Routing in Outer Space: Fair Traffic Load in Multihop Wireless Networks

Alessandro Mei, *Member*, *IEEE*, and Julinda Stefa, *Student Member*, *IEEE*

Abstract—In this paper, we consider security-related and energy efficiency issues in multihop wireless networks. We start our work from the observation, known in the literature, that shortest path routing creates congested areas in multihop 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 approximated versions of it) into a new protocol that does not create congested areas, does not have the associated security-related issues, and does not encourage selfish positioning. Moreover, the network is more energy efficient than the same network using the original routing protocol (in spite of using more energy globally) and dies more gracefully. We also describe applications of our idea to mobility and to a security protocol for the detection of node replication attacks.

Index Terms—Multihop wireless networks, routing, analysis, energy efficiency, load balancing, simulations.

1 Introduction

During the past years, the interest in multihop wireless networks has been growing significantly. These networks have an important functionality, that is, the possibility to use other nodes as relays in order to deliver messages and data from sources to destinations. This functionality makes multihop wireless networks not only scalable but also usable in various areas and contexts. One of the most representative and important examples of multihop wireless networks is wireless sensor networks, where small devices equipped with a radio transmitter and a battery are deployed in an geographic area for monitoring or measuring of some desired property like temperature, pressure, or others [1], [24]. Routing in a multihop wireless network is one of the most interesting and difficult issues to solve due to the limited resources and capacities of the nodes. Protocols that use less information possible and need minimal energy consumption of nodes have become more than valuable in this context.

Much research work has been devoted to finding energy efficient routing protocols for multihop wireless networks. Often, these protocols tend to find an approximation of the shortest path between the source and destination of the message, where shortest path is measured in number of hops. In [23], the authors analyze the impact of shortest path routing in a large multihop wireless network. They show that relay traffic induces congested areas. If the traffic pattern is uniform, i.e., every message has a random source and a random destination uniformly and independently chosen, and the network area is a disk, then the nodes at the center of the disk have to relay much more messages than the other nodes.

We have the same problem if the network area is a square, or a rectangle, or any other two-dimensional convex surface. Our experiments show that, when using geographic routing [21] on a network deployed in a square, 25 percent of the messages are relayed by the nodes in a small central congested region whose area is 3 percent of the total area of the square.

Congested areas are bad for a number of important reasons. They raise security-related issues: If a large number of messages are relayed by the nodes deployed in a relatively small congested region, then jamming can be a vicious attack. It is usually expensive to jam a large geographical area, it is much cheaper and effective to jam a small congested region. In the square, for example, it is enough to jam 3 percent of the network area to stop 25 percent 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 percent of the network nodes to handle 25 percent of the messages.

There are also energy efficiency issues: Aside from retransmissions, which 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 nodes in the same area 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 trying to balance the load just locally, as done by a few protocols in the literature (like GEAR [43])—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, but they cannot do much against congested areas and they do not help alleviate the above discussed security-related issues.

• *The authors are with the Department of Computer Science, Sapienza University of Rome, Via Salaria 113-terzo piano, 00198 Rome, Italy. E-mail: {mei, stefa}@di.uniroma1.it.*

Manuscript received 22 May 2008; revised 27 Nov. 2008; accepted 9 Dec. 2008; published online 9 Jan. 2009.
Recommended for acceptance by S. Nikoletseas.
For information on obtaining reprints of this article, please send e-mail to: tc@computer.org, and reference IEEECS Log Number TC-2008-05-0222.
Digital Object Identifier no. 10.1109/TC.2009.17.

Last, there may be other concerns in the contexts where the nodes are carried by individual independent entities. In this paper, we do not consider mobility. However, if the position of the node can be chosen by the node in such a way to maximize its own advantage, and if energy is an issue, then every node would stay close to the border, where it can get the same services without having to relay other nodes' messages. If the nodes are selfish, an uneven distribution of the load in the network area leads to an irregular distribution of the nodes—there is no point in positioning in the place where the battery is going to last the shortest. Selfish behavior is a recent concern in the networking community and it is rapidly gaining importance. Most mechanisms proposed in the literature [21], [38], [39] can be used to force selfish nodes to execute the protocol truthfully, wherever they are positioned, but they do not help in preventing selfish positioning or moving. 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, like in networks of individuals (e.g., students in a university campus network).

Solving these issues—security, energy efficiency, and tolerance to (a particular case of) selfish behavior—is an important and nontrivial problem, and, at least partially, our goal. In this paper, we attack this problem and set out *routing in outer space*, a new routing mechanism that transforms any shortest path routing protocol (or approximated versions of it) into a new protocol that, in case of uniform traffic, guarantees that the network does not have congested areas, does not have the associated security issues, and, in spite of using more energy globally, lives longer than the same network using the original routing protocol—that is, it is more energy efficient. We support our claims by showing routing in outer space based on geographic routing and by performing a large set of experiments.

The rest of the paper is organized as follows: In Section 2, we report on the relevant literature in this area; in Section 3, we present the theoretical idea behind our work, we come up with routing in outer space and prove its mathematical properties; in Section 4, after describing our node and network assumptions and our simulation environment, we discuss on the practical issues related to implementing routing in outer space starting from geographic routing; then, we present an extensive set of experiments fully supporting our claims; lastly, in Section 5, we describe a few applications of routing in outer space to mobility and to a security protocol for the detection of node replication attacks.

2 Related Work

Routing in multihop wireless networks is one of most important, interesting, and challenging problems due to network device limitations and network dynamics. As a matter of fact, this is one of the most studied topics in this area and the literature on routing protocols for multihop wireless networks is vast. There have been proposed protocols that maintain routes continuously (based on distance vector) [28], [44], [35], create routes on-demand [20], [26], [29], or a hybrid [15]. For a good survey and comparison, see [7], [34]. Other examples of routing protocols for multihop wireless networks are those based on link-state like OLSR [19], and others.

Geographic routing or position-based routing, where nodes locally decide the next relay based on information obtained through some Global Positioning System (GPS) or other location determination techniques [16], seems to be one of the most feasible and studied approach. Examples of research work on this approach are protocols like GEAR [43], GAF [42], and localization error-resilient version of geographic routing [2]. For a good starting survey, see [37].

All these protocols try to approximate the shortest path between source and destination over the network. In [30], the authors analytically study the impact of shortest single-path routing on node traffic load by approximating single paths to line segments, and show that multipath routing, although introducing a larger overhead, provides better congestion and traffic balancing. Further work in the same direction [13] shows that multipath routing can balance load only if a very high number of paths is used. In [23], the authors analyze the load for a homogeneous multihop wireless network for the case of straight line routing. Assuming uniform traffic, it is proven that relays induce so-called hot spots or congested areas in the network. Of course, geographic routing (which, in dense networks, approximates the shortest path between source and destination) also suffers from the same problems.

The problem of reducing congestion at the center of a network deployed in a disk in the case of uniform traffic has been considered in [18]. The authors consider a number of possible heuristics like selecting routes along inner and outer radii and switching between them at a random point, moving between the radii linearly, and so on. Later, and independently of this work, the same issues are addressed in [31]. The authors present a theoretical approach to solve the problem showing that an optimum routing scheme based on shortest paths can be expressed in terms of geometric optics and computed by linear programming. Being the optimal trajectories, they find not expressible by closed form formulas, hence not applicable in practice, they also present a practical solution that approximates the optimum. This solution is shown to be implementable and close to the optimum in the case of the disk, while its performance is not as good in the case of the square. In particular, routing in outer space has a better reported decrease of the central load and provides other interesting properties, like independence of the load of the node's position.

A lot of work has been done regarding energy efficiency issues and several approaches try to solve the problem locally, like [43], [47], [9]. These approaches are useful to balance the load reactively and to smooth the energy level among neighbors, while they cannot remove congested areas. These solutions can be used in routing in outer space as well to get locally a smoother load among neighbors.

3 Routing in Outer Space

We model the multihop wireless network as an undirected graph $G = (V, E)$, where V is the set of nodes and E is the set of edges. The nodes are ad-hoc deployed on the network area S. 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 by $d_S(u, v)$. 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 [8], [36], and that they know the boundaries of the network area S; this is possible either by preloading this information on the nodes before deployment or by using one of the protocols in [12], [22], [40].

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 phenomenon is not desirable. The same problem is present on the rectangle, on the disk, and on any two-dimensional convex deployment of the network, which is the common case in practice. Our idea is to get rid of congested areas by relinquishing shortest paths. 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 multihop 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 [23]—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 percent of the shortest paths traverse a relatively small central disk whose area is 3 percent 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). Note that there is no need that the mapping be continuous (actually, restricting to continuous mappings would make our idea lose most of its interest). 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, on average. In the following section, we will see that, based on this idea, we can design practical routing protocols that do not have highly congested areas. Furthermore, the routing protocol that we will present prolongs considerably the network lifetime. Now, let us take 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 u is a point taken uniformly at random on S, then $\phi(u)$ is also taken uniformly at random on T.
2. For every $r > 0$, $u, v \in S$, $u \neq v$, 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 between the images of u and v and through the images of some of the network nodes under ϕ on space T. Let $\phi(u), \phi(w_1), \phi(w_2), \ldots, \phi(w_h), \phi(v)$ be such a path. 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, due to Property 2. If T is *symmetric* as in Definition 1, the routing through ϕ will 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 original network area.

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 shows 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 2D manifold in 3D 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:

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

where

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

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

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 space in 2D.

Fact 1. *A torus 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 physically 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 $T = [0,2] \times [0,2]$ be a torus. We propose to define ϕ_{ST} as follows: $\phi_{ST}((x,y)) = (x',y')$, where

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

and

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

Even though ϕ_{ST} is partly probabilistic, this does not mean that routing in outer space is a *random* routing scheme, like sending the packet along a Brownian path or like sending the packet to a random intermediate (an idea that has been used a lot in routing in parallel architectures and, later, also in network routing). Indeed, it is pretty easy to come up with a very similar completely deterministic version of ϕ_{ST} with exactly the same properties, for our purposes. This deterministic version, however, is more complex to describe and to deal with, and this is the sole motivation to choose a partly probabilistic, and technically simpler, version.

An example of ϕ_{ST} can be seen in Fig. 1, where a node on the square is mapped to one of the four equally probable images on the torus.

Theorem 2. *ϕ_{ST} is a fair mapping.*

Proof. We show that ϕ_{ST} has both Properties 1 and 2. Let $F \subset S$ be equal to $\{(x,y) | (x = 0 \vee x = 1 \vee y = 0 \vee y = 1\}$. Set F is the set of the points on the borders of the four quadrants shown in the torus of Fig. 1. Since F is a measure-zero set, we can prove Property 1 in $T \setminus F$ without loss of generality.

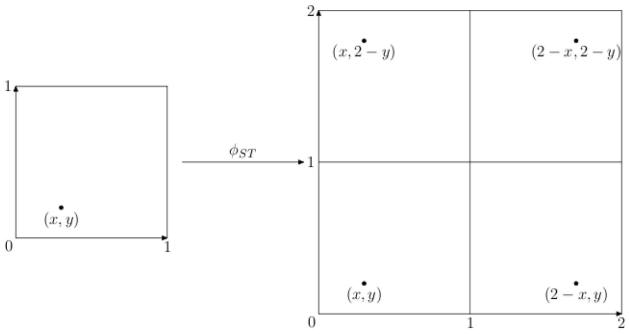


Fig. 1. Example of mapping a point from the square to the torus through ϕ_{ST}. Point (x,y) on the square $S = [0,1] \times [0,1]$ has four possible and equally probable images on the torus $T = [0,2] \times [0,2]$. According to ϕ_{ST}, only one of the images will actually appear on T.

Consider a point $z \in T \setminus F$. Point z lies in one of the four quadrants of the torus shown in Fig. 1—it cannot be on the border. Therefore, it is possible to find $\varepsilon > 0$ small enough, for which, the ball $B(z,\varepsilon)$ with center z and radius ε is completely contained in the same quadrant. To prove Property 1, we need to show that, if we take u uniformly at random in S, then the probability that $\phi_{ST}(u) \in B(z,\varepsilon)$ is $\varepsilon^2\pi/4$, just proportional to the area of $B(z,\varepsilon)$ in $T \setminus F$ (recall that the area of $T \setminus F$ is 4). This shows that $\phi_{ST}(u)$ is taken uniformly at random as well.

Assume that point z lies in the quadrant on the upper-right corner. The probability that $\phi_{ST}(u) \in B(z,\varepsilon)$ is equal to the probability that u is chosen in $B(z',\varepsilon) \subset S$, where $z'_x = 2 - z_x$ and $z'_y = 2 - z_y$, and that ϕ_{ST} maps u to the quadrant on the upper-right corner. The first event happens with probability $\varepsilon^2\pi$, since u is taken uniformly at random in S, $B(z',\varepsilon) \subset S$ has area $\varepsilon^2\pi$, and S has area 1. The second event happens with probability $1/4$. The two events are independent, and therefore, the probability that $\phi_{ST}(u) \in B(z,\varepsilon)$ is equal to $\varepsilon^2\pi/4$, as claimed. The case when z lies in one of the other three quadrants can be dealt similarly.

To show Property 2, we can prove it separately for each axis. We can prove the following: Let $r \in \mathbb{R}$, $r > 0$, and let $u, v \in S$, $u \neq v$. If $d^x_T(\phi(u),\phi(v)) \leq r$, then $d^x_S(u,v) \leq r$, where d^x denotes the distance along the x-axis. If ϕ_{ST} makes the same random choice for both u and v (that is, either both x-coordinates are not changed or both are reflected), then the claim is just trivial. Assume that ϕ_{ST} does not make the same random choice for both u and v. For example, say that ϕ_{ST} does not change the x-coordinate of u and reflects the x-coordinate of v. That is, $\phi^x_{ST}(u) = u_x$ and $\phi^x_{ST}(v) = 2 - v_x$, where ϕ^x_{ST} is the projection of ϕ_{ST} along the x-axis. If $d^x_T(\phi(u),\phi(v)) \leq r$, then either $|(2 - v_x) - u_x| \leq r$ or $2 - |(2 - v_x) - u_x| \leq r$. In both cases, it is easy to show by elementary algebra that $d^x_S(u,v) \leq r$, as claimed. Exactly in the same way, we can see that the claim holds for the y-axis. Therefore, Property 2 holds as well. □

It is interesting to note that even if two points are neighbors on the square, they might not be 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.

The outer space shortest path between two nodes may be different from the corresponding shortest path. Clearly, it cannot be shorter by the definition of shortest path on S. A natural question to ask is whether we can bound the stretch, that is, how much longer may the outer space shortest path be compared with the corresponding shortest path? Unfortunately, the answer is that the stretch cannot be bounded by a constant. However, quite surprisingly, we can prove a very good constant bound in the case when many messages are sent through the network, which is the common case in practice. Indeed, while in the worst case, the stretch can be high, it is not on average if we assume a uniform traffic. This claim is formalized in the following theorem, where we show that, on expectation, the distance of the images under ϕ_{ST} of two nodes taken uniformly and independently at random is at most the double of the original distance.

Theorem 3. *If nodes u, v are taken uniformly at random on the square $S = [0,1] \times [0,1]$, and $\phi_{ST}(u), \phi_{ST}(v)$ are their respective images under ϕ_{ST} on the torus $T = [0,2] \times [0,2]$, then*

$$E[d_T(\phi_{ST}(u), \phi_{ST}(v))] \leq 2E[d_S(u,v)].$$

Proof. Let $u, v \in S$ be two nodes whose position is taken uniformly at random and let $E[d_S(u,v)] = \mu$ be the expectation of their distance on S. Since ϕ_{ST} is fair, also $\phi_{ST}(u)$ and $\phi_{ST}(v)$ are taken uniformly at random in the torus. Clearly, the distance between $\phi_{ST}(u)$ and $\phi_{ST}(v)$ on the torus cannot be larger of the distance of $\phi_{ST}(u)$ and $\phi_{ST}(v)$ on a square $S' = [0,2] \times [0,2]$. Indeed, every path on the torus is also a path on the square (the opposite is not true); and the average distance of two random points in a square of edge two is the double of the average distance of two random points in a square of edge one. Therefore,

$$\begin{aligned} E[d_T(\phi_{ST}(u), \phi_{ST}(v))] &\leq E[d_{S'}(\phi_{ST}(u), \phi_{ST}(v))] \\ &= 2E[d_S(u,v)] \\ &= 2\mu. \end{aligned}$$

□

In the following, we will see with experiments that the actual average stretch is even smaller.

Of course, it is always possible to use the outer space shortest path only when the stretch of that particular path is small, and to use the classical shortest path when the stretch is high and the outer space shortest path is going to cost a lot more. However, we do not perform this kind of optimizations—even though they may reduce the global energy required by the network to deliver the messages, they also unbalance the load among the nodes. Therefore, we want to consider routing in outer space in its cleanest version. 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.

4 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 [21]. 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—in the square in our case. Every relay node 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 delivered. If the network is dense, every message is delivered to the node closest to destination. It is known that this simple version of geographic routing sometimes is not able to deliver the message to the node closest to destination, and there are plenty of ways to overcome this problem in the literature. However, we do not consider these extensions (outer space geographic routing could as well be based on these more complex and complete versions), since the increased complexity does not add much to this work.

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 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. (Actually, there are 16 possible and equiprobable such couples, which fall into four different classes of symmetry up to isomorphism.) 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 Fig. 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 for every node, it is enough to compute ϕ_{ST} by using the same pseudorandom number generator, seeded with the id of the node being mapped.

Note that the mapping makes the graph of the network sparser as neighbors in the original network may not be neighbors in the outer space. Thus, greedy forwarding may have a higher chance to get stuck at a dead end. Whenever this is a problem, we can implement the protocol by assuming that all of the four images of every node are present in the outer space, simultaneously. In this way, the network does not lose density while all the benefits of routing in outer space are preserved. This is what we have done in all of the experiments.

4.1 Node and Network Properties, Assumptions, and Simulation Environment

We model our network node as a sensor. An example can be the Mica2DOT node (outdoor range 150 m, 3 V coin cell battery). These nodes have been widely used in sensor network academic research and in real testbeds. We use

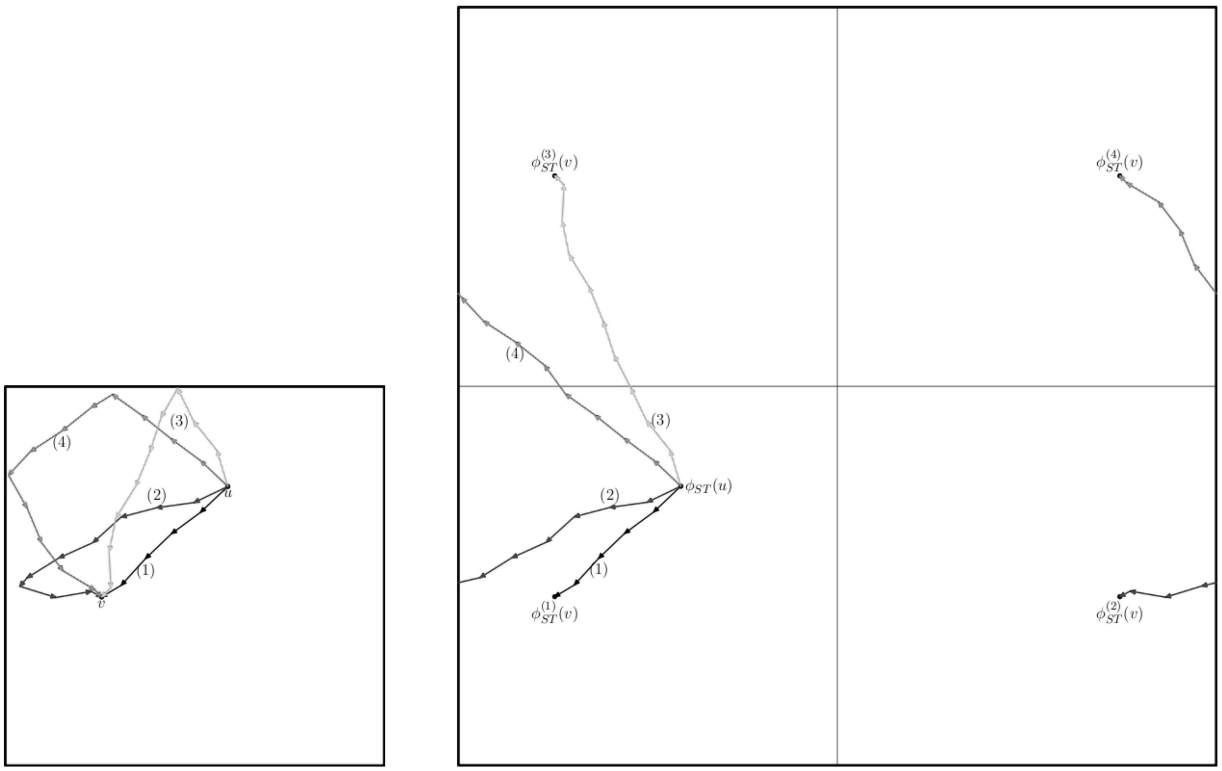


Fig. 2. Assume, without loss of generality, that $\phi_{ST}(u)$ is fixed. (b) The four equiprobable shortest paths from $\phi_{ST}(u)$ to the four possible $\phi_{ST}(v)$. (a) The corresponding four equiprobable outer space shortest paths. Path 1 is just the traditional geographic routing between u and v. The network used to build this example is made of 6,441 nodes. (If you choose another image for $\phi_{ST}(u)$, the shortest paths are moved in the torus without changing the corresponding outer space shortest paths.) Four equally probable outer space geographic routings between node u and node v. (b) Four equally probable outer space geographic routings between one of the possible image of node $u, \phi_{ST}(u)$, and the four possible images of $v, \phi_{ST}^{(1)}(v), \ldots, \phi_{ST}^{(4)}(v)$.

these devices for our experiments as a well-known energy model. However, we expect that the results are meaningful for ad hoc networks based on other devices as well, after proper scaling.

For our experiments, we have considered networks with up to 10,000 nodes, distributed using a Poisson process 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.

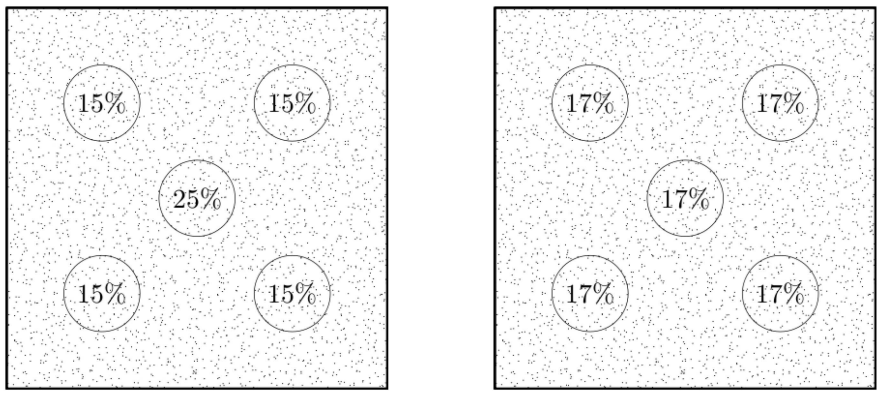
We inject a *uniform traffic* in the network—every message has a random source and a random destination uniformly and independently chosen. This type of traffic distribution is highly used in network simulations, for example, when the goal is to study network capacity limits, optimal routing, and security properties [14], [45], [17]. We assume that the nodes know their position on the network area. Therefore, they need to know both their absolute position and their position within the square. The nodes can get the absolute position either in hardware, by using a GPS, or in software. There exist several techniques for location sensing like those based on proximity or triangulation using different types of signals like radio, infrared acoustic, etc. Based on these techniques, several location systems have been proposed in the literature like infrastructure-based localization systems [41], [32] and ad hoc localization systems [8], [36]. In [16], you can find a survey on these systems, while in [33], the authors present NoGeo: A location system that permits routing based on virtual positions of nodes.

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 (see [12], [22], [40]).

In the next two sections, we present the results of the experiments we have performed, comparing our routing scheme with geographic routing over the same networks and with the same set of messages to route. For the experiments, we have used our own event-based simulator. The assumptions and the network properties listed above have been exactly reflected in the behavior of the simulator.

4.2 Security-Related Experiments

In these experiments, we measure the number of messages whose routing path traverses five subareas of the same size in the network area. Every subarea is a circle of radius 0.1 (incidentally, the same of the transmission radius of a network node), which corresponds to an area of 3.14 percent of the whole network surface. The subareas 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



(a) (b)

Fig. 3. The average fraction of the messages whose routing path traverses the selected subareas of a network of 1,336 nodes, in the case of (a) geographic routing and (b) outer space geographic routing.

significantly smaller number of messages. More specifically, we consider the subareas 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 run both geographic routing and outer space geographic routing on message sets of different cardinality (from 50,000 to 1,000,000 messages, generated as an instance of uniform traffic). In Fig. 3, we present the average of the results obtained with a network of 1,336 nodes generated by a Poisson process, but we stress 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 [23]. Geographic routing (see Fig. 3a) concentrates a relevant fraction of the messages on a small central area of the network, while the other subareas handle, on average, little more than the half. We have already discussed why this is dangerous and important to avoid. Fig. 3b 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 subarea is 32 percent lower compared with the load of the same subarea 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 subareas remains reasonably low, 17 percent, and equally distributed. As a result, the load among the network nodes is equally balanced and there are no "overloaded" areas. This network is intuitively stronger—there are no areas that are clearly more rewarding as objective of a malicious attack, and no areas that have more "responsibilities" than others.

Furthermore, Fig. 3a 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 subcentral areas, for example, where the battery is going to last 66 percent longer. Even better if you move toward one of the corners of the square, where there is virtually no traffic to relay. Conversely, when using outer space geographic routing, there is no advantage in choosing any particular position, since the relay traffic is equally distributed everywhere.

4.3 How to Live Longer by Consuming More Energy

In this section, we present the experiments related to energy efficiency. What Theorem 3 says in a sentence is that the paths used by outer space geographic routing are on average (at most) twice as long as the paths used by geographic routing. This should have an immediate consequence on energy consumption: Messages routed with outer space geographic routing should make the network nodes consume more energy, up to twice as much. And actually it is so. What it turns out with our experiments is that using routing in outer space, the average path stretch is 1.34. Even though this translates into a 34 percent larger global energy consumption, we will see that, in addition to better security and absence of congested areas, the network has also excellent benefits from an energy efficiency point of view when using routing in outer space.

Fig. 4 shows the global energy used by a network of 1,625 nodes, with both geographic routing and outer space geographic routing. We have done more experiments with

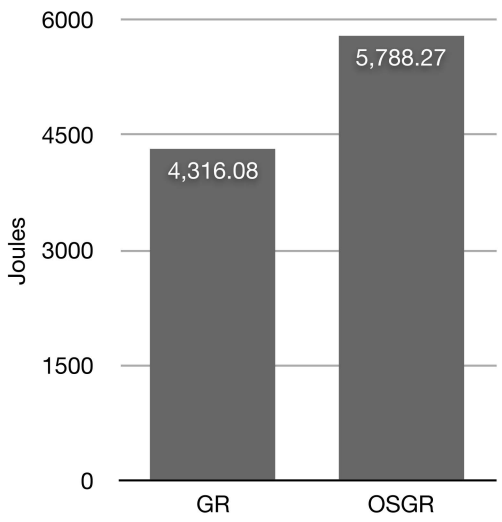


Fig. 4. Global energy consumption of the network after running geographic routing (GR) and outer space geographic routing (OSGR) on sets of 50,000 messages each. The network is made of 1,625 nodes.

different network sizes, up to 10,000 nodes, and the result does not change.

Usually, when a wireless network consumes more energy, its life is shorter. However, it is not always the case. Sometimes, it is better to consume more energy if this is done more equally in the network. This is exactly what happens with outer space geographic routing. We consider four measures of network longevity: time to first node death, time to loss of efficiency in message delivery, time to loss of network area coverage, and time to network disconnection. These measures are well known, used in the literature [4], [5], [46], and collectively cover most of the concerns related to network lifetime. We have made four sets of experiments, each using one of the above ways to measure the longevity of the network. In each of the experiments, we count the number of messages that are successfully delivered before network "death," where network death is defined according to each of the above four measures.

The first set of experiments is done according to the first measure. We have generated a network, a uniform traffic, and injected the traffic into two copies of the same network, one using geographic routing and one using outer space geographic routing. These have been iterated several times with networks of different sizes. The result is shown in Fig. 5a, where we show the number of messages delivered, on average, by a network of 1,625 nodes (the result does not change by considering network of different size), using both routing protocols.

As you can see, the network lifetime when using outer space geographic routing is 29.17 percent longer, on average, than geographic routing. As a matter of fact, the number of messages successfully delivered by the network until the very first node death is much larger with routing in outer space. Fig. 5b shows the result we get when considering the second definition of network lifetime. In this case, we consider the network dead when it is not efficient any more in delivering messages. Note that geographic routing (and similarly its outer space version) has the problem of "dead ends," places where the message cannot proceed because there is no node closer to destination, while the destination is still far. There are a number of solutions to this problem (see, for example, [9]), and there do exist more sophisticated versions of geographic routing that know how to deliver a message whenever there is a path between source and destination. These solutions can be used both by geographic routing and by outer space geographic routing. However, when the network is not able any longer to deliver messages without these sophisticated add-ons, that means that the network is deteriorated. We use this as a measure of the quality of its structure. In this set of experiments, we count the number of messages that reach destination until the success ratio of message delivery falls under some threshold (in our case 95 percent). As it can be seen in the figure, also in this case, outer space geographic routing wins and prolongs the life of the network by 12.54 percent on average.

The third set of experiments is related to area coverage. One of the main application scenarios of sensor networks is the monitoring of some area of interest. In such applications, a must in terms of network properties is the fact that the area of interest has to be fully covered by the network sensing

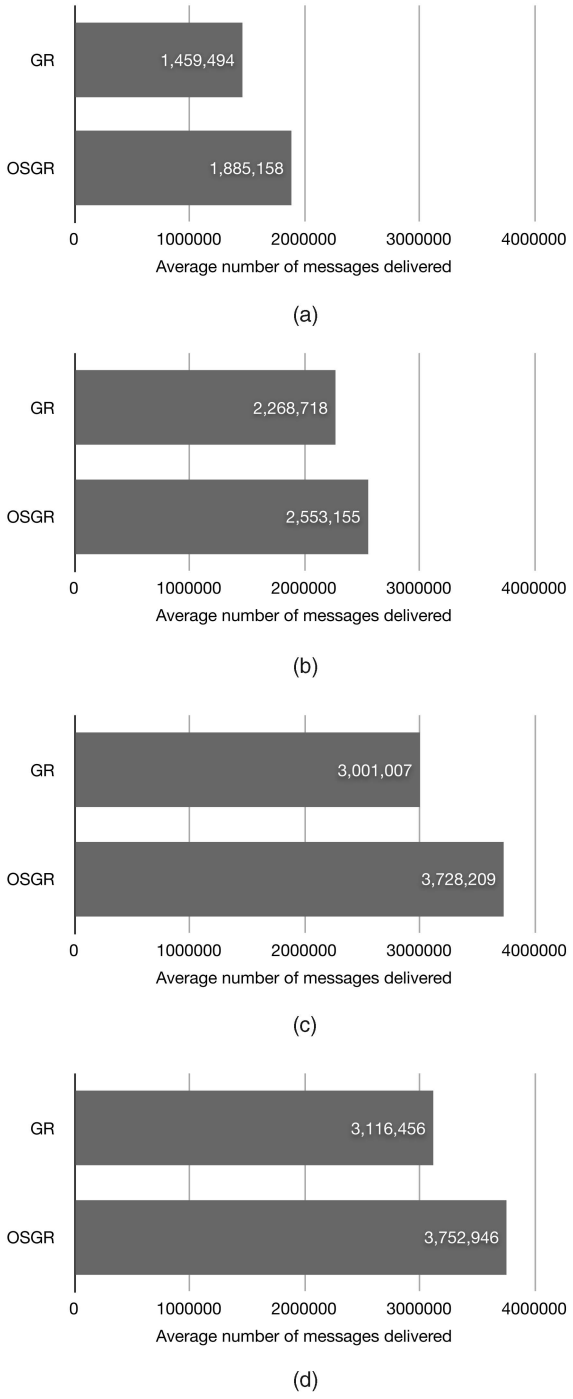


Fig. 5. The time is measured as the number of messages delivered to destination before the death of the first node. The network consists of 1,625 nodes. GR stands for geographic routing while OSGR stands for outer space geographic routing. (a) Time to first node death. (b) Time to loss of efficiency in message delivery. (c) Time to loss of area coverage. (d) Time to network disconnection.

power. Of course, as long as the nodes begin to die, achieving this task becomes more and more difficult. We have performed our experiments assuming that sensing radius is 0.1, just like transmission radius. Again, outer space geographic routing is better and guarantees area coverage much longer. From Fig. 5c, you can see that routing in outer space increases network lifetime of 24.23 percent when considering coverage.

Last, the fourth set of experiments considers network lifetime until network disconnection. Note that connectivity is one of the most important network properties, and that it is *different* from network coverage. Also in this case, outer space geographic routing wins over geographic routing. As it can be seen from Fig. 5d, with routing in outer space, the network lives 20.42 percent longer, on average.

Since security usually comes at a price, this is somewhat surprising. Routing in outer space delivers a network that, simultaneously, offers less front for an attack and is more energy efficient according to several different definitions of network lifetime.

5 Other Applications of Routing in Outer Space

5.1 Uniform Distribution of Nodes in the Random Waypoint Mobility Model

The random waypoint mobility model is one of the most classical models in the literature of mobile computing. The model is simple: Each node moves independently in the network and iterates a procedure in which it chooses a waypoint in the area uniformly at random, it moves straight to the waypoint with uniform speed chosen at random, it waits a randomly chosen period of time at the waypoint, and finally it iterates by choosing another waypoint. The reader is surely able to see immediately why the distribution of the mobile nodes is not uniform in the network when this mobility model is used on the square for some time, even though they were deployed uniformly at time 0. Intuitively, the straight paths followed by the nodes from waypoint to waypoint are random segments on the square, and therefore, the nodes tend to concentrate at the center of the network—this is not different from the phenomenon that generates hot spots when routing messages.

This problem is well known. The stationary properties of the random waypoint mobility model have been studied in [3], [6], among others. However, routing in outer space gives a clean and simple way to have uniform distribution of the nodes in the random waypoint mobility model. When moving from one waypoint to the other, do it by using the outer space shortest path. Immediately, this yields uniform distribution. Indeed, the random waypoint mobility model on the torus does generate uniform distribution of the nodes (the torus is symmetric under any rotation; to see a formal argument about the same property on the sphere, see [6], the proof for the torus is the same). Note that this outer space version of the random waypoint mobility model is *different* from random walk with reflection [6], which also has uniform distribution of the nodes but the node chooses a random direction instead of a random destination.

5.2 Distributed Detection of Replication Attacks in Wireless Sensor Networks

Wireless sensor networks are often deployed outdoor or in hostile environments. In this case, an adversary can physically capture some of the nodes, reprogram and replicate the nodes in a large number of clones, and redeploy them in the network. The clones are provided with the same cryptographic material as the originals, therefore they can fully communicate with the legitimate nodes and participate in the network operations such as data aggregation, consensus protocols, etc. This gives the adversary the capability of launching all sorts of vicious insider attacks. The detection of the *node replication attack* is thus an important problem in wireless sensor networks and there has been a large amount of work on this topic [10], [25], [27], [11].

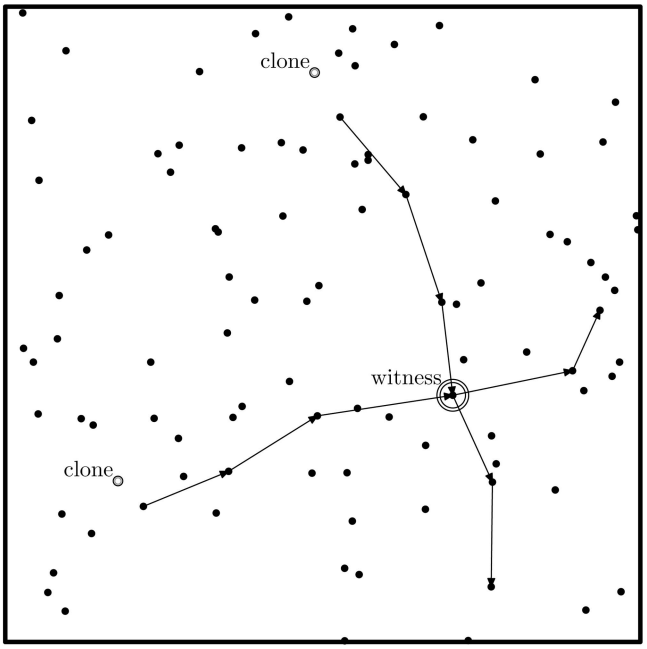


Fig. 6. A run of LSM. Two clones of the same node are present in the network. In this example, two neighbors of the clones send the location claim to a random destination. The two paths intersect at a node, the witness, and the attack is thus detected.

To the best of our knowledge, one of the most feasible and efficient solutions to this problem is the Line-Selected Multicast (LSM) protocol, a distributed approach introduced in [27], which provides globally-aware, distributed node-replica detection. LSM is based on a routine that executes at fixed intervals of time. The routine works as follows: Every node announces its location to its neighbors with a signed claim; each neighbor locally checks both the signature and the location claimed in the message and forwards it with probability p to a fixed number $g \geq 1$ of randomly selected destinations. Each node on the path to destination checks the signature of the claim, locally stores the message, and compares it with other location claims received during the same iteration of the detection protocol. If two clones are present in the network, there is a probability that some node receives two incoherent location claims—two claims with same node id and different location (see Fig. 6). When this is the case, the node is a *witness* of a node replication attack and can trigger a revocation protocol for the node id. Iteration after iteration, the probability that a node replication attack goes undetected gets smaller and smaller, and tends to zero very quickly.

LSM is a simple, intuitive, and efficient protocol. Also, it generates a uniform traffic pattern, routed by using geographic routing [27]. As we know, such conditions give

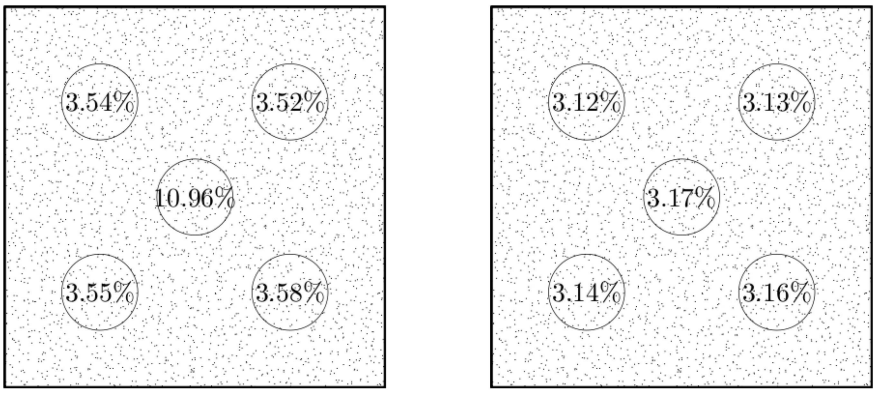


Fig. 7. Witness distribution of LSM with (a) geographic routing and (b) outer space geographic routing.

rise to congested areas, and therefore, to all the previously mentioned security and energy efficiency issues. More than that, as it is also observed in [11], the congestion phenomenon is exacerbated and even more pronounced if you consider the distribution of the witnesses—the intersection between the paths of two claim messages is much more likely to occur in a congested area of the network. This is also what we observed by simulating the LSM protocol over a square. Each individual experiment consists of one iteration of the basic routine of LSM. We run a very large number of experiments—one million of messages—and measured the percentage of witnesses in different subareas of the network. Fig. 7a shows the average of the results on different networks of different size.

Almost 11 percent of the witnesses belong to an area in the center of the network whose size is only 3.14 percent of the network. The percentage decreases significantly in subcentral areas of the same size—the number of witnesses in the areas placed at the middle-half diagonals is about 70 percent lower. A "smart" adversary [11] can perform powerful attacks to this detection protocol in many ways. For example, it can jam the small area in the center (of size 3.14 percent of the network) stopping 11 percent of the possible witnesses. Or it can simply subvert nodes starting from this central area. In such a way, LSM loses part of its efficiency and the probability of detecting clones decreases significantly. Clearly, these problems would not arise if the distribution of the witnesses were uniform.

One way to get uniform distribution of the witnesses is to run LSM on top of outer space geographic routing. Indeed, outer space shortest paths are uniformly distributed and so path intersections are. We run the same set of experiments shown in Fig. 7a with this idea and got the results shown in Fig. 7b. As predicted by our theory, the number of witnesses in each area is independent from its position and shows a virtually perfect distribution on the nodes of the network. This way, we get improved strength against the attacks that we mentioned above. Moreover, it is interesting to see that also efficiency in detection is improved. Indeed, paths are longer and thus intersect with higher probability. In our multiple set of experiments, done with networks of different size (from 1,000 to 10,000 nodes), the probability of detection is 53 percent higher when using outer space geographic routing instead of geographic routing.

To summarize, routing in outer space guarantees that LSM has uniform distribution of the witnesses (and thus more strength against a few "smart" attacks), higher detection efficiency, and longer life due to the improved energy efficiency of the routing layer.

6 Conclusions

Uniform traffic injected into multihop wireless networks generates congested areas. These areas carry a number of nontrivial issues regarding 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. We have shown that a network that uses routing in outer space does not have congested areas, does not have the associated security-related issues, does not encourage selfish positioning, and, in spite of using more energy globally, lives longer of the same network using the original routing protocol, according to a set of measures for network lifetime that collectively cover all the major concerns usually considered in the literature.

Lastly, routing in outer space has a few clean applications in mobility and security protocols. We have shown that a state-of-the-art protocol for node replica detection like LSM [27] gets improved detection efficiency, more security against "smart attacks," and more longevity just using outer space geographic routing instead of geographic routing, as done in [27], as the routing layer.

Acknowledgments

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.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," *IEEE Comm. Magazine,* vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] S. Basagni, M. Nati, and C. Petrioli, "Localization Error-Resilient Geographic Routing for Wireless Sensor Networks," *Proc. IEEE Global Comm. Conf. (GLOBECOM '08),* Dec. 2008.

[3] C. Bettstetter, G. Resta, and P. Santi, "The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks," *IEEE Trans. Mobile Computing,* vol. 2, no. 3, pp. 257-269, July-Sept. 2003.

[4] M. Bhardwaj and A.P. Chandrakasan, "Bounding the Lifetime of Sensor Networks via Optimal Role Assignments," *Proc. IEEE INFOCOM '02,* vol. 3, pp. 1587-1596, 2002.

[5] D.M. Blough and P. Santi, "Investigating Upper Bounds on Network Lifetime Extension for Cell-Based Energy Conservation Techniques in Adhoc Networks," *Proc. ACM MobiCom,* 2002.

[6] J.-Y Le Boudec and I. Vojnovic, "Perfect Simulation and Stationarity of a Class of Mobility Models" *Proc. IEEE INFOCOM '05,* vol. 4, pp. 2743-2754, Mar. 2005.

[7] J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," *Proc. ACM MobiCom '98,* pp. 85-97, 1998.

[8] N. Bulusu, J. Heidemann, D. Estrin, and T. Tran, "Self-Configuring Localization Systems: Design and Experimental Evaluation," *Trans. Embedded Computing Systems,* vol. 3, no. 1, pp. 24-60, Feb. 2004.

[9] P. Casari, M. Nati, C. Petrioli, and M. Zorzi, "Efficient Non-Planar Routing Around Dead Ends in Sparse Topologies Using Random Forwarding," *Proc. IEEE Int'l Conf. Comm. (ICC '07),* pp. 3122-3129, June 2007.

[10] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *Proc. IEEE Security and Privacy Symp.,* 2003.

[11] M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks," *Proc. Eighth ACM Int'l Sym. Mobile Ad Hoc Networking and Computing (MobiHoc '07),* pp. 80-89, 2007.

[12] Q. Fang, J. Gao, and L.J. Guibas, "Locating and Bypassing Holes in Sensor Networks," *Mobile Networks and Applications,* vol. 11, no. 2, pp. 187-200, 2006.

[13] Y. Ganjali and A. Keshavarzian, "Load Balancing in Ad Hoc Networks: Single-Path Routing vs. Multi-Path Routing," *Proc. IEEE INFOCOM '04,* vol. 2, pp. 1120-1125, 2004.

[14] P. Gupta and P.R. Kumar, "The Capacity of Wireless Networks," *IEEE Trans. Information Theory,* vol. 46, no. 2, 388-404 Mar. 2000.

[15] Z. Haas, "A New Routing Protocol for the Reconfigurable Wireless Networks," *Proc. IEEE Int'l Conf. Universal Personal Comm.,* Oct. 1997.

[16] J. Hightower and G. Borriello, "Location Systems for Ubiquitous Computing," *Computer,* vol. 34, no. 8, pp. 57-66, Aug. 2001.

[17] X. Hong, P. Wang, J. Kong, Q. Zheng, and J. Liu, "Effective Probabilistic Approach Protecting Sensor Traffic," *Proc. IEEE Military Comm. Conf. (MILCOM '05),* vol. 1, pp. 169-175, Oct. 2005.

[18] E. Hyytiä and J. Virtamo, "On Traffic Load Distribution and Load Balancing in Dense Wireless Multihop Networks," *EURASIP J. Wireless Comm. and Networking,* vol. 2007, no. 1, 2007.

[19] P. Jacquet, P. Mühlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol for Ad Hoc Networks," *Proc. Fifth IEEE Multi Topic Conf. (INMIC),* 2001.

[20] D.B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing,* vol. 353, T. Imielinski and H.F. Korth, eds., Kluwer Academic Publishers, 1996.

[21] B. Karp and H.T. Kung, "Gpsr: Greedy Perimeter Stateless Routing for Wireless Networks," *Proc. ACM MobiCom '00,* Aug. 2000.

[22] A. Kröller, S.P. Fekete, D. Pfisterer, and S. Fischer, "Deterministic Boundary Recognition and Topology Extraction for Large Sensor Networks," *Proc. 17th Ann. ACM-SIAM Symp. Discrete Algorithm (SODA '06),* pp. 1000-1009, 2006.

[23] S. Kwon and N.B. Shroff, "Paradox of Shortest Path Routing for Large Multi-Hop Wireless Networks," *Proc. IEEE INFOCOM '07,* May 2007.

[24] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless Sensor Networks for Habitat Monitoring," *Proc. First ACM Int'l Workshop Wireless Sensor Networks and Applications (WSNA '02),* pp. 88-97, 2002.

[25] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," *Proc. Third IEEE/ACM Int'l Conf. Information Processing in Sensor Networks (IPSN '04),* pp. 259-268, 2004.

[26] V.D. Park, M.S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *Proc. IEEE INFOCOM '97,* p. 1405, 1997.

[27] B. Parno, A. Perrig, and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," *Proc. 2005 IEEE Symp. Security and Privacy (SP '05),* pp. 49-63, 2005.

[28] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Proc. ACM SIGCOMM '94,* pp. 234-244, 1994.

[29] C.E. Perkins and E. Royer, "Ad Hoc On-Demand Distance Vector Routing," *Proc. IEEE Workshop Mobile Computing Systems and Applications,* pp. 90-100, Feb. 1999.

[30] P.P. Pham and S. Perreau, "Increasing the Network Performance Using Multi-Path Routing Mechanism with Load Balance," *Ad Hoc Networks,* vol. 2, pp. 433-459, Oct. 2004.

[31] L. Popa, A. Rostamizadeh, R. Karp, C. Papadimitriou, and I. Stoica, "Balancing Traffic Load in Wireless Networks with Curveball Routing," *Proc. Eighth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '07),* pp. 170-179, 2007.

[32] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System," *Proc. ACM MobiCom '00,* Aug. 2000.

[33] A. Rao, S. Ratnasamy, C. Papadimitriou, S. Shenker, and I. Stoica, "Geographic Routing without Location Information," *Proc. MobiCom '03,* pp. 96-108, 2003.

[34] E. Royer and C. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," *IEEE Personal Comm.,* vol. 6, no. 2, pp. 46-55, Apr. 1999.

[35] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," *Proc. Int'l Conf. Network Protocols (ICNP),* 2002.

[36] A. Savvides, C.-C. Han, and M.B. Srivastava, "Dynamic Fine-Grain Localization in Ad-Hoc Networks of Sensors," *Proc. ACM/MobiCom,* 2001.

[37] K. Seada and A. Helmy, "Geographic Protocols in Sensor Networks," technical report, University of Southern California, July 2004.

[38] V. Srinivasan, P. Neggehalli, C.F. Chiasserini, and R.R. Rao, "Cooperation in Wireless Ad Hoc Wireless Networks," *Proc. IEEE INFOCOM,* 2003.

[39] W. Wang, X. Li, and Y. Wang, "Truthful Multicast Routing in Selfish Wireless Networks," *Proc. ACM MobiCom '04,* Sept. 2004.

[40] Y. Wang, J. Gao, and J.S.B. Mitchell, "Boundary Recognition in Sensor Networks by Topological Methods," *Proc. ACM MobiCom '06,* pp. 122-133, 2006.

[41] A. Ward, A. Jones, and A. Hopper, "A New Location Technique for the Active Office," *IEEE Personal Comm.,* vol. 4, no. 5, pp. 42-47, Oct. 1997.

[42] Y. Xu, J. Heidemann, and D. Estrin, "Geography-Informed Energy Conservation for Ad Hoc Routing," *Proc. ACM MobiCom '01,* July 2001.

[43] Y. Yu, R. Govindan, and D. Estrin, "Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," Technical Report UCLA/CSD-TR-01-0023, University of California, Los Angeles, Computer Science Dept., May 2001.

[44] M.G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," *Proc. ACM Workshop Wireles Security (WiSe),* 2002.

[45] A. Zemlianov and G. deVeciana, "Capacity of Ad Hoc Wireless Networks with Infrastructure Support," *IEEE J. Selected Areas in Comm.,* vol. 23, no. 3, 657-667, Mar. 2005.

[46] H. Zhang and J. Hou, "On Deriving the Upper Bound of α—Lifetime for Large Sensor Networks," *Proc. ACM MobiHoc '04,* pp. 121-132, 2004.

[47] M. Zorzi and R.R. Rao, "Geographic Random Forwarding (geraf) for Ad Hoc and Sensor Networks: Energy and Latency Performance," *IEEE Trans. Mobile Computing,* vol. 2, no. 4, pp. 349-365, Oct.-Dec. 2003.

Alessandro Mei received the laurea degree (with highest honors) in computer science from the University of Pisa, Italy, in 1994, and the PhD degree in mathematics from the University of Trento in 1999. He was a visiting scholar at the Department of EE-Systems of the University of Southern California during 1998 and part of 1999. After holding a postdoctoral position at the University of Trento for one year, he joined the faculty of the Computer Science Department at Sapienza University of Rome, Italy, where he is currently an associate professor at the Computer Science Department. His main research interests include computer system security and parallel, distributed, and networked systems. He was presented with the Best Paper Award of the 16th IEEE International Parallel and Distributed Processing Symposium in 2002, the EE-Systems Outstanding Research Paper Award of the University of Southern California for 2000, and the Outstanding Paper Award of the Fifth IEEE/ACM International Conference on High Performance Computing in 1998. He is a member of the ACM and the IEEE, an associate editor of the *IEEE Transactions on Computers* since 2005, and the general chair of the IEEE IPDPS 2009, Rome, Italy.

Julinda Stefa received the laurea degree (with highest honors) in computer science from Sapienza University of Rome, Italy, in 2006. Currently, she is working toward the PhD degree at the Computer Science Department of Sapienza University of Rome, Italy. In 2005, she joined the Google Zürich office for three months as an engineering intern. Her research interests include computer systems and networks security, algorithms for parallel and distributed systems, and analysis and modeling of social mobile wireless networks. From November 2008 to April 2009, she was a visiting scholar at the Computer Science Department of University of North Carolina-Chapel Hill. She is a student member of the IEEE.