y|, t - |u_y, v_y|\}. \tag{3}$$

The common way to visualize a torus is to consider a square, and then to fold it in such a way that the left side is glued together with the right side, and that the top side is glued together with the bottom side. In the following, we will picture the torus unfolded, just like a square, as it is commonly done to easily see this 3-dimensional surface as a 2-dimensional one.

Fact 1: A torus surface is *symmetric* as in Definition 1.

Clearly, virtually no wireless network in real life is deployed on a torus. Here, we are using the torus just as an abstract space. We are *not* making any unreasonable assumption on the nodes of the network being placed on a torus like area with continuous boundaries, nor are we assuming that the network area becomes suddenly a torus. Indeed, we assume that the real network is deployed on the square, where the nodes close to one side *cannot* communicate with the nodes close to the opposite side. Crucially, the paths used to deliver the messages are computed as they are defined through a fair mapping onto the torus, the outer space. Coming back to our idea, now that the target symmetric outer space has been chosen, what is left to do is to find a fair mapping ϕ_{ST} from the square to the torus.

Let $S = [0, 1] \times [0, 1]$ be a square, and let $T = [0, 2] \times [0, 2]$ be a torus. As the mapping ϕ_{ST} from S to T we propose the following:

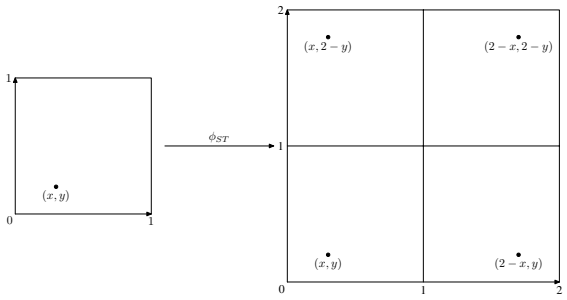


Fig. 1. Example of transformation of a point from the square to the torus through the mapping ϕ_{ST}. Point (x, y) on the square $S = [0, 1] \times [0, 1]$ has four possible and equally probable images on the torus $T = [0, 2] \times [0, 2]$. According on ϕ_{ST}, only one of the images will actually appear on T.

$\phi_{ST}((x, y)) = (x', y')$ where:

$$x' = \begin{cases} x & \text{with probability } 1/2 \\ 2 - x & \text{with probability } 1/2, \end{cases} \text{ and}$$

$$y' = \begin{cases} y & \text{with probability } 1/2 \\ 2 - y & \text{with probability } 1/2. \end{cases}$$

An example of such a mapping can be seen in Figure 1, where a node on the square is mapped to one of the four equally probably images on the torus.

Theorem 2: ϕ_{ST} is a *fair* mapping with probability one.

Proof: The proof of this claim follows directly from the definition of the mapping ϕ_{ST}. The full proof is technical, without adding much to the understanding of this work. Therefore, for the sake of brevity, we omit the details. ■

It is interesting to note that it is *not* true that points that are neighbors on the square are also neighbors on the torus when mapped through ϕ_{ST}. Generally speaking, it is impossible to build a mapping with both this property and Property 2, since the square and the torus are topologically different.

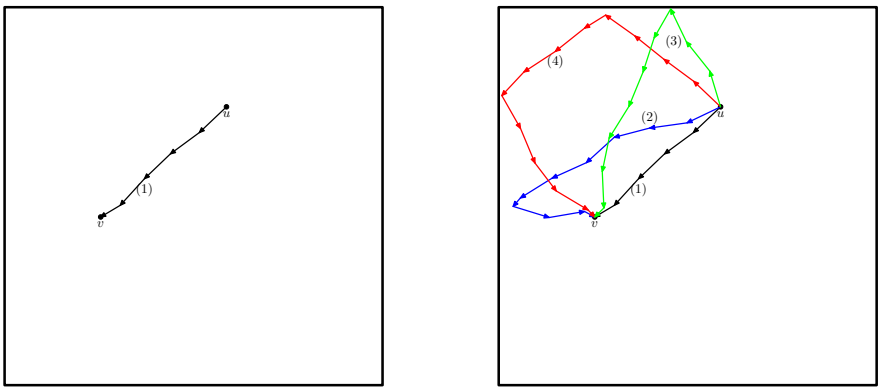
In the following, we will implement our idea in a practical routing protocol derived from geographical routing, and show its performance by means of experiments.

III. Routing in Outer Space in Practice

We start from geographic routing, a simple protocol that, when the network is dense enough, can be shown to approximate shortest path routing quite well [3]. Here, we define *outer space geographic routing*, its outer space counterpart.

In geographic routing, the destination of a message is a geographical position in the network area. Every relay node that is not the destination's neighbor performs a very simple protocol: send the message to the node that is closer to destination. If such a node does not exist, then the message is not delivered. Outer space geographic routing works quite as simply. Every relay node looks at the destination x of the message, and forwards it to the node u that minimizes $d_T(\phi_{ST}(x), \phi_{ST}(u))$. Just like geographic routing, implemented on the outer space.

Take, as an example, a message from node u destined to a geographic position close to node v. According to the



(a) Geographic routing between node u and v.

(b) Four equally probable outer space geographic routings between node u and node v.

Fig. 2. Transformation of a geographic route on the square into four possible outer space geographic routes between nodes u and v. As can be seen, depending on which possible $\phi_{ST}(u)$ and $\phi_{ST}(v)$ images are chosen for u and v on the torus surface, there are four possible outer space geographic routes on the square between u and v. The network is made of $6,441$ nodes.

definition of ϕ_{ST}, each node on the square S has four possible and equally probable images on the torus T. This implies that for each pair u, v of nodes on S there are four possible and equally probable pairs of images $\phi_{ST}(u)$, $\phi_{ST}(v)$ on T[1]. This yields four possible and different outer space geographic routes between the images u and v under ϕ_{ST}. Hence, between any two nodes on the square there is one out of four different and equally probable outer space routes. To see an example of the four routes, see Figure 2.

To implement such a routing, it is enough that the nodes know their position in the square. Then, computing ϕ_{ST} for itself and the neighbors is trivial and fast. Note that it is not really important that the nodes agree on which of the four possible images is actually chosen for any particular node (except for the destination, but the problem can easily be fixed). However, to get this agreement it is enough that every node uses the same pseudo-random number generator, seeded with the id of the node being mapped.

A. Node and Network Properties, Assumptions, and Simulation Environment

For the experiments we have used our own event-based simulator whose behavior reflects exactly the assumptions and properties we have made and that are listed here below.

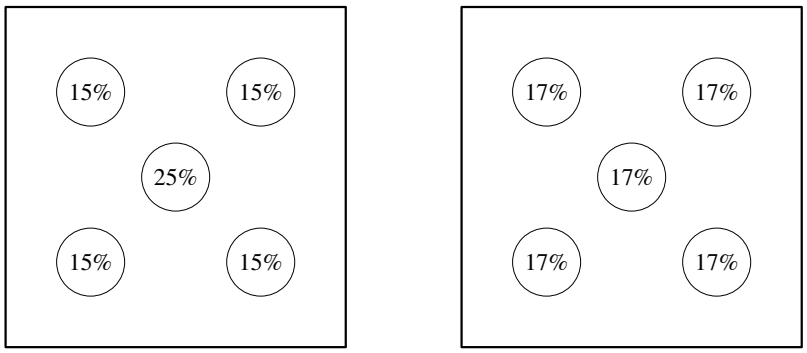
We model our network node as a sensor. A typical example can be the Mica2DOT node (outdoor range 150m, 3V coin cell battery) widely used in academic research. We use in our experiments networks with up to 10,000 nodes, distributed on a square of side $1,500$m. In the following, we will assume for the sake of simplicity that the side of the square is 1, and that the node transmission range is 0.1. The nodes are placed according to a Poisson distribution with density ρ, chosen in such a way that every node has 30–40 neighbors on average.

We inject a *uniform traffic* [2] in the network—every message has a random source and a random destination uniformly and independently chosen. We assume that the nodes know their position on the network area: They can get the absolute position either in hardware, by using a GPS (Global Positioning System), or in software using one of the location systems proposed in the literature (see [8] for a survey on these systems). Once the absolute position is known, we can get the nodes to know their relative position within the square by preloading the information on the deployment area, or by using one of the several techniques for boundary detection based on geometry methods, statistical methods, and topological methods like in [9], [10].

[1]Actually, there are 16 possible and equiprobable such couples up to isomorphism, which fall into 4 different classes of symmetry.

B. Security-Related Experiments

In these experiments, we measure the number of messages whose routing path traverses five sub-areas of the same size in the network area. Every sub-area is a circle of radius 0.1 (incidentally, the same of the transmission radius of a network node), that corresponds to an area of 3.14% of the whole network surface. The sub-areas are centered in some "crucial" points of the network area: The center and the middle-half-diagonals points. The center of the network is known to be the most congested area. We want to test whether the middle-half-diagonal centered areas handle a significantly smaller number of messages. More specifically we consider the sub-areas centered in the points of coordinates $(0.5, 0.5)$, $(0.25, 0.25)$, $(0.25, 0.75)$, $(0.75, 0.25)$, $(0.75, 0.75)$, assuming a square of side one. Our experiments are done on networks with different number of nodes (from 1,000 to 10,000). For each network we have launched both geographic routing and outer space geographic routing on message sets of different cardinality (from $50,000$ to $1,000,000$ of messages, generated as an instance of uniform traffic). In Figure 3 we present the average of the results obtained with a network of $1,336$ nodes generated by a Poisson process, but we stress out that exactly the same results are obtained for networks with up to $10,000$ nodes. As it can be seen, the experiments fully support the findings in [2]. Geographic routing (see Figure 3(a))



(a) Geographic routing. (b) Outer space geographic routing.

Fig. 3. The average fraction of the messages whose routing path traverses the selected sub-areas of a network of $1,336$ nodes, in the case of geographic routing and in the case of outer space geographic routing.

concentrates a relevant fraction of the messages on a small central area of the network, while the other sub-areas handle on average little more than the half. We have already discussed why this is dangerous, and important to avoid.

Figure 3(b) shows the result with the same set of messages and the same network deployment, this time using outer space geographic routing. The message load in the central sub-area is 32% lower compared with the load of the same sub-area in the case of the geographic routing. Outer space geographic routing seems to transform the network area in a symmetric surface, making sure that the number of message handled by all the sub-areas remains reasonably low, 17%, and equally distributed. As a result, the load among network nodes is equally balanced and there are no "over-loaded" areas. This network is intuitively stronger than the same network using geographic routing, there are no areas that are clearly more rewarding as objective of a malicious attack, and no network areas have more "responsibilities" than others.

Furthermore, Figure 3(a) clearly shows that, with geographic routing, it is not a good strategy to stay in the center of the network if you want to save your battery. If the nodes are selfish, it is a much better strategy to position in one of the sub-central areas, for example, where the battery is going to last 66% longer. Even better if you move toward the side of the square. Conversely, when using outer space geographic routing, there is no advantage in choosing one position or the other, which is exactly our goal to guarantee an even distribution of the nodes, although part of them are selfish.

IV. Conclusions

Uniform traffic injected into multi-hop wireless networks generates congested areas. These areas carry a number of non-trivial issues about security, energy-efficiency, and tolerance to (a particular case of) selfish behavior. In this paper we describe routing in outer space, a mechanism to transform shortest path routing protocols into new protocols that do not have the above mentioned problems.

Routing in outer space guarantees that every node of the network is responsible for relaying the same number of messages, on expectation. Hence, the message flow is homogeneously distributed over all the network area.

We can show that a network that uses routing in outer space does not have congested areas, does not have the associated security-related issues and does not encourage selfish positioning. Furthermore, with routing in outer space the load among network nodes is equally balanced, by giving us the intuition that this routing protocol brings also significant improvement in energy-efficiency issues.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communcations Magazine*, vol. 40, pp. 102–114, August 2002.

[2] S. Kwon and N. B. Shroff, "Paradox of shortest path routing for large multi-hop wireless networks," in *IEEE INFOCOM'07 Anchorage*, May 2007.

[3] B. Karp and H. T. Kung, "Gpsr: Greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '00)*, Boston, MA, USA, August 2000.

[4] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks," UCLA Computer Science Department, Tech. Rep. UCLA/CSD-TR-01-0023, May 2001. [Online]. Available: citeseer.ist.psu.edu/yu01geographical.html

[5] V. Srinivasan, P. Neggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc wireless networks," in *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, 2003.

[6] W. Wang, X. Li, and Y. Wang, "Truthful multicast routing in selfish wireless networks," in *Proceedings of the 10th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '04)*, Philadelphia, PA, USA, September 2004.

[7] M. Zorzi and R. R. Rao, "Geographic random forwarding (geraf) for ad hoc and sensor networks: Energy and latency performance," *IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp. 349–365, 2003.

[8] J. Hightower and G. Borriello, "Location systems for ubiquitous computing," *IEEE Computer*, vol. 34, no. 8, pp. 57–66, August 2001.

[9] A. Kröller, S. P. Fekete, D. Pfisterer, and S. Fischer, "Deterministic boundary recognition and topology extraction for large sensor networks," in *SODA '06: Proceedings of the seventeenth annual ACM-SIAM symposium on Discrete algorithm*. New York, NY, USA: ACM Press, 2006, pp. 1000–1009.

[10] Y. Wang, J. Gao, and J. S. Mitchell, "Boundary recognition in sensor networks by topological methods," in *MobiCom '06: Proceedings of the 12th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM Press, 2006, pp. 122–133.