INHERENT SECURITY OF ROUTING PROTOCOLS IN AD-HOC AND SENSOR NETWORKS

Tanya Roosta[1], *Sameer Pai*[2], *Phoebus Chen*[1], *Shankar Sastry*[1], *Stephen Wicker*[2]

Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA[1]
School of Electrical and Computer Engineering, Cornell University Ithaca, NY [2]

ABSTRACT

Many of the routing protocols that have been designed for wireless ad-hoc networks focus on energy-efficiency and guaranteeing high throughput in a non-adversarial setting. However, given that ad-hoc and sensor networks are deployed and left unattended for long periods of time, it is crucial to design secure routing protocols for these networks. Over the past few years, attacks on the routing protocols have been studied and a number of secure routing protocols have been designed for wireless sensor networks. However, there has not been a comprehensive study of how these protocols compare in terms of achieving security goals and maintaining high throughput. In this paper, we focus on the problem of analyzing the inherent security of routing protocols with respect to two categories: multi-path and single-path routing. Within each category, we focus on deterministic vs. probabilistic mechanisms for setting up the routes. We consider the scenario in which an adversary has subverted a subset of the nodes, and as a result, the paths going through these nodes are compromised. We present our findings through simulation results.

I. INTRODUCTION

Due to recent technological advances, the manufacturing of small, low cost sensors became technically and economically feasible. Thousands of these sensors can potentially be networked as a Wireless Sensor Network (WSN) for many applications that require unattended, long-term operations. Sensor networks are typically ad-hoc, infrastructure-free, multi-hop wireless networks where every node can be either a host or a router forwarding packets to other nodes in the network. Some current applications of sensor networks are providing health care for the elderly, surveillance, emergency disaster relief, detection and prevention of chemical or biological threats, and gathering battlefield intelligence. Sensor networks are becoming widely integrated into critical infrastructures such as Supervisory Control And Data Acquisition systems (SCADA), making security of these networks a prerogative.

One of the critical challenges to making sensor networks more pervasive and secure is the severe resource constraints on the sensor nodes. A typical example of a sensor node, sometimes called a mote, is the Mica2 mote which has a 4MHz, 8-bit processor with 128KB of instruction memory, 4KB of RAM, and 512KB of external flash memory. It also has a 433/916 MHz radio with 38.4 Kbps maximum data rate and runs on a AA battery. The limited energy, bandwidth, and computational resources make it difficult to implement security primitives such as strong cryptography and implement secure services such as secure routing.

The challenge of resource constraints is compounded with the challenge of reliably communicating over an unreliable wireless channel. Sensor networks are usually deployed in environments where the channel is affected by harsh fading. Given the energy, memory, and processing constraints on the motes it is not possible to use sophisticated antennas or modulation schemes. Yet another challenge in sensor networks is to design communication protocols that can scale from tens to thousands of motes. Finally, sensor networks typically are physically unattended after deployment. As a result, the nodes are vulnerable to physical capture and compromise. All of these issues combined make it difficult to design energy/memory efficient, scalable communication protocols which are also secure.

A number of challenges exist in the area of secure routing in sensor networks. Most of the existing protocols deal with specific attacks and deploy cryptography as a means to secure the routing protocols. The authors are not aware of any complete model of attacks on routing protocols or any holistic evaluation of the security of these protocols in sensor networks. In this paper, we abstract away the details of specific attacks and specific routing protocols; instead we focus on characterizing the statistics of attacks on different classes of routing algorithms, specifically single-path and multi-path routing. This is a first step in developing a comprehensive model for evaluating security in sensor

This work was supported in part by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support NSF grant CCF-0424422, and the following organizations: Cisco, ESCHER, HP, IBM, Intel, Microsoft, ORNL, Qualcomm, Pirelli, Sun and Symantec. The second author is also supported by a National Science Foundation IGERT Fellowship. {roosta, phoebusc,sastry}@eecs.berkeley.edu. {skp27, sbw11}@cornell.edu

networks.

The objective of our experimental analysis is to compare the security properties of multi-path versus single-path routing protocols for the scenario in which the adversary has compromised a subset of the nodes in the network and has subverted their normal operations[1]. Even though it is possible to add cryptographic protocols to the routing to enhance the security features of a particular routing protocol, it is important to consider how secure each class of routing protocols is based on the scheme used for finding the routes, i.e. single-path vs. multi-path, and deterministic as opposed to probabilistic. The rest of the paper is organized as follows: Section II gives a statement of the secure routing problem we are considering and outlines our assumptions on the nature of the wireless network, the trust model, the security requirements, and the threat model. Section III gives a summary of different types of single-path routing protocols while Section IV discusses the concept of multi-path routing and different types of multi-path routing protocols. Section V details the simulator we designed to carry out our experiments and the metrics used for comparison of different categories of routing protocols. Finally, Section VI outlines the result of our MATLAB simulations and summarizes our findings.

II. PROBLEM STATEMENT

In this section we explain the network assumptions, security objectives, and threat and trust models used throughout this paper.

II-A. Network Assumptions

Recently, the mathematical models of random graphs and percolation theory have been used to describe the topology of ad-hoc networks. In this paper, we use a *fixed radius random graph* which has been the most common and practical graph model proposed for modeling wireless, ad-hoc network topologies. In this model the nodes are randomly placed in an $m \times n$ region according to some probability distribution, such as a uniform distribution. A link exists between two nodes i and j if the Euclidean distance between these two nodes is less than the communication range. We assume that the wireless links in our graph are bi-directional, meaning if node A hears node B, then node B will hear node A.

We do not model the underlying medium access control (MAC) protocol. Even though the reliability of a path in a network is dependent on the performance of the MAC layer, the objective of our study is to compare the security properties of single-path and multi-path routing protocols.

[1]This is a realistic setting since currently there is no tamper-resistant hardware for the motes.

II-B. Security Objectives

The security objectives in sensor networks are similar to that of other types of networks and can be categorized as *Data Confidentiality*, *Data Authentication*, *Data Integrity*, *Data Freshness*, *Data Availability*, and *Graceful Degradation*.

II-C. Trust Model

In sensor networks, there is typically one or more base stations, typically PCs or laptops, which serve as aggregation points for the information gathered by the sensor nodes and as interfaces between the sensor network and the users. Since base stations are often connected to a larger and less resource-constrained network, it is generally assumed that a base station is trustworthy. On the other hand, there are no trust requirements on the sensor nodes since they are vulnerable to physical capture and other attacks.

II-D. Threat Model

Attacks on sensor networks can be put into different general categories:

- A *mote-class* attacker vs. a *laptop-class* attacker: A mote-class attacker has access to a few motes with the same capabilities as other motes in the network. A laptop-class attacker has access to devices with more computational resources, such as laptops. As a result, he can launch more serious attacks.
- An *insider* attacker vs. an *outsider* attacker: An outsider attacker such as a passive eavesdropper has no special access to the sensor network, but an insider attacker has access to the encryption keys or other code used by the network. For example, an insider attacker could be a compromised node which was originally a legitimate part of the sensor network.
- *Passive* vs. *active* attacker: A passive attacker is only interested in collecting sensitive data from the sensor network, which compromises the privacy and confidentiality requirements. In contrast, the goal of the active attacker is to disrupt the function of the network and degrade its performance.

In this paper, we discuss the inherent security of different categories of routing protocols when a certain number of network nodes have been compromised, i.e. we assume there is an insider attacker who is active. We consider this type of attack because there exist protocols that use cryptography as the primary means for security [1]. However, this does not preclude a compromised nodes from disrupting the normal operation of the network by jeopardizing data integrity and availability. As the experiments in [2] have shown, the sensor nodes can be physically compromised and information regarding the cryptographic keys can be easily extracted from these nodes.

Throughout this paper, we assume the attacker does not want to be detected, and hence does not change the routing topology of the network, as is done in the blackhole or similar types of attacks. This means that a compromised node continues to route packets to the destination specified in the packet header, so that the routing algorithm does not detect a route error and actively reroute around the compromised node. However, the content of the packets may be altered by the attacker or he might drop the packets randomly (which will look like noise from the network's perspective).

III. SINGLE-PATH ROUTING

There has been a large number of one-to-one, single-path routing protocols proposed for wireless ad-hoc networks in the recent years [3]. They can be categorized as *Deterministic Single-Path* and *Probabilistic Single-Path* routing protocols.

III-A. Deterministic Single-Path Routing Protocols

The most well-known deterministic single-path routing protocol is shortest path routing (SPR), where packets travels down the path with a minimum number of hops from source to destination. SPR is a special case of minimum-weight path routing, where the edges in the network topology are assigned weights and packets travel down the path minimizing the sum of the weights. Many of the standard single path routing algorithms implemented for sensor networks in TinyOS [4], a popular operating system for sensor networks, use minimum-weight paths [5], [6]. The algorithms vary in the way they define weights for the edges in the path, where the weights correspond to some estimate of link quality.

III-B. Probabilistic Single-Path Routing Protocols

This category of protocols builds on the idea of a directed random walk in a graph. The objective of these random walk protocols is to achieve load balancing in a statistical sense. In contrast to the deterministic routing protocols, probabilistic protocols choose the next node using a dynamically assigned probability. For example, [7] suggests a probabilistic geographic routing protocol. The probability assigned to a node is proportional to $\frac{E}{r}$, where E is the residual energy of the node and r is the link reliability. The routing algorithm is simple because the nodes only need to maintain minimal state information. Another example of the probabilistic single-path routing can be found in [8].

IV. MULTI-PATH ROUTING PROTOCOLS

Multi-path routing is a class of routing mechanisms that establish multiple paths between a given source and destination. Multi-path routing can potentially yield a higher throughput and provide more reliability than single-path routing since the load is distributed across multiple routes. It increases reliability and resilience to path failures by sending multiple copies of a data packet along different paths. Furthermore, load balancing in sensor networks can spread energy utilization across the network, potentially resulting in longer lifetimes. In order to fully utilize load balancing, the routing protocol should find paths that push the traffic further from the center of the network [9].

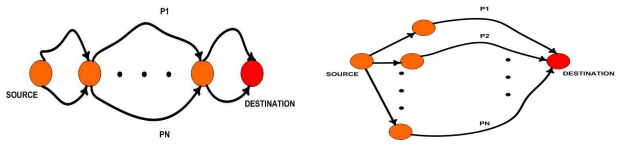

Fig. 1. (left) An example of edge disjoint paths. (right) An example of node disjoint paths.

As for security, multi-path routing protocols are more resilient to Denial of Service Attacks. Generally speaking, for better security the algorithm should select paths whose failures are less correlated. For instance, the algorithms might want to select disjoint paths, whether they be node-disjoint or edge-disjoint (See Figure 1). Of these two types, node-disjoint paths are typically preferable for security. If the routes were only edge-disjoint an adversary can physically capture/compromise n nodes to control/compromise more than n paths. In addition to characterizing multi-path routing protocols by node-disjointness and edge-disjointness, we can divide them into two categories: *Deterministic* routing protocols and *Parametric Probabilistic Routing* protocols.

IV-A. Deterministic Multi-Path Routing Protocols

The problem of reliable data delivery using multiple paths can be classified into two distinct problems:

- The problem of assessing the link failure probabilities, and using them to assign probabilities of reliable data delivery to different paths. Then, we can find a number k of reliable, disjoint paths to route information through. This problem is best addressed by finding the k most reliable edge-disjoint paths.
- The problem of assessing node failure probabilities, and using them to assign probabilities of reliable data delivery to different paths. Then, we can choose a number k of reliable, disjoint paths to route information through. This problem is best addressed by finding the k most reliable node-disjoint paths.

For secure routing the objective is to route information around or away from a path containing a compromised node, because this node could compromise data integrity. This objective directly maps to the second problem discussed above, namely, the one of finding the k most reliable node-disjoint paths. One way to find k disjoint paths is to employ an iterative procedure where the shortest paths are found one after the other, removing the links of each path after

it is found [10]. A similar recursive algorithm can be used to find the minimum or maximum weighted paths where the weights can be any metric, for instance link reliability. General methodologies for finding k node-disjoint paths in a distributed fashion between a source and a destination node in a uniformly weighted, undirected network, such as a sensor network, are given by the *Distributed Augmenting Paths Algorithm* in [11] and a modified version of the *Disjoint Path Selection Protocol (DPSP)* in [12].

IV-B. Parametric Probabilistic Multi-Path Routing Protocols

Parametric Probabilistic Routing (PPR) protocols are a family of light-weight, adaptive routing protocols proposed in [13]. PPR builds on the simple flooding algorithm, with the addition that now every node has a retransmission probability for forwarding received messages to all of its neighbors. The retransmission probability can be a function of various factors — for example, the number of hops to the destination, the number of the hops the packet has already traveled, the number of neighbors of a node, or the number of times a node has forwarded the same packet[2] [13]. Each retransmission probability describes a different member in the family of PPR protocols, and it can be formulated as follows [13]:

$$p = \exp[-k_1(d_{RD} - d_{SD} + k_2 \cdot h) - k_3 \cdot c]$$

where d_{SD} is the shortest-path hop-distance between the source and the destination, d_{RD} is the distance from an intermediate node holding the packet to the destination, and parameters k_1, k_2, and k_3 are tuned differently for each family of PPR protocols.

V. THE SIMULATOR SETUP

We built a simulator in MATLAB to evaluate how well the multiple routing schemes discussed above perform in sensor networks. The Secure Sensor Network Routing Simulator (SSNRS) allows for the use of different channel models, routing topologies, routing protocols, and attack scenarios in a discrete packet-time marching network simulation. We give an overview of the simulator and its outputs, with details omitted due to space restrictions.

SSNRS allows the selection of different radio models for how link probability varies as a function of distance between nodes. The simulator also allows the user to specify the node placement topology of the sensor network or generate a uniformly random placement topology over a given area with a specified number of nodes. The network communication topology is then determined by the radio connectivity model of the nodes. SSNRS currently allows for probabilistic parametric flooding, probabilistic single path, k-disjoint minimum weight paths, and minimum weight single path routing. These encompass the multiple classes of routing protocols described in Sections IV and III. The attack scenarios constructed in SSNRS consist of mostly insider attacks. SSNRS simulates a directed random walk from a compromised node within the network, uniform random attacks on the nodes, and attacks on a large clusters of nodes.

In each scenario, first SSNRS generates a predefined wireless channel and sensor network topology. For this topology, and a given attack scenario, we measure the performance of the routing protocols mentioned above in terms of energy usage, average number of paths found containing compromised nodes, and average number of packets intercepted by compromised nodes.

VI. ANALYSIS AND RESULTS

There are several criteria for comparing single-path and multi-path routing in wireless ad-hoc networks. First is the overhead of route discovery, which is higher for multi-path routing. Second is the frequency of route discovery, which is much lower in multi-path routing since the network can utilize multiple paths even if a subset of the routes are not operational. Third is the energy spent transmitting packets using the four routing protocols discussed above. We do not consider the first two criteria. The result of our simulation for the third criteria (average energy per transmission) is shown in Table I, where an energy unit is equivalent to the energy for one radio transmission and we assume the difference in energy for computation for the different routing protocols is negligible. Under our attack models, the energy expenditure of the routing protocols are not dependent on the attacks because the attacker continues to route corrupted packets through the network, and is equivalent to energy expenditure under no attacks.

Table I. Baseline Energy Expenditure

Routing Protocol	***Average energy per packet***
Deterministic single-path	3.62 units
Probabilistic single-path	7.56 units
Deterministic multi-path	15.11 units
PPR	209.35 units

The focus of our simulations is on comparing the four routing protocols in terms of the number of times each protocol is successful in delivering packets to the destination. The different attack scenarios (Figure 2) that we simulated can be described as follows: The *uniformly distributed attack* compromises a number of k nodes uniformly at random. The *random walk attack* first chooses a node to compromise uniformly at random and then performs a directed random walk towards the periphery of the network. Finally, the *spatial attack* chooses a node to compromise uniformly at random and also compromises all nodes within a set preset

[2]It has been shown that if $p \geq 0.7$, there is over 90% success rate [14].

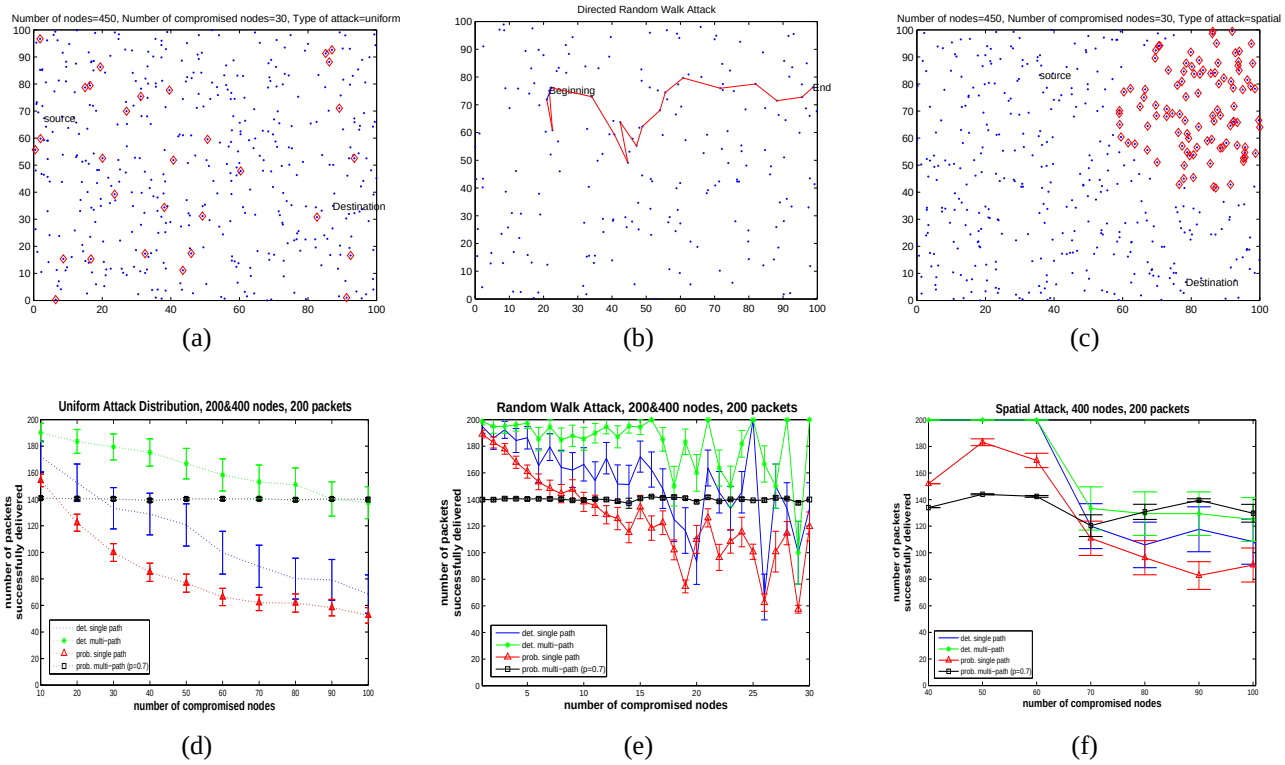

Fig. 2. Examples of a (a) Uniform attack, (b) Directed random walk attack, and (c) Spatial attack. Success versus number of compromised nodes for the (d) Uniform attack, (e) Directed random walk attack, (f) and Spatial attack.

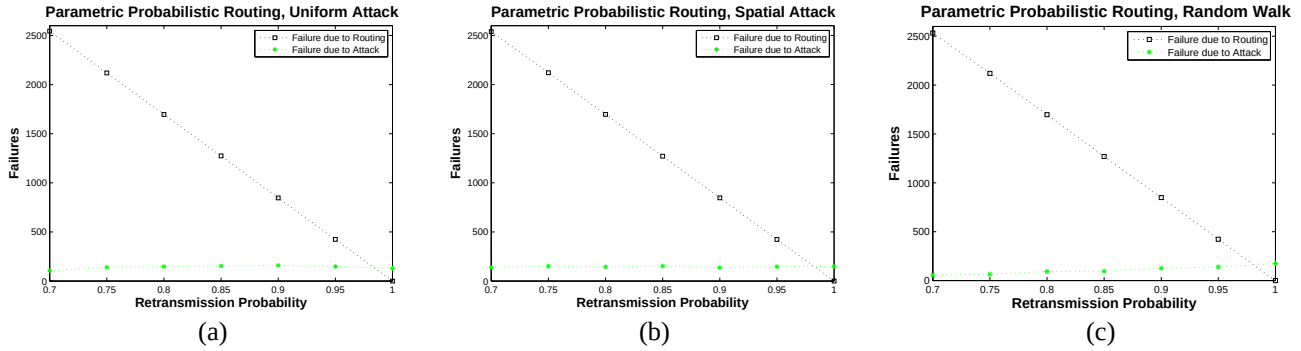

Fig. 3. Failures due to routing and failures due to attack from compromised nodes versus the retransmission probability of PPR for the (a) Uniform attack, (b) Spatial attack, and (c) Directed random walk attack.

radius. The parameters used in the simulations are given in Table II.

Prior to the simulations, we expected that the different attacks would affect various routing protocols in very specific ways. To explain this, we consider a scenario where there is a fixed number of compromised nodes in the network. The uniform attack is the most detrimental to successful end-to-end delivery of the packets. This is because every node has an equal likelihood of lying on a path from a given source to a destination, and in order to compromise a single path, it is sufficient to compromise a single node on that path. In contrast, spatial attacks are highly clustered attacks which have a lower likelihood of lying on a path from the source to the destination. We expected that the random walk attack has packet delivery performance degradation results in between that of the uniform attack and the spatial attack scenarios. This is due to the fact that the nodes are not as highly clustered in one region as in the spatial attack; at the same time, the nodes are not as highly distributed as in the uniform attack scenario. Our simulations results, shown in Figure 2 (d,e,f), validate our performance expectations.

Our simulation results show that PPR has a relatively high

Table II. Parameters Used In SSNRS Simulations

Parameter	*Value*
Number of nodes	200, 400
Grid size	100×100
Topologies tested	uniform random distribution
Number of packets	200
Number of paths in multi-path scenarios	4
Link probability	linear, $\frac{1}{r^{\alpha}}$
Transmission range	30
Number of compromised nodes	1-100
Attack scenario	uniform, spatial, random walk
Number of runs for each scenario	25

rate of successful packet delivery and minimal variance. However, to achieve this, PPR expends the most amount of energy per packet. The deterministic multi-path protocol has the highest success rates and does not expend as much energy as the PPR protocol but has a higher variance in its success rates. The probabilistic single path routing protocol performed the worst with respect to our metrics because of its low end-to-end delivery success rate, high variance in success rate, and relatively high energy expenditure for single path routing. In addition, we looked at the performance of PPR under different retransmission probabilities, p, ranging from 0.7 to 1. The metric in this set of simulations is the number of failures due to route failure and the number of failures due to attacks. Routing failure occurs when the algorithm quits retransmitting a packet (because $p \neq 1$) before it arrives at the destination node. As it can be seen in Figure 3 the two types of failure cross when the retransmission probability is approximately 0.97. This shows that in order to have more reliable delivery, we need to move toward flooding, which consumes more energy.

VII. CONCLUSIONS

In this paper, we gave an overview of the families of routing protocols that are employed in wireless ad-hoc sensor networks. These include deterministic single-path, probabilistic single-path, node-disjoint k-path, and PPR protocols. We did a focused study of the inherent security of these protocols under multiple types of active insider attacks. Our simulations show that the multi-path routing protocols have better end-to-end packet delivery under different types of attacks than the single-path routing protocols. Although our results show that probabilistic single-path routing protocol performs the worst in terms of this metric, it is generally believed that the probabilistic protocols could be used to preserve confidentiality [15].

VIII. REFERENCES

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, 2005.

[2] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: The need for secure systems," Department of Computer Science University of Colorado at Boulder, Tech. Rep., 2005.

[3] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," *IEEE Wireless Communications*, 2004.

[4] W. Weber, J. Rabaey, and E. Aarts, Eds., *Ambient Intelligence*. Springer-Verlag, 2005, ch. TinyOS: An Operating System for Sensor Networks.

[5] A. Woo, T. Tong, and D. Culler, "Taming the underlying challenges of reliable multihop routing in sensor networks," in *SenSys*, 2003.

[6] G. Tolle, "A network management system for wireless sensor networks," Master's thesis, Univ. of California, Berkeley, 2005.

[7] T. Roosta and S. Sastry, "Probabilistic geographic routing protocol for ad hoc and sensor networks," in *International Workshop on Wireless Ad-hoc Networks (IWWAN)*, 2005.

[8] S. D. Servetto and G. Barrenechea, "Constrained random walks on random graphs: Routing algorithms for large scale wireless sensor networks," in *1st ACM International Workshop on Wireless Sensor Networks and Applications*, 2002.

[9] Y. Ganjali and A. Keshavarzian, "Load balancing in ad hoc networks: Single-path routing vs. multi-path routing," in *INFOCOM, 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*, 2004.

[10] V. A. Kaustov, E. Litvak, and I. Ushakov, "The computational effectiveness of reliability estimates by the method of nonedge-intersecting chains and cuts," *Soviet Journal on Computing and Systems Science*, 1986.

[11] S. Arora, H. Lee, and R. Thurimella, "Algorithms for finding disjoint paths in mobile networks."

[12] P. Papadimitratos, Z. J. Haas, and E. G. Sirer, "Path set selection in mobile ad hoc networks," in *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, 2002.

[13] C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith, "Parametric probabilistic sensor network routing," in *WSNA '03: Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, 2003.

[14] Y. Sasson, D. Cavin, and A. Schiper, "Probabilistic broadcast for flooding in wireless mobile ad hoc networks," in *Proceedings of IEEE Wireless Communications and Networking (WCNC)*, 2003.

[15] P. Kamat, Y. Zhang, and W. Trappe, "Enhancing source-location privacy in sensor network routing," *Proceedings of the* 25^{th} *IEEE International Conference on Distributed Computing Systems*, 2005.