International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May 2014)

Techniques to Provide Location Privacy to Objects and Sinks against a Global Eavesdropper

Ambika.V[1].Dept of CSE KBNEC,Gulbaraga.Karanataka.
ambikapallu41@gmail.com
Prof.Shameem.Aktar[2],Dept of CSE KBNEC Gulbaraga.
Shameem_najam@yahoo.com

Abstract: **While many protocols for sensor network security provide confidentiality for the content of messages, contextual information usually remains exposed. Such information can be critical to the mission of the sensor network, such as the location of a target object in a monitoring application, and it is often important to protect this information as well as message content. There have been several recent studies on providing location privacy in sensor networks. We first argue that a strong adversary model, the *global eavesdropper*, is often realistic in practice and can defeat existing techniques. We then formalize the location privacy issues under this strong adversary model and show how much communication overhead is needed for achieving a given level of privacy. We also propose two techniques that prevent the leakage of location information: *periodic collection* and *source simulation*. Periodic collection provides a high level of location privacy, while source simulation provides trade-offs between privacy, communication cost, and latency. Through analysis and simulation, we demonstrate that the proposed techniques are efficient and effective in protecting location information from the attacker.**

Index Terms—**Sensor Networks, Location Privacy**

1. INTRODUCTION

A wireless sensor network (WSN) typically consists of a large number of small, multi-functional, and resource-constrained sensors that are self-organized as an ad-hoc network to monitor the physical world [1]. Sensor networks are often used in applications where it is difficult or infeasible to set up wired networks. Examples include wildlife habitat monitoring, security and military surveillance, and target tracking. For applications like military surveillance, adversaries have strong incentives to eavesdrop on net-work traffic to obtain valuable intelligence. Abuse of such information can cause monetary losses or endanger human lives. To protect such information, researchers in sensor network security have focused considerable effort on finding ways to provide classic security services such as confidentiality, authentication, integrity, and availability. Though these are critical security requirements, they are insufficient in many applications. The communication patterns of sensors can, by themselves, reveal a great deal of *contextual information*, which can disclose the location information of critical components in a sensor net-work. For example, in the Panda-Hunter scenario [15], a sensor network is deployed to track endangered giant pandas in a bamboo forest. Each panda has an electronic tag that emits a signal that can be detected by the sensors in the network. A sensor that detects this signal, the *source* sensor, then sends the location of pandas to a data sink (destination) with help of intermediate sensors. An adversary (the hunter) may use the communication between sensors and the data sinks to locate and then capture the monitored pan-das. In general, any target-tracking sensor network is vulnerable to such attacks. As another example, in military applications, the enemy can observe the communications and locate all data sinks (e.g. base stations) in the field. Disclosing the locations of the sinks during their communication with sensors may allow the enemy to precisely launch attacks against them and thereby disable the network.

Location privacy is thus very important, especially in hostile environments. Failure to protect such information can completely subvert the intended purposes of sensor network applications. Location privacy measures thus need to be developed to prevent the adversary from determining the physical locations of *source sensors* and *sinks*. Due to the limited energy lifetime of battery-powered sensor nodes, these methods have to be energy efficient. Since communication in sensor networks is much more expensive than computation, we use communication cost to measure the energy consumption of our protocols. Providing location privacy in a sensor network is very challenging. First, an adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets. He can use information like packet transmission time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. Second, sensors usually have limited processing speed and energy supplies.

2. EXISTING SYSTEM:

However, these existing solutions can only be used to deal with adversaries who have only a local view of network traffic. A highly motivated adversary can easily eavesdrop on the entire network and defeat all these solutions. For example, the adversary may decide to deploy his own set of sensor nodes to monitor the communication in the target network. However, all these existing methods assume that the adversary is a local eavesdropper. If an adversary has the global knowledge of the network traffic, it can easily defeat these schemes. For example, the adversary only needs to identify the sensor node that makes the first move during the communication with the base station. Intuitively, this sensor node should be close to the location of adversaries interest

2.1DISADVANTAGES OF EXISTING SYSTEM

- The existing approaches assume a weak adversary model where the adversary sees only local network traffic.
- Existing techniques defend the leakage of location information from a limited adversary who can only observe network traffic in a small region.

3. PROPOSED SYSTEM:

We show the performance of the proposed privacy-preserving techniques in terms of energy consumption and latency and compare our methods with the phantom single-path method, a method that is effective only against local eavesdroppers. For the purpose of simulation, we assume that the network application only needs to detect the locations of pandas and always wants to know the most recent locations. We thus have every sensor node drop a new packet if it has already queued a packet that was generated on the same event. In our simulation, we assume that the adversary has deployed a network to monitor the traffic in the target network.

3.1ADVANTAGES OF PROPOSED SYSTEM:

- The proposed system provides trade-offs between privacy, communication cost, and latency.
- The proposed techniques are efficient and effective for source and sink-location privacy in sensor networks.
-

4. MODULES:

- Network Modules.
- Privacy-Preserving Routing Techniques.
- Adversary Model.
- Privacy Evaluation Model.
- Security Analysis**.**

4.1 Network Model

Sensor networks are a relatively recent innovation. There are number of different types of sensor nodes that have been and continue to be developed [12]. These range from very small, inexpensive, and resource-poor sensors such as Smart Dust up to PDA-equivalent sensors with ample power and processing capabilities such as Star gate. Applications for networks of these devices include many forms of monitoring, such as environmental and structural monitoring or military and security surveillance.

In this paper, we consider a *homogeneous network model*. In the homogeneous network model, all sensors have roughly the same computing capabilities, power sources, and expected lifetimes. This is common network architecture for many applications today and will likely continue to be popular moving forward. It is well-studied and provides relatively straightforward analysis in research as well as simple deployment and maintenance in the field.

Although our research can be applied to a variety of sensor platforms, most sensors run off battery power, especially in the kinds of potentially hostile environments that we are studying. Given this, each sensor has a limited lifespan and the network must be designed to preserve the sensors' power reserves.

In [6], Deng et al. described a technique to protect the locations of sinks from a local eavesdropper by hashing the ID field in the packet header. In [8], it was shown that an adversary can track sinks by carrying out *time correlation* and *rate monitoring* attacks. To mitigate these two kinds of attacks, Deng et al. introduced a *multiple-parent routing* scheme, a *controlled random walk* scheme, a *random fake path* scheme, and a *hot spots* scheme [8]. In [13], a protocol called LPR was proposed for sink location privacy. The LPR algorithm provides privacy to the sink by adding redundant hops and fake packets when data are sent to the sink. However, these techniques all assume that the adversary is a local eavesdropper. A global eavesdropper can easily defeat these schemes. For example, the global eavesdropper only needs to identify a region of high activity, i.e., the region exhibiting a high number of transmissions, to locate the sink. In this paper, we focus on privacy-preserving techniques designed to defend against a global eavesdropper.

4.2Privacy-PreservingRouting Techniques:

In this module presents two techniques for privacy preserving routing in sensor networks, a *periodic collection* method and a *source simulation* method. The periodic collection method achieves the optimal location privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source simulation method provides practical trade-offs between privacy, communication cost, and latency; it can be effectively applied to real-time applications. In this paper, we assume that all communication between sensor nodes in the network is protected by pair wise keys so that the contents of all data packets appear random to the Global eavesdropper. This prevents the adversary from correlating different Data packets to trace the real object.

4.3Adversary Model

For the kinds of sensor networks that we envision, we expect highly-motivated and well-funded attackers whose objective is to learn sensitive information such as the locations of monitored objects and sinks.

The objects monitored by the network can be critical. Such objects could be soldiers, vehicles, or robots in a combat zone, security guards in a protected facility, or endangered animals in the wild. If the locations of these objects were known to an adversary, the endangered animals could be captured for profit, security guards could be evaded to enable theft of valuable property, and military targets could be captured or killed. Sinks are also critical components of sensor networks. In most applications, sinks act as gateways between the multi-hop network of sensor nodes and the wired network or a repository where the sensed information is analyzed. Unlike the failure of a subset of the sensors, the failure of a sink can create permanent damage to sensor network applications. Compromise of a sink will allow an adversary to access and manipulate all the information gathered by the sensor network, because in most applications, data is not encrypted after it reaches a sink. In some military applications, an adversary could locate sinks and make the sensor network non-functional by destroying them. Thus, it is often critical to the mission of the sensor network to protect the location information of monitored objects as well as data sinks. In this paper, we consider *global eavesdroppers*. For a motivated attacker, eavesdropping on the entire network is a fast and effective way to locate monitored objects and sinks. There are two realistic options for the attacker to achieve this. The first option is to deploy his own snooping sensor network to snoop on the target network. Note that, at the current price for a Blue Radios SMT Module at $25, the attacker needs only $25,000 to build a network of 1000 nodes [3]. Further, the number of snooping nodes can typically be smaller than the number of nodes in the target net-work as they monitor radio signals instead of directly sensing the environment. Thus, for even moderately valuable location information, this can be worth the cost and trouble. Another option is to deploy a few powerful nodes to snoop on the network. However, due to the short radio ranges of typical sensor plat-forms, the snooping nodes still need to be deployed densely enough to sense the radio signals from all sensor nodes. Thus, in practice, we may not be able to reduce the number of snooping nodes significantly by using powerful devices It is certainly possible that an adversary deploys sensors to directly sense the objects of his interest, instead of collecting and analyzing the traffic in the original network. However, directly recognizing an object is a very challenging problem in practice due to the difficulty of distinguishing the physical features of the objects from background noises. For example, recognizing a panda is much harder than detecting a packet and estimating some physical features (e.g., RSSI) from this packet. In most scenarios, such sensing problem is simply avoided by installing a small device (e.g., a sensor node) on each object; these small devices emit signals from time to time so that we can sense them accurately. Thus, locating objects by monitoring the traffic in the original network becomes much more attractive to the adversary. We consider our defense a success if the adversary is forced to launch the direct sensing attack although such an eavesdropping sensor network would face some system issues in being able to report the precise timing and location of each target network event, we do not believe that these would keep the attackers from learning more approximate data values. This kind of attacker would be able to query his own network to determine the locations of observed communications. He could have appropriate sensors send signals that could then be physically located. He could equip his sensors with GPS to get locations or use localization algorithms to avoid the cost of GPS. We do not assume that the adversary has to precisely locate each node in the target network. In most cases, a rough idea about where the critical events occurred would be sufficient for the adversary.

It should thus be feasible to monitor the communication patterns and locations of events in a sensor network via global eavesdropping. An attacker with this capability poses a significant threat to location privacy in these networks. We therefore focus our attention to this type of attacker.

4.4 PRIVACY EVALUATION MODEL

In this section, we describe a model for evaluating the location privacy of critical components in sensor net-works. In this model, the adversary deploys a *snooping network* to monitor the wireless transmission activity in the target network. We consider a scenario in which an adversary can monitor all transmissions of the sensors in the network. In practice, the adversary does not need to know exactly where a packet is sent or the exact location of the sensor node that sends the packet. A rough estimate of the location will be good enough for the attacker to conduct traffic analysis. However, in this section, we assume the worst case scenario: for every observed packet, the adversary knows where it is sent or which sensor node sends the packet. This indicates that each sensor i is an *observation point*, and a tuple (i, t, e) is available to the adversary by observing each packet e send by node i at time t. We assume that all transmissions are encrypted and hence the actual useful information available to the adversary is (i,t). We assume that the network begins operations at time t = 0.

The attacker's objective is to locate the source or the sink by snooping on the wireless transmissions. The main observation used by the global adversary is: *there must be a sequence of spatial-temporal correlated packets involved in each communication from the source to the sink*. As long as the adversary knows the routing protocol, he can easily identify all these sequences from the traffic and determine the set of possible sources and sinks. Intuitively, the defender has to create dummy sequences in the network to confuse the attacker; such dummy sequences usually require the addition of dummy traffic into the network, leading to more communication overhead. Clearly, there is a tradeoff between the location privacy and the communication overhead. In this section, we develop a theoretical study of this trade-off.

4.4.1Measuring Privacy

An intuitive way of measuring location privacy is to evaluate the attacker's accuracy in locating sources. Note that the adversary will need to identify the areas in which the objects of his interest can be found. We assume that the attacker that knows the routing protocol and does not miss any real sources.

In other words, the real sources can always be found in the sensing range of the possible source sensors identified by the adversary (S_T). We could measure the total area covered by these sensors' sensing range as a metric of how much area the attacker would need to search to find the sources. However, since all sensors have the same sensing radius in our model, we simplify this by just taking the size of the set S_T . Intuitively, the larger the size of S_T , the more uncertainty the adversary will have about the locations of real sources. We assume that the sensors in S_T are equally likely to be source sensors. The probability of any sensor node in S_T being a source sensor can thus be estimated by $\frac{|S_P|}{|S_T|}$. Hence, we formally define the location privacy of our system as:

$$b=\sum -1/ST \ \ \mathrm{Log}_2 \,|Sp/S_T|= \mathrm{Log}_2 \,|Sp/S_T|$$

We can use this notion to define the optimal privacy, Let S_T reprasent the set of all possible locations for the object at time T based on the set of all possible observations OT i.e

$$S_T =\{I|K□ \ S_A,\ Ai,k \ □ \ OT,(i=fp(Ai,k))\neq \perp\}$$

We have yuhe optimal location privacy as

$$b \leq \log_2 \frac{|S_T^{□}|}{|S_P|} = \log_2 \frac{N}{|S_P|}.$$

The level of location privacy is measured in terms of bits of information. Depending on the users and applications, this can be easily modified to support different kinds of privacy measurement models. For example, we can define high, medium, and low privacy levels by using appropriate values of b.

We note that the traffic in the network can cause the level of privacy to vary. The privacy would go lower if the attacker ascertains that a particular trace is no longer a candidate trace. If a candidate traces splits into two candidate traces, then the level of privacy goes up because S_T grows. The interpretation of this depends on the sensor network application and the attacker model considered. For example, if the attacker seeks to physically destroy the object being observed with a missile (instantaneous attack), then the privacy should be taken as the minimum at any time before T . In cases where the attacker must spend time to investigate the candidate locations, then the average privacy over time is adequate. We provide a snapshot of the privacy at any given time, which can be used for either purpose.

4.5 Security Analysis:

The generation number of a packet can be hidden in the secure routing scheme through link-to-link encryption. In this way, attackers cannot find the generation number of a packet for their further analysis. Notice that secure routing paths are only required to be established at the beginning of each session; during the packet transmission, secure routing paths are not required to change or re-established for each new generation.

5. SIMULATION EVALUATIONS

In this section, we use simulation to evaluate the performance of our techniques in terms of energy consumption and latency. We will use the terminology from this example to describe our simulation. In this application, a sensor network is deployed to track endangered pandas in a bamboo forest. Each panda has an electronic tag that emits a signal that can be detected by the sensors in the network. We include 5,093 sensor nodes distributed randomly in a square field of 1000 × 1000 square meters to monitor the pandas. The base station is the sink for all real data traffic. Each sensor node can communicate with other sensor nodes in a radius of 50 meters, while an electronic tag attached to a panda can emit radio signals that can reach sensor nodes within 25 meters. We noticed that, on average, each sensor node has 40 neighbors and that the presence of any panda will be detected by 10 sensor nodes. For source location privacy techniques, we assume that the base station is located at the center of this field. For sink location privacy techniques, we randomly choose the locations of fake base stations in the field.

The proposed techniques assume a routing protocol for sensor networks, though the choice of routing protocol does not affect our results. For simplicity, we adopt a simple and widely-used routing method used in many studies [7]. In this method, the routing paths are constructed by a beacon packet from the base station. Each node, on receiving the beacon packet for the first time, sets the sender of the beacon packet as its parent. In this way, each node will likely select a parent that is closest to the base station.

For the purpose of simulation, we assume that the network application only needs to detect the locations of pandas and always wants to know the most recent locations. We thus have every sensor node drop a new packet if it has already queued an identical packet that was generated from the same event.

In our simulation, we assume that the adversary has deployed a network to monitor the traffic in the target network. Specifically, he is able to locate every sensor node in the target network and eavesdrop on every packet this node delivers. Though the adversary may face some engineering problems in developing methods to collect the observations from its network, we do not believe that this will be a very difficult issue to address. For simplicity, we assume the adversary can always reliably collect all the observations in the network.

Each simulation in our experiment lasts for 6,000 intervals of τ seconds each. The initial locations for pandas are randomly selected. In the experiments, the tag attached to a panda emits a signal for detection at a rate of one per 10 × τ seconds. In addition, every panda moves from its current location (x, y) to a random location (x ± a1, y ± a2) every 10 × τ seconds, where a1 and a2 are two random values uniformly selected between 0 and 60.

We compare our techniques with the optimal technique that follows a Steiner tree to route packets to the base stations. We use the approximation algorithm from approximating the construction of Steiner trees. Section 4 includes a brief description of this algorithm. We also compare our source privacy techniques with the Proxy-based Filter Scheme (PFS). Dividing the field into square cells of length 17.68 meters gives us 3249 cells in the entire field. Each of these cells has a candidate proxy. Finding the close to optimal number of proxies and their locations in the network using the proxy placement algorithm (O(n7)) will take significant time. We therefore divide the field into square cells of 100 meters so that the number of cells reduces to 100. For simulation of PFS, proxy nodes emit one packet every interval and other sensor nodes generate traffic with inter-packet delays following an exponential distribution with a mean of 10 (intervals).

5.1 Source Location Privacy

5.1.1Periodic Collection

The analysis in Section 5 shows that the periodic collection method achieves optimal location privacy.

5.1.2Source Simulation

The location privacy achieved by the source simulation approach is determined by the number of virtual sources simulated in the network. Thus, the focus of our simulation evaluation is on how much communication cost we have to pay to achieve a given level of location privacy. We use these results to illustrate the efficiency of the proposed technique.

During the simulation, we assume that there is only one panda in the network. Multiple fake pandas are created and simulated in the field. The initial positions of the fake pandas are randomly selected. In addition, we assume that the sensor network is deployed to handle real-time applications. In other words, when- ever a sensor node receives a packet, it will forward it to the next hop as soon as possible. Thus, while we set the time interval for periodic collection as = τ, we set it to = 10τ for source simulation. In other words, in source simulation, nodes will forward packets ten times faster than in the periodic collection method. We set P to 1, which means that the adversary has the same knowledge about the panda behavior as the defender and thus cannot distinguish between fake pandas and real pandas based on the observed behavior.

5.2 Sink Location Privacy

5.2.1Sink Simulation

The focus of our simulation evaluation is on the latency and the packet drop rate when there are multiple base stations in the field.

Fig. 1 shows the latency of packet delivery when there are multiple fake base stations in the field. We can see that as the number of fake base stations in- creases, thereby providing more location privacy, the latency increases. This is because having more base stations causes more traffic in the network and thus more packets to be buffered. When the number of fake base stations grows too large, the buffered packets start being dropped due to nodes' limited queue sizes, while the latency of the packets that do arrive at the base station becomes stable after a certain point. When the queue size q decreases, packets traveling long distances have a high probability of getting dropped, making the latency of the packets that do arrive at the real base station smaller. This can be seen by a drop in the latency for smaller values of q.

Fig. 2 shows the percentage of detected events received by the real base station. We see that the percentage of events received decreases when there are more fake base stations in the field. Fig. 2 and Fig. 1 give guidelines for confguring the queue size q and the number of fake base stations to meet various requirements.

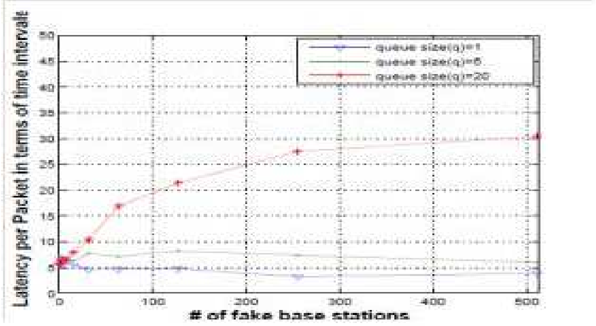

Fig1 .Effect of number of fake base station on latency(Sink simmulation scheme)

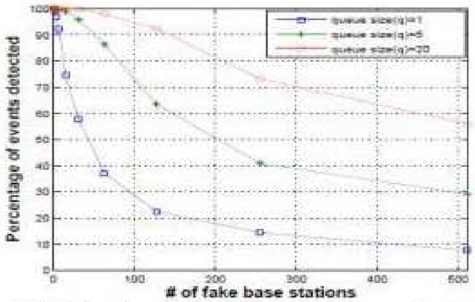

Fig2.Effect of number of fake base station on the percentage of events detected by base station(Sink simmulation scheme)

6. CONCLUSIONS

Prior work on location privacy in sensor networks assumed a local eavesdropper. This assumption is unrealistic given a well-funded, highly-motivated attacker. In this paper, we formalized the location privacy issues under a global eavesdropper and estimated the minimum average communication overhead needed to achieve a given level of privacy. We also presented techniques to provide location privacy to objects and sinks against a global eavesdropper. We used analysis and simulation to show how well these techniques perform in dealing with a global eavesdropper.

There are a number of directions that worth studying in the future. First, in this paper, we assume that the global eavesdropper does not compromise sensor nodes; he only performs traffic analysis without looking at contents of packets. However, in practice, the global eavesdropper may be able to compromise a subset of the sensor nodes in the field and per-form traffic analysis with additional knowledge from insiders. This presents interesting challenges to our methods. Second, some applications may require both source and sink location privacy. It will be interesting to investigate issues arising from integrating the source and sink location privacy techniques. Third, while we believe that it is possible for a well-funded and technically-savvy adversary to obtain a complete picture of network traffic, we recognize that complete coverage and perfect traffic analysis may be beyond the reach of some attackers. It is thus very interesting to study location privacy issues when the adversary can see only a fraction of the network traffic and must deal with the complexities of wireless signals. Finally, it takes time for the observations made by the adversarial network to reach the adversary for analysis and reaction. Studying the impact of such "delayed" analysis and reaction will be another interesting research direction.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. *Computer Networks*, 38(4):393–422, 2002.

[2] B. Bamba, L. Liu, P. Pesti, and T. Wang. Supporting anony-mous location queries in mobile environments with Privacy-Grid. In *Proc. Intl. Conference on World-Wide Web (WWW)*, 2008.

[3] BlueRadios Inc. Order and price info. http://www.blueradios.com/orderinfo.htm. Accessed in February 2006.

[4] B. Bollobas, D. Gamarnik, O. Riordan, and B. Sudakov. On the value of a random minimum weight Steiner tree. *Combinator-ica*, 24(2):187–207, 2004.

[5] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proc. IEEE Symposium on Security and Privacy (S&P)*, pages 197–213, May 2003.

[6] J. Deng, R. Han, and S. Mishra. Enhancing base station security in wireless sensor networks. Technical Report CU-CS-951-03, Dept. of Computer Science, University of Colorado, 2003.

[7] J. Deng, R. Han, and S. Mishra. Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks. In *Proc. Intl. Conf. on Dependable Systems and Networks (DSN)*, June 2004.

[8] J. Deng, R. Han, and S. Mishra. Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks. *Elsevier Pervasive and Mobile Computing Journal*, 2:159–186, April 2006.

[9] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *Proc. ACM Conf. on Computer and Communications Security (CCS)*, November 2002.

[10] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. L. Tan. Private queries in location based services: anonymizers are not necessary. In *Proc. ACM Intl. Conf. on Management of Data (SIGMOD)*, 2008.

[11] H. Gupta, Z. Zhou, S. Das, and Q. Gu. Connected sensor cover: self-organization of sensor networks for efficient query execution. *IEEE/ACM Trans. Netw.*, 14(1):55–67, 2006.

[12] J. Hill, M. Horton, R. Kling, and L. Krishnamurthy. The platforms enabling wireless sensor networks. *Commun. ACM*, 47(6):41–46, 2004.

[13] Y. Jian, S. Chen, Z. Zhang, and L. Zhang. Protecting receiver-location privacy in wireless sensor networks. In *Proc. IEEE INFOCOM*, May 2007.

[14] D. B. Johnson, D. A. Maltz, Y. Hu, and J. G. Jetcheva. The dynamic source routing protocol for mobile ad hoc networks (DSR). Internet Draft, February 2002. draft-ietf-manet-dsr-07.txt.

[15] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk. Enhancing source-location privacy in sensor network routing. In *Proc. Intl. Conf. on Distributed Computing Systems (ICDCS)*, June 2005.

[16] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In *Proc. ACM Conference on Computer and Communications Security (CCS)*, October 2003.

[17] K. Mehta, D. Liu, and M. Wright. Location privacy in sensor networks against a global eavesdropper. In *Proc. of IEEE Intl. Conf. on Network Protocols (ICNP)*, 2007.

[18] D. Niculescu and B. Nath. Ad hoc positioning system (APS) using AoA. In *Proceedings of IEEE INFOCOM*, April 2003.

[19] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon. Entrap-ping adversaries for source protection in sensor networks. In *Proc. Intl. Conf. on World of Wireless, Mobile, and Multimedia Networking (WoWMoM)*, June 2006.

[20] C. Ozturk, Y. Zhang, and W. Trappe. Source-location privacy in energy-constrained sensor network routing. In *Proc. Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, Oct. 2004.