# E-LPG: Energy Efficient Location Privacy Scheme Against Global Attackers in Sensor Networks

Sejun Song
*The Dwight Look College of Engineering*
*Texas A&M University, College Station, TX 77843, USA*
sjsong@tamu.edu

Hyungbae Park
*School of Computing and Engineering*
*University of Missouri - Kansas City, MO 64110, USA*
hpark@umkc.edu

Baek-Young Choi
*School of Computing and Engineering*
*University of Missouri - Kansas City, MO 64110, USA*
hpark@umkc.edu

***Abstract***

*Many sensor network security schemes protect the content of messages, while the contextual information is left vulnerable by disclosing the location of the monitored objects. Preserving location privacy is important and one of the most challenging issues in many mission critical sensor network applications. Prior solutions are mostly designed to protect privacy from local attackers who eavesdrop on traffic in a small region at a time. However, they can be easily defeated by highly motivated global attackers that can trace the entire network's communication events. Although a few recent privacy solutions are proposed against global attackers, they suffer from significant communication overhead as they inject dummy traffic or send messages in a globally synchronized manner. As a result, they consume a lot of energy to maintain a desired privacy level that makes the network lifetime shorter. We propose an energy-efficient source location privacy preserving solution, named the Energy Efficient Location Privacy Scheme against global attackers (E-LPG). E-LPG hides original source locations through a spatial scatter of messages using stealthy wormholes and through a temporal scatter using random delays when permitted. With a limited number of wormholes, E-LPG can achieve a high privacy level without incurring extra communication overhead. We evaluated the efficiency and effectiveness of E-LPG through theoretical analysis and extensive simulations. We have shown that E-LPG also produces dramatic synergistic results when used with other privacy schemes complementarily.*

## 1. Introduction

As wireless sensor networks are ad hoc networks built with low-power and low-cost sensor nodes, they have been considered as an enabling technology, especially for remote

resource surveillance applications in harsh environments. For example, sensor nodes can be deployed to assist the strategic movement of field-deployed soldiers or to track the habitat of endangered animals. Security is an essential requirement for those sensor network applications to be dependably used, as adversaries may monitor the network traffic and abuse it to endanger lives or inflict various manner of harm. In addition, these applications should function for as long as possible. It may be inconvenient or impossible to recharge node batteries.

While content privacy protection can be achieved by applying the traditional encryption and authentication mechanisms [10, 11, 25], for the most of the applications, preserving *contextual* privacy [19] is still one of the most challenging issues. Since sensor networks mostly use open-architecture based broadcast mediums, adversaries can easily observe the existence of data communications to infer critical information such as source sensor locations and target object movement patterns without knowing the content of the messages.

Many prior source location privacy preserving techniques [15, 19, 20, 23, 24] have been proposed to extend the safety period by injecting random/multiple paths toward the original source in order to thwart local traffic tracing attacks. However, when highly motivated attackers execute global traffic analysis/tracing attacks [22] that can monitor the entire network traffic, none of the aforementioned approaches will be successful. As the cost of sensors and radio devices is lowered, for adversaries in many scenarios, the reward of successful target tracking can be much higher than the cost of a global sensor network deployment. For example, catching the opponent soldiers' physical locations and movement patterns to preempt their action can pose a much more critical motivation than the cost of an adversary sensor network. Detecting an elephants' location with a few thousand dollars of sensor network costs (a single elephant catch can result in tens of thousand of dollars [28]) that can provide a greater profit for illegal ivory poachers. Considering the large gain of a successful attack and the low cost of sensor deployment, more adversaries may want to deploy attacker nodes globally to maximize their chances of detection. As the global attacker model becomes more realistic, it is critical for sensor networks to equip themselves with a contextual privacy preserving technology against global attackers.

A few recent source location privacy solutions are proposed that are against a global attacker model [21, 22, 29]. Their approaches are to hide the original source location by injecting either multiple fake simulated sources or sending network-wide periodic/statistical dummy messages. However, the approaches based on network-wide periodic or statistical dummy messages suffer from the significant overhead, and thus, they are not efficient in terms of the network lifetime. While the Source Simulation techniques [21] can reduce the excessive overhead by lowering the privacy level expectation, their safety period is then bounded by the number of fake simulated sources and the quality of movement simulation.

In this paper, we propose an efficient source location privacy preserving approach, named the Energy Efficient Location Privacy Scheme against a global attacker model (E-LPG). E-LPG hides an original source location using a spatial scatter with stealthy wormholes that can silently deflect an original communication event to a distant location. A wormhole is a stealth direct communication channel used by a pair of two distant sensors in a network. A wormhole can be established in various ways, for example, a wire-line or an out of band long-range wireless transmission. Once wormholes are established in a network, a message is sent by an original source node on one end of a wormhole channel without incurring any communication on the node's regular channel. It reappears on a regular wireless communication at the other end of the wormhole. Therefore, unless a global

adversary knows the phantom pattern of wormholes, it cannot capture the original source locations. In addition, the established wormholes may be used probabilistically to further hide their existence over a long term. Therefore, unlike the existing source location privacy mechanisms against global attackers, E-LPG achieves a high privacy level without incurring extra communication overhead or latency.

As for a practical deployment of wormholes in sensor networks, we note that wormhole nodes have often been used as a security attack to be protected against [9, 18]. In addition, a few recent studies have used wormholes positively in order to improve energy consumption [7, 17] and to overcome jamming attacks [5, 12]. As the effectiveness of E-LPG depends upon the feasibility of deploying multiple wormhole nodes, we are also keenly aware of the potential overhead. To this end, we perform an effectiveness analysis to show that E-LPG can provide high privacy levels with a small set of wormholes while maintaining the flexibility of a sensor network's self-organization. We also discuss a synergistic effect when E-LPG is used with other existing location privacy schemes complementarily, such as the Source Simulation. Since movement patterns may be inferred by the sophisticated timing correlation of detected network traffic, E-LPG further disguises movement patterns for the non-real time applications by using a temporal scatter that selectively controls the timing of message forwarding.

The contributions in this paper are as follows:

- We propose a privacy preserving technique against global attackers that can achieve a high privacy level without incurring extra communication overhead by using spatial deflect with stealthy wormholes. A temporal scatter of messages may be used for elastic applications to add an uncertainty of location to global attackers.
- We quantify the privacy level of E-LPG and evaluate the effectiveness of a spatial scatter and a temporal scatter, respectively, and the effectiveness when they are used simultaneously as well via analysis and extensive simulations.
- We quantify the required proportion of wormholes corresponding to the level of uncertainty for planning a budget of a hybrid network.
- We present a synergistic effect when E-LPG is combined with other approaches such as the Source Simulation scheme.

The rest of the paper is organized as follows. In Section 2, we first define the wormhole, network, and adversary models used in this paper. Section 3 presents a survey of existing privacy preserving techniques in sensor networks. We discuss the characteristics of the proposed E-LPG approach in Section 4. The analysis and evaluation of E-LPG are presented in Sections 5 and 6, respectively. We conclude the paper in Section 7.

## 2. System Models

In this section, we describe the wormhole, network, and adversary models used in this paper.

### 2.1. Wormhole Model

- A wormhole is a stealthy communication channel between a pair of two distant sensors, and can be established by either a wire-line or an out of band long-range wireless

communication. It can be stretched into multiple hop wormholes

- A wormhole channel length is assumed to be greater than the transmission range of the regular wireless sensor link, so that it can effectively deflect the original source location spatially.
- Wormholes are randomly deployed in a field. Multiple wormholes may be connected together extending an effective wormhole channel length and adding randomness in the routing. A receiving wormhole node can forward a packet toward a sink node through a regular channel or another wormhole node depending on the routing algorithms. For example, in Figure 1, two wormholes *WH(A,B)* and *WH(B,C)* are directly connected. Although the target is detected by wormhole node $A$, the communication event will start to be observed at wormhole node $C$ in this scenario, when node $B$ uses wormhole *WH(B,C)*. Hence, the attacker node $Y$ will first detect the source event instead of the attacker node $X$. Considering the physical resource limitation, we assume up to only two wormhole ports for a wormhole node (i.e., the wormhole node $B$ has two wormhole ports).
- The sink node can identify the original source address by the original source address encrypted within the packet payload.

### 2.2. Network Model

- To implement an energy-efficient privacy scheme, we assume that there is a process to elect a designated node for sending a message to a sink by clustering the network. The clustering algorithm can be found in [13, 14]. In E-LPG, we prefer to select a wormhole node as a cluster head and only the cluster head will report the event without data aggregation from the members in a cluster. For example, in Figure 1, although sensors $A$, $A_1$, and $A_2$ can detect a target, only a designated node $A$ (wormhole node) relays the event to the sink.
- The sensor nodes are assumed to have the localization [6, 16, 31] and neighbor discovery schemes [2, 27].
- The routing information to the sink node is known. Either a hop-count-based or a delay-based routing [1] may be used.

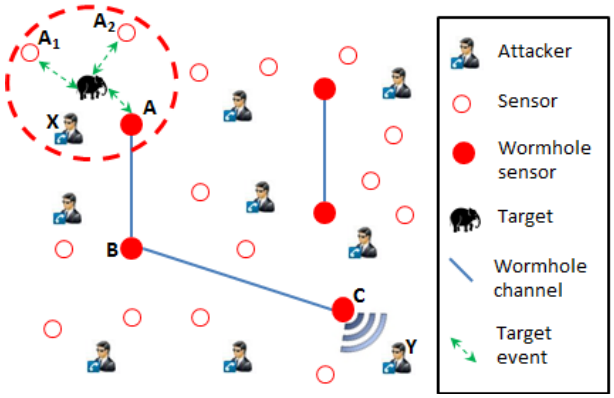



**Figure 1. An example of wormhole deployments and global attack adversary**

- The wormhole nodes may participate in routing as regular nodes and deliver the packets earlier or with shorter hops, or as a preferred node, unless it worsens the delivery time or increases the hop length toward a sink node.
- The content privacy of each message can be provided by data encryption and authentication mechanisms [10, 11, 25]. We focus on the contextual privacy as the content privacy service is out of the scope of this paper.

### 2.3. Adversary Model

- The adversary can monitor and trace all of the network traffic. Note that the price for sensor nodes keeps decreasing, and an attacker can build a snooping sensor network of 400 nodes with only $10,000, at the current price for a BlueRadios SMT Module, which is around $25 [4]. Moreover, the number of snooping nodes can typically be smaller than the number of nodes of a target network since they only monitor specific wireless signals of target network sensors rather than directly sensing the targets in the environment.
- The adversary cannot eavesdrop on the communication events between a target object and sensor nodes, as it is a very challenging problem in practice. The target objects and sensor nodes may use special signal emitters or sensing devices, respectively. For example, in Figure 1, although sensors $A$, $A_1$, and $A_2$ can detect a target, the attacker $X$ cannot detect the original communication event.
- The adversary's main objective is to identify the target object location(s). The adversary can use network traffic observations such as the packet transmission location, as well as time and frequency, to perform traffic analysis and infer the locations of target objects. Since the target event can be sensed by a proximate sensor node and the sensor node becomes the source of the communication event, we assume that the adversary can directly deduce the target object locations from the captured communication events.
- The adversary just monitors and traces the network traffic and does not interfere with the network traffic by injecting packets or jamming signals.
- The adversary does not know the wormhole deployment patterns and does not actively perform any wormhole detection scheme.

## 3. Related Work

Many source location privacy preserving algorithms have been proposed in sensor networks. Most of the approaches are designed to extend the safety period against local traffic tracing attacks. For example, P. Kamat et al. [19] introduced fake source-based routing and phantom routing. The fake source-based routing achieves source privacy by creating multiple sources that inject fake messages along with the original message. The phantom routing makes the original source message walk a random path before routing to the sink node. When the packet is captured by the local attacker, the source privacy can be ensured, as the packet source is far from the original source. However, as the pure random walks may cancel each other by going forward and backward, they use a directed walk. Y. Li et al. [20] provided source location privacy by routing the message to randomly chosen one or

more intermediate nodes before the packets were finally transmitted to the sink. The angle and quadrant information are used to select intermediate nodes. The work in [23] extended a safe period by activating several looping traps on the routing path between the source and sink nodes. When a local attacker traces back the routing path toward the source location, it takes a longer time as it will follow the looping traps repeatedly. However, as these algorithms are based upon the assumption of the local attacker, they are effective only if they are applied before the local attacker's observation. Hence, if a global attacker model where the attacker can monitor the entire network traffic is applied, the communication events of any initial sensor can be identified. Thus, the solutions against local attackers will be easily defeated by global attackers.

There are a few recent source location privacy solutions against global attackers such as a periodic collection [21], a statistically strong source anonymity (SSSA) scheme [29], and $k$-anonymity Source Simulation schemes [21, 29]. In a periodic collection approach, all nodes send fake or real messages synchronously in a period. Hence, the network traffic patterns observed by global attackers are periodic regardless of the individual node's network traffic events. Although it can achieve a maximum safety period, it is not a practical solution due to the excessive communication overhead and energy consumption as well as the latency that prohibits real time transmission. The SSSA scheme focuses on reducing the latency in support of real time transmission. Involved nodes send messages in statistically different message periods. When there is an event message to send, it can be sent immediately without waiting for the message period. It is hard for global attackers to distinguish the event message from the periodical messages, because the message event can be considered as the statistical disturbance. Although the SSSA reduces a latency problem, it is still suffering greatly by the excessive communication overhead and energy consumption. The $k$-anonymity Source Simulation schemes are proposed to mitigate the periodic collection's traffic overhead by lowering the privacy level. They create multiple fake sources/paths to extend the safety period of the original source/trace. The safety period is then bounded by the number of candidate fake sources/paths as well as by the effectiveness of a fake-source simulation model of the real object's movement trajectory.

In our previous work [26], the usage of wormhole pairs was proposed for preserving the contextual privacy against a global attacker in a sensor network. In this paper, we first extend the concept of a wormhole so that the stealth communication can go beyond a pair, and can be stretched into multiple hop wormholes. We also introduce temporal scatter strategy for non-real time applications in order to further increase anonymity. Furthermore, we provide theoretical analysis to quantify the level of privacy. Note that E-LPG can be used with other privacy schemes in a complementary manner, and provides significant synergy in improving privacy.

## 4. E-LPG Approach

In this section, we first explain the proposed E-LPG algorithm, then discuss several aspects of the E-LPG approach, especially with limited deployment of wormholes.

The E-LPG algorithm is illustrated in Algorithm 1. For simplicity of presentation, we assume that a sensor network has already been deployed, and each node knows its neighbor nodes by its neighbor discovery mechanism and identifies which neighbors are wormhole nodes. As discussed in Section 2, when a sensor node senses a target event, it sends out a

**Algorithm 1** E-LPG Algorithm – runs on a wormhole node

```
if senses a target event then
  creates a report message;
  if allows latency then
    applies temporal scatter;
  end if
  selects a wormhole port and forwards the report message;
else if receives a report message and is a forwarding node then
  select-forwarding-port-type( );
  if allows latency then
    applies temporal scatter;
  end if
  if a wormhole port is selected then
    forwards the report message;
  else if a regular wireless port is selected then
    applies a regular routing algorithm to decide the next forwarding node;
    forwards the report message;
  end if
end if
```

report message toward a sink node to update the target movement. We assume that the sensor nodes within a small communication area have already agreed upon their designated node that can create and send a report message.

A wormhole node may sense a target event or receive a report message. When a wormhole node senses a target event, it creates a report message that includes target event information and original source information within its payload, that is encrypted. It also puts a null in the next forwarding node value within its message header. It selects a wormhole port to forward the report message to the other side's wormhole node. When a wormhole node receives a report message, if the messages's next forwarding node field is empty, then the wormhole node recognizes itself as a forwarding node sending the message using its regular communication port. It applies a regular routing algorithm [14] to select the next forwarding node of the message. Since a wormhole can shorten the hop count toward a sink node, a wormhole neighbor node is likely to be chosen as the next forwarding node, when available. The report message header is updated with a newly selected next forwarding node.

In addition, a sensor node may perform a temporal scatter where it selectively controls the timing of report messages before forwarding. The added random latency will confuse global attackers in the order of messages observed. For instance, in Figure 2, the original order of events occurred in the sensor network is node 1, 2, 3, then 4. With the random latency in each node, $l_i$s at node $i$, a global attacker will observe traffic in the order of nodes 1, 3, 4, then 2 which breaks the original trace of the target movements. We use the temporal scatter scheme only when an application allows some latency of the message delivery. The latency can be controlled so that it conforms to the requirement of the application. For example, the maximum delay per node is bounded, or the expectation of the random delay variable is to be a given value, say $\mu_{del}$.

Let us illustrate example scenarios of E-LPG usage with Figure 3. The degree of a spatial scatter with wormholes would be decided by the privacy requirement and the available budget of specific applications. For instance, life-critical military applications may deploy at

least one wormhole for each area to completely eliminate the target traceability. As depicted in Figure 3 (a), the global attackers' view (notated as red explosion marks with attached numbers to display the temporal order of observation) does not reveal a soldier's original movement pattern from $X$ to $Y$ at all. Meanwhile, a small number of wormholes may be used to partially hide the source locations. In some cases, a sophisticated global attacker may be able to find the original target movement pattern from a series of network traffic observations and analysis. In Figure 3 (b), the global attackers may observe unrealistic target movement patterns from the spatial and temporal correlation. They can then deduce a soldier's original movement pattern by filtering out a couple of outliers such as the events on times 3 and 6 in Figure 3 (c). For the given same degree of the spatial scatter, Figure 3 (d) illustrates a case where a temporal scatter of messages effectively preserves the privacy of the original movement pattern.

The privacy level can be further enhanced by employing E-LPG complementarily with other schemes. Specifically, we discuss how a limited number of wormholes, along with the Source Simulation technique can effectively preserve the privacy of target movement against the global attacker's observation. The Source Simulation algorithm alone, as illustrated in Figure 4 (a), simulates and generates three additional movement patterns ($k = 3$) along with an original movement pattern (i.e., the trajectory of an elephant). The numbers next to the nodes indicate the timing information of observed communication signals. A global attacker can observe all the four potential movement patterns including the original source trace. Although it may take time (a longer safety period), it can detect the original movement pattern eventually by an exhaustive search from the patterns. Even worse, due to the difficulty of simulating a realistic object movement trajectory [21, 29] in fake Source Simulation, some simulated fake sources may be filtered out easily. In contrast, Figure 4 (b) depicts an example of observed signals with 25% of wormhole (yellow line) proportions (that is, on average 2 wormholes out of 8 sensor areas) are used together with the Source Simulation ($k = 3$). We observe that the sequential traces we have seen in Figure 4 (a) have been eliminated by a spatial scatter. As the simulated sources benefit from the wormholes, the impact of a spatial scatter is synergistically multiplied, and the privacy level is significantly improved. In addition, as we have described in Figure 3 (d), a temporal scatter can be also used to further enhance the privacy level. In the following sections, we analytically quantify and evaluate that E-LPG, with a limited wormhole deployment, can

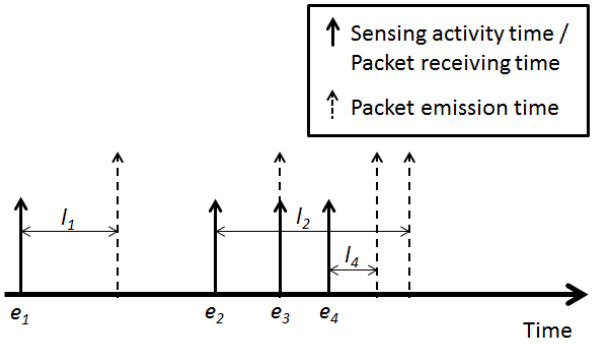



**Figure 2. An example of distorted sequences of packet transmission by temporal scatter**

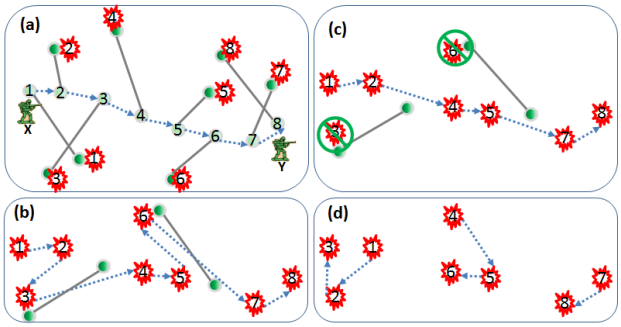
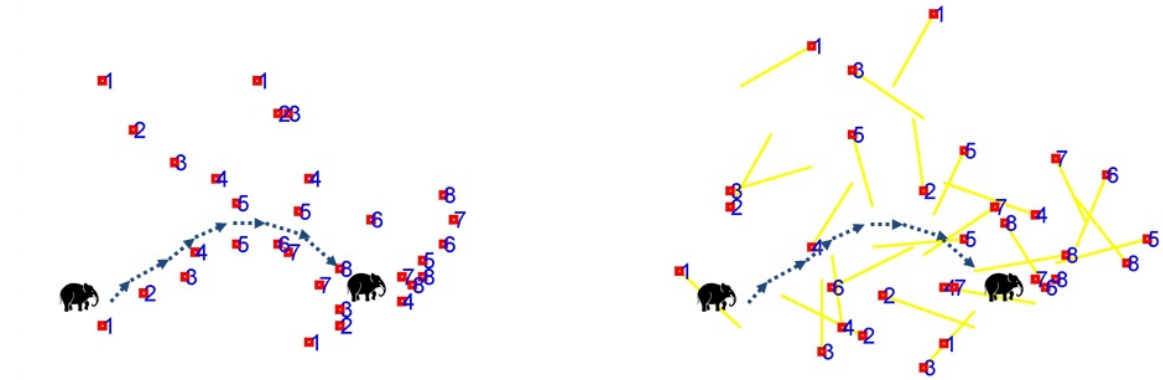



**Figure 3. Source trace scatter examples ((a) Observed trace with spatial scatter (b) Observed trace with partial spatial scatter (c) Adversary's trace detection after outlier removal (d) Observed trace with temporal scatter)**



(a) Source Simulation ($k = 3$, $p_{wh} = 0$) (b) E-LPG with Source Simulation ($k = 3$, $p_{wh} = .25$)

**Figure 4. Illustration of global attacker's view: a complementary usage of E-LPG and Source Simulation**

produce dramatic synergistic results in improving privacy when used complementarily with other privacy schemes.

## 5. Analysis

In this section, we analytically quantify source location privacy and communication costs.

We measure the privacy level via the uncertainty area that an attacker has to search to find out the actual location of a target. A higher privacy is achieved by a greater uncertainty area, and it also relates to a longer safety period. Figure 5 illustrates a scenario where the uncertainty area is increased by the spatial scatter of E-LPG with a wormhole. The star represents an instance of a target object location. Given a communication observation seen via node $A$, without any wormhole, to an attacker, the target is expected to be within a sensing range of $d$ around sensor node $A$, resulting in the uncertainty area, $U_A = \pi d^2$. Once a wormhole is used at node $A$ to node $B$, an attacker would have to search the surrounding area from the observed point $B$ and extends the search area until the target is found. Thus,

the uncertainty is increased at most by $U_{wh(A,B)} \leq \pi D^2$. Later, we use $U^{\mathcal{A}}$ and $U^{wh(\mathcal{A})}$ to denote the uncertainty areas for a source without and with wormholes, respectively.

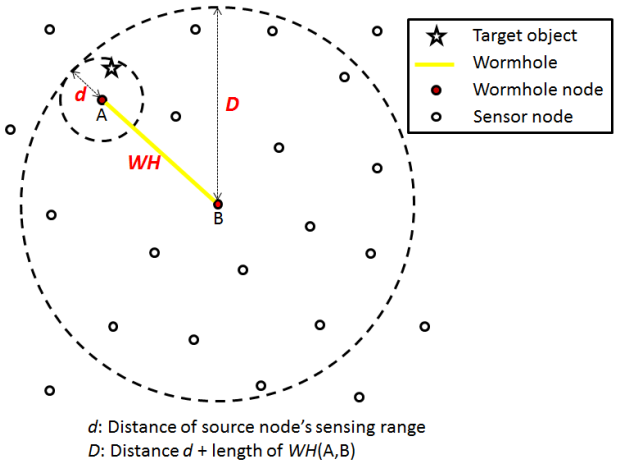



**Figure 5. Increased uncertainty by length of $WH(A,B)$**

Suppose a sensor network contains randomly deployed wormholes with the proportion of $p_{wh}$, and a target object $o$ moves from one location to another location encountering a set of multiple sensing areas along the way, $\mathcal{A}^o$. Each location may be sensed by a sensor with a wormhole with a probability of $p_{wh}$ or a sensor without a wormhole with a probability of $1 - p_{wh}$. Note that $p_{wh} = 1$ means all the $N$ sensing areas of the field (a set of grids or clusters) are equipped with at least one wormhole, that is the number of wormholes is equal or greater than $N/2$.

Let us consider the expectation of the uncertainty area of a target object $o$'s trace $\mathbb{T}^o$. The expectation $(E)$ of the uncertainty area of a target trace $(\mathbb{T}^o)$ achieved by E-LPG is computed as below:

$$E(\mathbb{T}^o) \leq \frac{\sum_{i \in \mathcal{A}^o} \left\{ (1 - p_{wh}) U_i^{\mathcal{A}} + p_{wh} U_i^{wh(\mathcal{A})} \right\}}{|\mathcal{A}^o|} \tag{1}$$

Note that our analysis measures the uncertainty of target traces more generally than the one in [21] where a point uncertainty is measured by the number of the nodes that may sense the target.

In case the Source Simulation scheme is complementarily used with E-LPG, the uncertainty caused by the paths of fake traces, as well as the wormholes, impacts all those paths. Suppose $I$ and $\mathcal{A}^T$ denote a set of all targets and fake sources as well as a set of all sensing areas that are traversed by the objects in $I$, respectively.

$$\mathbb{A}^T = \cup_{i \in I} A^i \tag{2}$$

Then, the trace uncertainty of an object $o$, only with the Source Simulation, is formally defined with the entropy (in bits) as follows:

$$b = \log_2 \frac{\sum_{i \in \mathcal{A}^T} U_i^{\mathcal{A}}}{|\mathcal{A}^o|} \tag{3}$$

In addition, the trace uncertainty of the spatial scatter of E-LPG with the Source Simulation can be formulated in the same manner as Equation (3):

$$b = \log_2 \frac{\sum_{i \in \mathcal{A}^T} \left\{ (1 - p_{wh}) U_i^{\mathcal{A}} + p_{wh} U_i^{wh(\mathcal{A})} \right\}}{|\mathcal{A}^o|} \tag{4}$$

Here, we quantify the privacy achieved by the temporal scatter of E-LPG. A higher privacy is achieved by the greater mean delay as well as the higher probability of applying delay. We quantify temporal scatter privacy taking the Source Simulation scheme into account. Meanwhile, the target is moving around the field and sensor nodes are sensing the target while some of the sensor nodes selected with the probability of $p_{del}$, will intentionally delay sending the report packets as long as $\mu_{del}$. Then, the adversary's trace on the target will be discontinued until the next report packets are sent by another sensor node. Therefore, these delayed events create more distinct traces. As $p_{del}$ and $\mu_{del}$ increase, the probability to eliminate the sequential trace is higher. The expectation ($E$) of the uncertainty area of a target object, $o$'s trace $\mathbb{T}^o$ is bounded as below:

$$E(\mathbb{T}^o) \leq \frac{\sum_{i \in \mathcal{A}^o} \left( U_i^{\mathcal{A}} + p_{del} \mu_{del} U_i^{\mathcal{A}} \right)}{|\mathcal{A}^o|} \tag{5}$$

Then, the following formula represents the privacy (in bit) achieved by the temporal scatter with the Source Simulation.

$$b = \log_2 \frac{\sum_{i \in \mathcal{A}^T} \left( U_i^{\mathcal{A}} + p_{del} \mu_{del} U_i^{\mathcal{A}} \right)}{|\mathcal{A}^o|} \tag{6}$$

Now, we put together the uncertainty of both the spatial scatter and temporal scatter schemes. The equation below represents the level of uncertainty achieved by spatial and temporal scatters as well as the Source Simulation.

$$b = \log_2 \frac{\sum_{i \in \mathcal{A}^T} \mathbb{U}}{|\mathcal{A}^o|} \tag{7}$$

where

$$\mathbb{U} = (1 - p_{wh}) U_i^{\mathcal{A}} + p_{wh} U_i^{wh(\mathcal{A})} + p_{del} \mu_{del} U_i^{\mathcal{A}} \tag{8}$$

Next, we derive the proportion of wormholes in the network in order to achieve a given level of uncertainty. It enables us to plan a budget of the hybrid network in satisfying a certain level of uncertainty. Suppose $n_o$ and $n_f$ denote the number of target objects and the number of the fake sources, respectively. Then we can compute the required proportion of wormholes corresponding to the level of uncertainty ($b$) as follows:

$$p_{wh} = \frac{2^b - (n_o + n_f) U^{\mathcal{A}} (1 + p_{del} \mu_{del})}{(n_o + n_f) \left\{ U^{wh(\mathcal{A})} - U^{\mathcal{A}} \right\}} \tag{9}$$

Now we consider the communication cost incurred for a certain privacy level for E-LPG as well as the Source Simulation. It is measured by the number of messages incurred in the network. The communication cost is utilized as a metric to measure the overall energy consumption in networks in order to compare the energy efficiency of the different schemes. The communication cost of the Source Simulation increases proportionally to the number of

objects and fake sources. Meanwhile, E-LPG may reduce the hop counts when encountered with wormholes [7]. Let $H_{avg}$ be an average hop count of a path from a source and a sink. It can be represented as follows:

$$H_{avg} = \frac{1}{N} \times \left( \sum_{i=1}^{N} P_i \cdot H_{max} \right) \tag{10}$$

where $H_{max}$ denotes the maximum distance between an object and the sink in the network and $P_i$ is a normal random distribution ranging from 0 to 1. The following equations, (11) and (12), show the communication costs for the Source Simulation ($C_s$) and E-LPG ($C_c$), respectively.

$$C_s = H_{avg} \times (n_o + n_f) \tag{11}$$

$$C_c = \{(1 - p_{wh})H_{avg} + p_{wh}\,(H_{avg} - W_{avg\_sav})\} \times (n_o + n_f) \tag{12}$$

where $W_{avg\_sav}$ is the average hop count reduced by wormholes towards a sink. Depending on the direction of how it is laid in the network, the saved distance can range from 0 to $len_{wh}$. $W_{avg\_sav}$ can be described as follows:

$$W_{avg\_sav} = len_{wh} \times P_i \tag{13}$$

## 6. Evaluation

In this section, we evaluate the performance of E-LPG through extensive simulations. We first explore the uncertainty level achieved by the spatial and temporal scatter schemes of E-LPG under various conditions. We then compare the performance of E-LPG and that of the Source Simulation approach. We also investigate the synergistic effect of E-LPG with the Source Simulation in terms of the uncertainty level and the communication cost.

We implemented our discrete event simulator in Matlab. The simulation system settings are listed in Table 1. In our simulation system setup, 400 sensor nodes were distributed randomly in a square field of 100 by 100 distance unit network area. The same number of eavesdropper sensor nodes was also randomly distributed in the network field in order to monitor all of the network traffic. We assumed that each sensor node's sensing and transmission ranges were both 5 distance units. We set one $I_m$ for the communication time interval between its immediate neighbors. A sink node was placed in the center of the network. The target mobility model used in the simulation was a Random Waypoint with less than 10 distance units per movement. Total simulation time was set from 100 to 1,000 $I_m$s. For the system setting, we varied the simulation parameters as summarized in Table 2 to evaluate E-LPG with diverse scenarios.

We first observed the impact of the pure spatial scatter on the level of uncertainty varying the proportion ($p_{wh}$) and length ($len_{wh}$) of wormholes. While changing those spatial scatter parameters, all other settings remained constant. As shown in Figure 6, when the longer length and higher proportion of wormholes are used in the network, the higher level of uncertainty can be achieved. The results also showed that the increment of the proportion of wormholes improved the uncertainty level more significantly than the increment of the

**Table 1. Simulation Sensor Network Settings**

| System Settings | Values |
|---|---|
| Area of field | 100×100 |
| Number of sensor nodes | 400 |
| Number of eavesdropper sensor nodes | 400 |
| Sensing range ($R_s$) | 5 |
| Transmission range ($R_t$) | 5 |
| Neighbor communication time interval ($I_m$) | 1 |

**Table 2. Simulation Parameter Settings**

| Parameter Settings | Values |
|---|---|
| Number of fake sources ($k$) | 0, 1, 2,..., 24 |
| Proportion of wormholes ($p_{wh}$) | 0, .1, .2,..., .5 |
| Length of wormholes ($len_{wh}$) | $2R_t$, $3R_t$,...,$7R_t$ |
| Probability of delay application ($p_{del}$) | 0, .1, .2,..., 1 |
| Mean delay time ($\mu_{del}$) | $I_m \sim 10I_m$ |

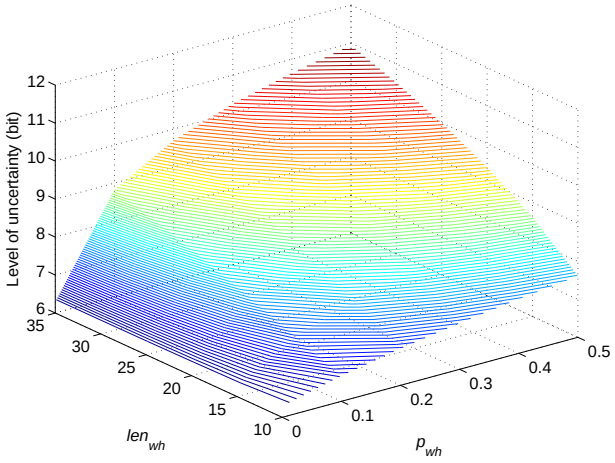



**Figure 6. E-LPG with spatial scatter only: Level of uncertainty varying proportion ($p_{wh}$) and length ($len_{wh}$) of wormholes**

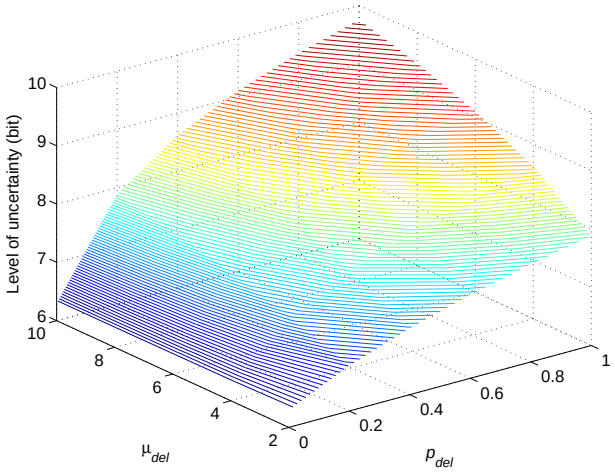



**Figure 7. E-LPG with temporal scatter only: Level of uncertainty varying probability of delay application ($p_{del}$) and mean delay time ($\mu_{del}$)**

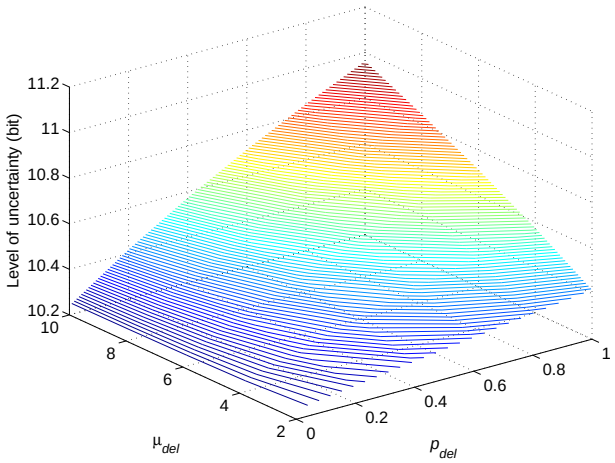



**Figure 8. E-LPG with spatial and temporal scatters: Level of uncertainty varying probability of delay application ($p_{del}$) and mean delay time ($\mu_{del}$) for a given spatial scatter ($p_{wh} = .3$, $len_{wh} = 6R_t$)**

length of the wormholes. It provided an insight as to how we can allocate the E-LPG's spatial scatter budget to satisfy a given level of uncertainty.

The level of uncertainty achieved by the temporal scatter of E-LPG was evaluated by varying the probability of the delay application ($p_{del}$) and mean delay time ($\mu_{del}$). While varying the temporal scatter parameters, all other settings remained constant. The result in Figure 7 shows the impact of the pure temporal scatter to the level of uncertainty. The result illustrates that the impact of $p_{del}$ is significantly higher than that of $\mu_{del}$. This intuitively, indicates even if there are a few long delayed events that scatter temporal sequences, adversaries can easily deduce the source movement patterns from the rest of the event sequences. We can effectively achieve the higher level of uncertainty by mainly changing $p_{del}$.

We also investigated the impact of the temporal scatter on the performance of the spatial scatter. Figure 8 shows the level of uncertainty achieved with the fixed spatial scatter ($p_{wh} = .3$, $len_{wh} = 6R_t$) parameters and varying the probability of the delay application ($p_{del}$) and mean delay time ($\mu_{del}$). The initial level of uncertainty achieved by the spatial scatter is 10.24 when the parameters of the spatial scatter of E-LPG were fixed to $p_{wh} = .3$ and $len_{wh} = 6R_t$. As seen in Figure 8, complementary usage of the temporal scatter proportionally improves the overall performance in terms of the level of uncertainty.

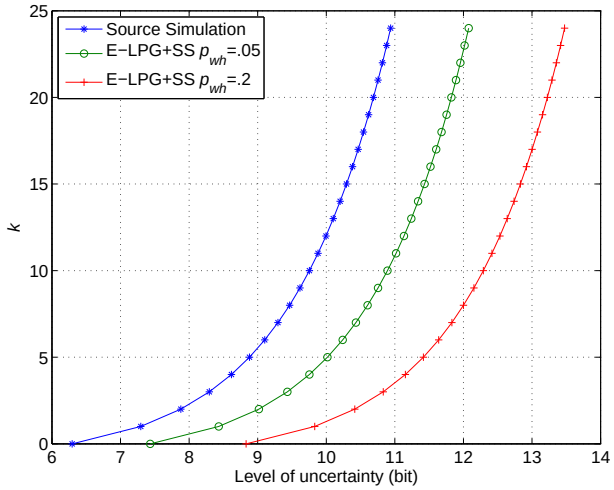



**Figure 9. Number of fake sources to achieve a given level of privacy: Source Simulation only vs. E-LPG+Source Simulation (E-LPG: $len_{wh} = 6R_t$, $p_{del} = .5$, $\mu_{del} = 5$)**

We compared the level of uncertainty of the Source Simulation scheme only and that of E-LPG combined with the Source Simulation together in Figure 9. The result shows that it requires almost 25 fake sources in the pure Source Simulation scheme to achieve the uncertainty level 11. However, if E-LPG with the Source Simulation is used, the same level of privacy can be achieved with the drastically less number of fake sources such as one second for E-LPG with $p_{wh} = .05$ and one eighth for E-LPG with $p_{wh} = .2$. By lowering the number of fake sources in the network, we can decrease the communication cost. As a result, we can reduce energy consumption [3, 8, 30] which is a critical requirement in the sensor network.

Next we compared E-LPG and the Source Simulation in terms of the proportion of

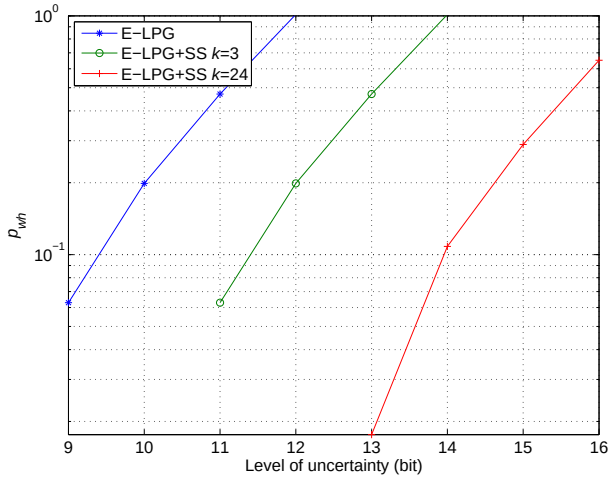



**Figure 10. Proportion of wormholes to achieve a given level of privacy: E-LPG only vs. E-LPG+Source Simulation (E-LPG: $len_{wh} = 6R_t$, $p_{del} = .5$, $\mu_{del} = 5$)**

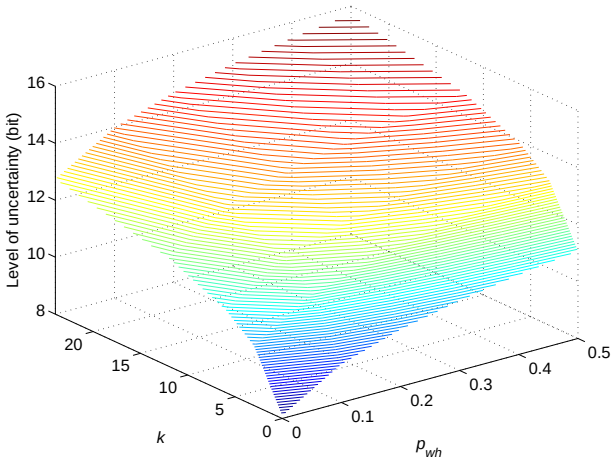



**Figure 11. Performance of E-LPG with Source Simulation ($k$=number of fake sources, $len_{wh} = 6R_t$, $p_{del} = .5$, $\mu_{del} = 5$)**

wormholes needed to achieve a given level of privacy in Figure 10. Although a certain privacy level can be achieved only by E-LPG, deploying a high proportion of wormholes into the network is not desirable especially when a budget is limited. A higher level of privacy can be achieved easily from complementary usage of E-LPG with the Source Simulation. As illustrated in Figure 10, it requires almost 50% of wormhole proportion ($p_{wh} = .5$) to achieve the uncertainty level 11. However, if E-LPG is used with only a few fake sources ($k = 3$), the same level of privacy can be achieved with a drastically less wormhole proportion (only around 6%).

Figure 11 presents the level of uncertainty with the combined parameters of the proportion ($p_{wh}$) of wormholes and the number of fake sources ($k$) as used in Figure 9 and Figure 10.

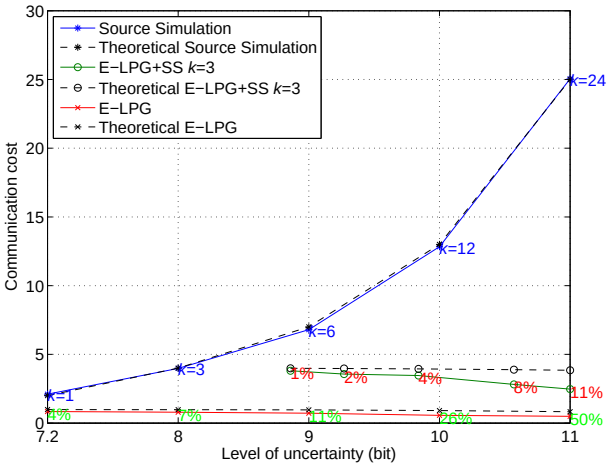



**Figure 12. Communication cost: E-LPG ($len_{wh} = 6R_t$, varying $p_{wh}$), E-LPG with Source Simulation ($k$ = 3, $len_{wh} = 6R_t$, varying $p_{wh}$), and Source Simulation (varying $k$)**

Finally, we evaluated the communication cost of E-LPG, E-LPG with the Source Simulation, and the Source Simulation in order to achieve a given privacy level. The results from both simulation and theoretical analysis are shown in Figure 12. The communication cost is presented as the ratio of the total number of messages after applying a scheme to that of without applying any scheme. As seen in the graph, the level of uncertainty 9 can be achieved either using the Source Simulation with six fake sources or using E-LPG with $p_{wh} = .11$ wormholes. To achieve the same level of uncertainty, that is 9, the amount of traffic caused by the Source Simulation approach can be almost 7 times more than that of E-LPG. The result clearly demonstrates that E-LPG is more efficient in communication cost overhead than the Source Simulation scheme. The amount of traffic in the Source Simulation scheme is linearly increased by the increment of the level of uncertainty. The Source Simulation scheme needs to have an additional 24 fake sources to achieve the privacy level 11. However, it causes almost 25 times more messages that are proportional to the number of fake sources. This implies that having a large amount of communication costs is inevitable for the Source Simulation approach to achieve a higher level of privacy. In contrast, it should be noted that the amount of traffic caused by E-LPG is slightly decreased for the higher level of uncertainties, as wormholes are also used to shorten the routing

path. Although E-LPG with the Source Simulation causes slightly more traffic than pure E-LPG proportionally to the number of fake sources, it also decreases the communication costs along with a higher level of uncertainty. The results validate that E-LPG can reduce excessive traffic by taking a drastically different approach than the Source Simulation while achieving a high level of privacy. We have also presented that our analysis is valid since the theoretical results are as close as the measured communication costs from the simulations.

## 7. Conclusion

Prior approaches on location privacy in sensor networks are mostly designed against local attackers and thus, can be easily defeated by highly motivated global attackers. Although a few solutions against global attackers have recently been proposed, they inject fake traffic and/or send traffic in a synchronized manner in order to confuse global attackers and thereby suffer from significant communication overhead and latency. We have presented the Energy Efficient Location Privacy Scheme against Global Attackers (E-LPG) that effectively and efficiently preserves source location privacy. E-LPG uses a limited number of stealthy wormholes to enhance privacy in sensor networks. Wormholes provide a spatial scatter of traffic using hybrid link architecture without incurring any extra communication overhead. We also employed random delays of traffic for a temporal scatter when the applications allowed a controlled amount of delay in message delivery. We have analytically quantified the source location privacy level of our approaches, and shown how to control the level of uncertainty with a limited budget. We have evaluated the efficiency and effectiveness of E-LPG through extensive simulations with various parameters. E-LPG can be used complementarily with other privacy schemes, and we have shown E-LPG produces dramatic synergistic results in improving privacy when used with a fake traffic injection scheme. As for future work, we are investigating strategic wormhole deployment schemes that improve network resilience and performance while providing location privacy.

## References

[1] K. Akkaya and M. Younis. A Survey of Routing Protocols in Wireless Sensor Networks. *in the Elsevier Ad Hoc Network Journal*, 3:325–349, 2005.

[2] D. Angelosante, E. Biglieri, and M. Lops. A Simple Algorithm for Neighbor Discovery in Wireless Networks. In *Proceedings of IEEE ICASSP*, 2007.

[3] Seema Bandyopadhyay and E.J. Coyle. An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks. In *In Proceedings of IEEE INFOCOM*, pages 1713–1723, 2003.

[4] BlueRadios Inc. Order and Price Information. http://www.blueradios.com/orderinfo_new.htm, 2011.

[5] Mario Cagalj, Srdjan Capkun, and Jean-Pierre Hubaux. Wormhole-Based Antijamming Techniques in Sensor Networks. *IEEE Transactions on Mobile Computing*, 6(1):100–114, 2007.

[6] X. Cheng, A. Thaeler, G. Xue, and D. Chen. Tps: A Time-based Positioning Scheme for Outdoor Wireless Sensor Networks. In *IEEE INFOCOM*, volume 4, pages 2685–2696, 2004.

[7] Rohan Chitradurga and Ahmed Helmy. Analysis of Wired Short Cuts in Wireless Sensor Networks. In *Proceedings of International Conference on Pervasive Services (ICPS)*, pages 167–176, 2004.

[8] J. Chou, D. Petrovic, and Kannan Ramachandran. A Distributed and Adaptive Signal Processing Approach to Reducing Energy Consumption in Sensor Networks. In *In Proceedings of IEEE INFOCOM*, volume 2, pages 1054–1062, 2003.

[9] Yih chun Hu, Adrian Perrig, and David B. Johnson. Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks. In *IEEE INFOCOM*, pages 1976–1986, 2003.

[10] J. Deng, R. Han, and S. Mishra. Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks. In *Proceedings of International Conference on Dependable Systems and Networks (DSN)*, 2004.

[11] L. Eschenaur and V. Gligor. A Key-Management Scheme for Distributed Sensor Networks. In *Proceedings of 9th ACM conference on Computer and Communications Security*, 2002.

[12] Alessandra Flammini, Paolo Ferrari, Daniele Marioli, Emiliano Sisinni, and Andrea Taroni. Wired and Wireless Sensor Networks for Industrial Applications. In *Microelectronics Journal*, volume 40, pages 1322–1336, 2009.

[13] Wendi Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan. Energy-Efficient Communication Protocol for Wireless Microsensor Networks. In *Proceedings of the 33rd International Conference on System Sciences*, pages 3005–3014, 2000.

[14] Wendi Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan. An Application-Specific Protocol Architecture for Wireless Microsensor Networks. *IEEE Transactions on Wireless Communications*, 1(4):660–670, 2002.

[15] B. Hoh and M. Gruteser. Protecting Location Privacy Through Path Confusion. In *Securecomm*, pages 194–205, 2005.

[16] Lingxuan Hu and David Evans. Localization for mobile sensor networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking (Mobicom)*, pages 45–57, 2004.

[17] W. Hu, C. T. Chou, S. Jha, and N. Bulusu. Deploying Long-Lived and Cost-Effective Hybrid Sensor Networks. In *Proceedings of The First Workshop on Broadband Advanced Sensor Networks (BaseNets)*, 2004.

[18] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Wormhole Attacks in Wireless Networks. *IEEE JOURNAL on SELECTED AREAS IN COMMUNICATIONS*, 24(2), 2006.

[19] Pandurang Kamat, Yanyong Zhang, Wade Trappe, and Celal Ozturk. Enhancing Source-Location Privacy in Sensor Network Routing. In *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, pages 599–608, 2005.

[20] Yun Li and Jian Ren. Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks. In *IEEE INFOCOM*, pages 2660–2668, 2010.

[21] K. Mehta, D. Liu, and M. Wright. Protecting Location Privacy in Sensor Networks Against a Global Eavesdropper. *Mobile Computing, IEEE Transactions on*, 2011.

[22] Kiran Mehta, Donggang Liu, and Matthew Wright. Location Privacy in Sensor Networks Against a Global Eavesdropper. In *Proceedings of IEEE International Conference on Network Protocols (ICNP)*, pages 314 –323, 2007.

[23] Yi Ouyang, Zhengyi Le, Guanling Chen, James Ford, and Fillia Makedon. Entrapping Adversaries for Source Protection in Sensor Networks. In *Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 23–34, 2006.

[24] Celal Ozturk, Yanyong Zhang, and Wade Trappe. Source-location Privacy in Energyconstrained Sensor Network Routing. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN)*, pages 88–93, 2004.

[25] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler. SPINS: Security Protocols for Sensor Networks. *Wireless Networks*, 8:521–534, 2002.

[26] Sejun Song, Hyungbae Park, and Baek-Young Choi. STEP: Source Traceability Eliminatoin for Privacy against Global Attackers in Sensor Networks. In *In Proceedings of IEEE ICCCN Workshop (MobiPST)*, 2011.

[27] S. Vasudevan, J. Kurose, and D. Towsley. On Neighbor Discovery in Wireless Networks with Directional Antennas. In *IEEE INFOCOM*, volume 4, pages 2502–2512, 2005.

[28] Poachers Target African Elephant for Ivory Tusks. http://www.npr.org/templates/story/story.php?storyId=6677444.

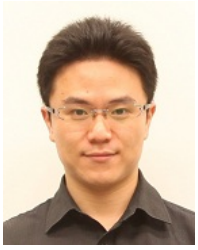
[29] Yi Yang, Sencun Zhu, Guohong Cao, and Thomas LaPorta. An Active Global Attack Model for Sensor Source Location Privacy: Analysis and Countermeasures. In *5th International ICST Conference on Security and Privacy in Communication Networks*, 2009.

[30] Wei Ye, J. Heidemann, and D. Estrin. An Energy-Efficient MAC Protocol for Wireless Sensor Networks. In *In Proceedings of IEEE INFOCOM*, volume 3, pages 1567–1576, 2002.

[31] Y. Zhang, W. Liu, Y. Fang, and D. Wu. Secure Localization and Authentication in Ultra-Wideband Sensor Networks. *Selected Areas in Communications, IEEE Journal on*, 24:829–835, 2006.

# Authors

Dr. Sejun Song received the B.S. degree in computer science from Pusan National University, Pusan, Korea, and the M.S. and Ph.D. degrees in computer science and engineering from the University of Minnesota, Twin Cities, in 1999 and 2001, respectively. He is an Assistant Professor in the Department of Engineering Technology and Industrial Distribution at Texas A&M University, College Station. Prior to joining academia, he had several years of industry experience from Cisco Systems, Honeywell Research Lab, and Positive Networks. His research interests lie in broad areas of networked systems including measurement, security, high availability, data storage, real-time, and embedded systems.



Hyungbae Park received the B.E. degree in Computer Engineering from Kwangwoon University, Seoul, Korea in 2005 and the M.S. degree in Computer Science from South Dakota State University, Brookings, South Dakota, USA in 2007. He is a Ph.D. student in Computer Science at University of Missouri - Kansas City since 2008. His research interests include security in sensor networks, network traffic/performance analysis and modeling, smartphone-based localization, and fault tolerance computing systems.

Dr. Baek-Young Choi is an Associate Professor in the Department of Computer Science and Electrical Engineering at the University of Missouri - Kansas City. She received her Ph.D. in Computer Science from the University of Minnesota, Twin Cities in 2003. She held positions at Sprint Advanced Technology Labs and the University of Minnesota, Duluth as a post-doctoral researcher and 3M McKnight distinguished visiting assistant professor, respectively. Her research interests include network measurement and resource management of diverse network types.