A new 'Direction' for Source Location Privacy in Wireless Sensor Networks'

Shehla S Rana
Department of Electrical and
Computer Engineering
University of Illinois at Urbana-Champaign
Email: ssrana2@illinois.edu

Nitin H. Vaidya
Department of Electrical and
Computer Engineering
University of Illinois at Urbana-Champaign
Email: nhv@illinois.edu

***Abstract*—Preserving source location privacy in wireless sensor networks can be critical for several practical applications. Existing solutions proposed specifically for sensor networks rely on a combination of dynamic routing and dummy traffic to hide real event messages. While some privacy protection guarantees can be given, these solutions also tend to be expensive due to fake transmissions and non-shortest path routing overheads.**

In this paper, we propose a novel idea, of using a combination of directional antennas, transmit power control and information compression to provide lightweight and energy-efficient source location privacy. We discuss the adversary model extensively and then carefully layout characteristics of a realistic adversary. We show how use of directional antennas makes eavesdropping more costly for a realistic adversary and establish relationships between probability of compromise of location privacy, characteristics of directional antennas and size of the adversary's eavesdropping network. Finally, we show how a simple information compression measure can greatly reduce message latency and prolong battery life by conserving energy. Results of extensive simulations in NS2, with our realistic directional antenna add-on, show that compared to existing solutions, we can achieve comparable privacy protection, better message latency, delivery ratio and many orders of magnitude improvement in energy consumption.

I. Introduction and Related Work

Wireless sensor networks (WSNs) have found applications in a large variety of scenarios. Examples include, but are not limited to, target tracking, vehicular networks, military surveillance and habitat monitoring. Applications carrying sensitive data through WSN's are highly concerned about privacy. While there is a huge body of work on protecting *content privacy* through sophisticated cryptographic mechanisms, preservation of *contextual privacy* has not been addressed as thoroughly. By eavesdropping on network communications, even though an adversary may not be able to "understand" a message, it can still gather information. For example, in a military environment, an adversary that can overhear messages on the wireless channel can infer that there is military presence in the neighborhood. Contextual privacy entails protection of such information and is clearly critical to overall security.

Preserving source location privacy becomes important in several scenarios. However, one most common example used for reference in literature, is the "Panda-Hunter" problem [1]-[2], where a monitoring network composed of wireless sensors is in place to track presence of pandas and report this information to a sink. The adversary's objective is to indirectly track the panda's location by locating source of messages received by the sink. This problem has been looked at from several perspectives and with varying assumptions on capabilities of the network and the adversary. On a broader level, however, all existing approaches fall into one of two categories: Those that consider the adversary to have local monitoring capabilities and those that assume the adversary has global eavesdropping capabilities.

Phantom routing [1] was one of the earliest works belonging to the first category. It presented two approaches: Using fake sources designated by the sink to generate cover traffic and a two-stage routing technique where a packet first did a directed walk in a random direction and then a *phantom source* routed it directly to sink. The adversary is mobile and starts at the sink. When the first packet is received, adversary moves to immediate source of the packet and keeps on repeating this, moving hop-by-hop towards the actual message source. The paper, however, considers a static panda that appears at a random point and stays there until it is captured or simulation ends. Therefore, no realistic analysis could be done about constraints on the adversary's speed of mobility and on the time period for which an event prevailed.

This model of local overhearing by an adversary was later adopted by several other approaches. A greedy random walk from both source and sink was proposed in [3] but it suffers from higher message delivery latency. A two-stage message forwarding idea was used in [4] where an event message first travels via MAC layer broadcasts and is later routed by some intermediate node directly to sink. The issue with all these schemes is that despite incurring significant overhead in terms of redundant traffic, their privacy protection degrades as the adversary's overhearing range or its level of eavesdropping increases.

A very strong adversary model has been assumed in [2], [5], [6]. Here, the adversary is considered capable of global eavesdropping and therefore the only way to protect source location is via cover traffic which these approaches study in various ways to understand tradeoffs between privacy and communication/energy cost.

In this paper, we provide a novel perspective to the source

location privacy problem. We argue that while the adversary may be resourceful, target network can still make it infeasible for the adversary to achieve global eavesdropping thus reducing or eliminating need for redundant cover traffic. The paper makes the following contributions:

- We provide a detailed critical analysis of an adversary's capabilities and then come up with a realistic adversary model with due consideration to limits on mobility, localization and overhearing. This is an improvement to existing adversary model that is either too weak (local) or too strong (global).
- We propose use of directional antennas for a two-fold reason. First, it reduces probability of a message being overheard by reducing the area in which signal energy is present. Second, it increases cost of achieving global overhearing by adversary since the adversary will need a denser network and this density grows as beamwidth of the directional antennas becomes narrower. To the best of our knowledge, this is the first time directional antennas have been used for protecting source location privacy.
- We identify redundancy in existing model for sending event messages to the sink and propose simple information prediction where only new information is reported to sink.
- With our own, realistic add-on for directional antennas in NS2, we provide results of extensive simulations to understand how their use can improve location privacy, message latencies, delivery ratios and decrease energy consumption.

A. *Adversary Model*

We start with formally specifying a realistic adversary model. As mentioned in Sec. I, two popular models exist in literature: the locally eavesdropping adversary and the globally eavesdropping adversary. Below, we identify how we improve on both these models. Throughout this paper, we term the sensor network monitoring the objects (e.g. pandas) as *target network* and the adversary as the *adversary network*. Now, let N_g and N_{adv} denote the set of nodes in target network and adversary's network respectively and let total monitored area be A.

1) **Overhearing Capabilities:** We assume that the adversary is not *perfectly* global. The most practical approach for an adversary to eavesdrop on target network seems to be that of deploying its own sensor network for monitoring target network's communications [2], [5]. However, if the adversary's network requires a very large number of monitoring nodes and other collection, synchronization and analysis infrastructure to achieve global eavesdropping, then it may just be more feasible and cost-efficient to invest in a small number of visual sensors and monitor the objects of interest directly. We therefore assume that the adversary deploys a sensor network of its own which is *no denser* than target network and that sensor nodes of both networks are comparable in terms of their computational power and overhearing range.
2) **Mobility Capabilities:** We also assume that while the adversary can move around, it can only do so with realistic constraints on its velocity. Suppose an event is detected by a sensor node $n \in N_g$ at a distance of h hops from the sink and this event lasts for t_e seconds. Suppose further that communication range of sensors in target network is r. Then, if the adversary starts at sink, and backtracks the messages in a hop by hop fashion, it will travel a distance of $\frac{r}{2}$ on average per hop. If there are at least h messages from the source, then the adversary must travel with a velocity $v_{adv} \geq \frac{hr}{2.t_e}$. Two observations are in order here: First, a source at h hops from the sink must send at least h messages for the single mobile adversary to be able to reach it. Second, if the event lasts for a small duration, the adversary must move very fast in order to reach the source. This is also one of the reasons why an adversary would choose to deploy a distributed network of its own so that it does not have to necessarily start at the sink.
3) **Localization Capabilities:** Existing approaches assume that when the adversary overhears a message, it can tell the sender's location. This assumption is also optimistic. Even if the adversary employs RF localization techniques, these techniques require making observations over at least some non-zero time interval before they can localize the sender. They also have requirements about time synchronization, interference, knowledge of sender's transmit power, number of signal receivers etc. For example, any received signal strength (RSS) based localization employed by the adversary requires knowledge of sender's transmit power, and simple transmit power variation by target sensors can be used to defeat this scheme.

In summary, we assume that while the adversary does deploy a network of its own to monitor the target network, it can only do so within certain constraints. For a realistic adversary, collisions and wireless channel fading must also be considered. Even if the adversary makes its own network very large despite the cost of sensors, exchange of observations between these sensors without exposing themselves poses another challenge. If nodes in target network can sense adversary's presence, they can adopt several ways of protecting their transmissions from being overheard. Therefore we assume that while an adversarial network may achieve a high level of overhearing, perfect global overhearing is still unlikely.

B. *Antenna Model*

The use of directional antennas in wireless sensor networks has historically been considered infeasible due to size and cost-related constraints. However, with advances in technology, switched beam antennas can be made small, inexpensive and feasible for use in sensors [7].

We assume that sensors in target network use antennas for directional transmission and omnidirectional reception

(DTOR) [8]. The motivation behind using directional antennas is manifold. First, they are known to provide several advantages including increase in throughput capacity and reduction in delays by reducing the number of hops required to traverse a network [9]. Second, for a constant transmission range, directional antennas require much less transmit power than omnidirectional ones to provide the same coverage. In source location privacy context, however, the biggest motivation is that for a given $|N_{adv}|$, directional antennas can substantially lower probability of a transmission in target network being overheard by some $n \in N_{adv}$.

An ideal directional antenna concentrates all its energy in a beam of width θ giving a gain of 1 in this direction and a gain of 0 in all other directions. While this model is simple, it is anything but realistic. Practical directional antennas do have some signal radiation in directions other than the mainlobe. We incorporate this in our implementation of directional antennas in NS2 by using the idea from [10]. Our directional antenna has a higher gain in the desired direction but also has smaller but non-zero gain in all other directions. The magnitude of this gain is controlled by a parameter we term as *main to sidelobe ratio*. The gain for a particular beamwidth θ is calculated as $g_{dir} = \frac{4}{\tan^2(\frac{\theta}{2})}$.

C. Network Model

Our network model comprises a wireless sensor network deployed to monitor a number of objects in the field. The objects have RF tags on them that emit a special signal. Whenever a sensor node detects this signal, it reports this event (the presence of object) to a single special node called the *sink*. We discuss several variations on how these events are reported to the sink in the next section.

II. Information Prediction and Directional Transmissions for Source Location Privacy

In this section, we identify ways to improve source location privacy. Our idea is to enhance protocol-based source location privacy schemes such that they can exploit advancement in device-level capabilities of wireless sensor nodes to provide stronger location privacy. For further discussions in this section, we assume a target network consisting of a set of sensor nodes $n \in N_g$ monitoring a set of objects $o \in Obj$.

A. Periodic Message Generation with Omni-directional Antennas (P-OA)

The first scheme we evaluate is when a sensor node $n \in N_g$, that can sense an object $o \in Obj$, sends out periodic messages to the sink using an omnidirectional antenna for as long as it can sense the object. This is the model most commonly adopted in existing literature [1]-[2].

*1) **Periodic Message Generation with Omni-Directional Antenna and Adversary with Probabilistic Overhearing (Prob-OA)** :* We also consider a special case of overhearing which encompasses effects of all shortcomings in adversary's ability to eavesdrop (Sec. I-A). We model those with an adversary that can overhear *every* message in the network (making it a global eavesdropper), but only with a probability $p_{overhear}$. As we show in our results, this model provides some interesting insights into the relationship between location privacy and adversary's overhearing capability.

B. Periodic Message Generation with Directional Antennas (P-DA)

This scenario is same as P-OA, except that sensors use directional antennas with steerable beams to send event messages to the sink. The transmit power P_t is reduced to maintain the same communication range as that for P-OA. The directional gain is calculated with respect to beamwidth according to Sec I-B.

C. Information Compression with Directional Antennas (IC-DA)

We devise a new scheme which incorporates information compression so that source location privacy is improved while the sink still receives the same information. Our idea is that when an object is sensed by a node, if the sink only needs to know about presence of the object, this information need not be sent periodically. In all existing literature, these messages are assumed to be sent periodically for as long as the object remains in the sender's sensing range. If the object remains in range of some node n_i from time t_1 to t_2, and if n_i sends k messages m_1 to m_k in this duration, then after m_1, the entropy of all messages from $m_2 \ldots m_{k-1}$ is exactly 0. Therefore, we employ a simple information compression scheme that eliminates messages containing no new information. The meaning of remaining messages is changed however. In our scheme, m_1 is meant to indicate that the object has been located in sensing range of source node n_i and that unless a new message is received from n_i, the object may be implicitly assumed to be there. When n_i can no longer sense the object in its range, it sends another message m_k to sink, informing it that the object has now moved away from it. We use MAC layer ACKs and retransmissions to ensure that messages reach their corresponding destinations(sink and relaying sensors). We highlight main advantages of this scheme below:

1) By sending a smaller number of messages, we reduce the energy consumed by monitoring sensors prolonging their battery life.
2) With only two messages, we defeat an adversary that starts at sink and follows a message hop by hop towards the source, except when source is at 2-hops from sink. We overcome this latter problem simply by making all nodes at 2-hops or lesser from sink send out dummy messages with a small probability in every time slot. This way, the adversary will not be able to distinguish real event messages and dummy messages.
3) It is reasonable to assume that a monitored object will often be in sensing range of more than one sensor in a single neighborhood. In such a scenario, with lesser traffic in the network, we avoid formation of a "hot-spot" and reduce message delivery latency and channel contention resulting in better packet delivery ratio.

III. EVALUATION

We used NS2 simulations for studying location privacy with and without directional antennas. We simulated a $1000m \times 1000m$ area and experimented with several network sizes and densities ranging from 300 nodes (communication range 100m) to 1200 nodes (communication range 50m). NS2 does not support directional antennas so we added our own realistic implementation of directional antennas with steerable beams according to the model in Sec. I-B. We experimented with several main to side lobe gain ratios ($M/S = \{10, 100, 1000\}$) but show results only for $M/S = 100$ due to space constraints. All sensor nodes in target network are static and know their own location as well as that of their 1-hop neighbors. To simulate monitored objects (e.g. pandas), we simulate mobile nodes $o_i \in Obj$ that move around throughout simulation at realistic velocities ($\leq 1m/sec$). Any sensor node $n \in N_g$ that can sense $o_i \in Obj$ must send a message to sink at this point.

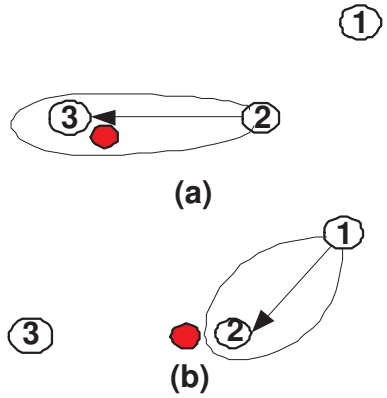

Fig. 1. A mobile adversary against directional antennas

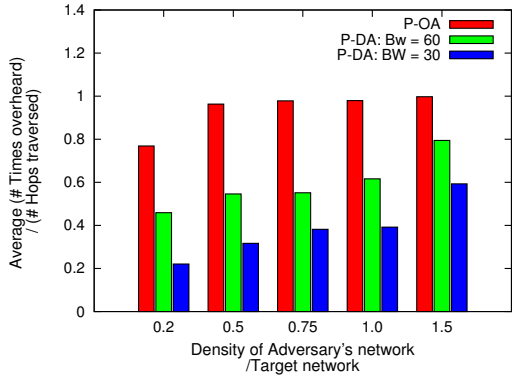

Fig. 2. Tradeoff between density of Adversary's network and overhearing capability

To start with, we evaluate feasibility of global eavesdropping when adversary deploys its own monitoring network. We consider this an important metric since we assume that location of a source node is compromised if one the following happens:

1) For $n_0 \in N_g$ sending an event message at time t_0:
   - Its messages are overheard by the adversary on each hop before they reach the sink.
   - n_0 had not received a message from another node from time $\tau = t_0 - t_{min}$ to t_0 where t_{min} can be some application dependent constraint on tolerable message delays.
2) With periodic message sending, the event lasts for so long that adversary can follow messages hop-by-hop to the sender. This is harder with directional antennas. To see why, consider Fig. 1. Red node depicts the adversary. There is a flow of messages between nodes $1, 2, 3$ in that order. The adversary overhears a message at node 3 and moves to the sender i.e. node 2. At this point, unless the adversary falls in the beam formed by node 1, it can still fail to overhear the next message. If it chooses to come too close to node 2, it can even get caught (for example trying to come too close to a military base). With omni-directional transmission, if the adversary could overhear a message at distance d from node 2, it could maintain that distance in any direction and still overhear it. However, with directional beamforming, adversary must not only be at distance d, but also in the direction of transmission.

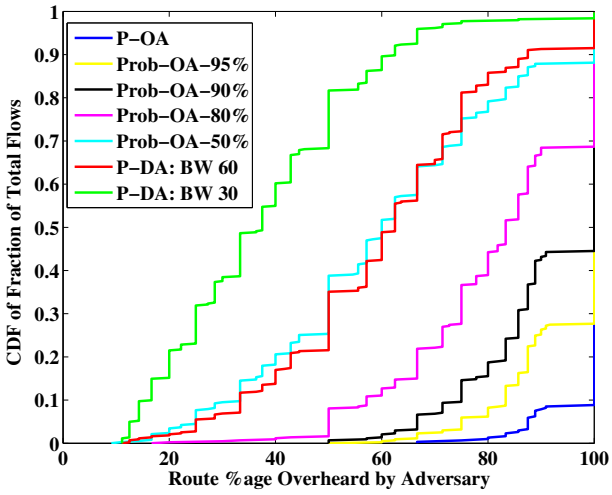

Fig. 3. CDF of percentage of route over which a flow's packets were overheard by adversary ($|N_{adv}| = |N_g|$ for P-OA and P-DA)

Fig. 2 relates adversary's overhearing capability with its density relative to target network. We vary density of the adversary's network from $|N_{adv}| = 0.2|N_g|$ to $|N_{adv}| = 1.5|N_g|$. Y-axis shows the ratio $\frac{N_{heard}}{N_{fwd}}$. Here, N_{heard} is the number of times a packet was overheard by some node $n \in N_{adv}$ and N_{fwd} is the number of times the packet was forwarded in the network. This was averaged over all packets sent during the simulation. A value of $Y = 0.5$ means that all packets were overheard over an average of 50% of the hops they traversed. As can be seen, with omni-directional antennas*(P-OA)*, adversary can achieve close to global overhearing even with very few nodes($|N_{adv}| \geq 0.5|N_g|$). This validates claims in [5] that global overhearing can be achieved with $|N_{adv}| << |N_g|$. The power of directional antennas against defeating global overhearing also manifests itself in

figure. Even with $|N_{adv}| = 1.5|N_g|$, the adversary can only monitor a packet over less than 60% and 80% of the route for beamwidths of 30^o and 60^o respectively. Due to space constraints we do not show how these results can improve further with narrower beamwidths and better sidelobe compression.

We also look at per-flow privacy for scenarios in Sec. II. Fig. 3 shows a CDF of the percentage of total flows which were observed over a certain fraction of their route. More than 90% of all flows sent omni-directionally were *completely* monitored by the adversary ($X = 100$ for $Y \geq 0.1$). This drops to 9% and 2% when event messages are sent using directional antennas with a beamwidth of 60^o and 30^o respectively. This number is a measure of location privacy because when the adversary can overhear a message over only a portion of its route from the source to the sink, there is a higher uncertainty about the message originator. The fact that only very small percentage of flows are completely overheard by the adversary when target network uses directional antennas shows their potential at thwarting an adversary's attempts to invade location privacy. Curves for probabilistic adversary *(Prob-OA)* in the figure give some interesting insights. Suppose sensors in target network use omni-directional antennas but take measures to degrade the adversary's overhearing capabilities. This may be done by creating deliberate interference and noise in areas where the adversary is suspected to be present. Fig. 3 shows that even if adversary's overhearing is degraded so much that it can only hear every message with probability $p = 0.5$, this can only provide as much privacy protection as that possible with directional transmissions with a 60^o wide main lobe.

So far, we have shown how directional transmissions can provide better message hiding capabilities for protecting location privacy, now we show how they can also improve other network characteristics including message delivery rate, end-to-end message latency and finally how they can prolong network lifetime by conserving battery usage.

Fig. 4 compares message delivery ratio w.r.t frequency of periodic messaging for schemes mentioned in Sec. II-A, II-B and II-C. We note here that the first scheme (*P-OA*) should be seen as an upperbound on the performance of all the existing schemes since it uses ideal parameters including no dummy messages and no non-shortest path routing. Theoretically speaking therefore, none of the existing schemes can do any better than the *P-OA* scheme presented in these results.

Fig. 4 shows, as expected, that message delivery ratio falls as sending rate increases. For message latency, Fig. 5 shows that when only new information is sent *(IC-DA)*, message latency remains low and remains constant which is not surprising. However, what's unexpected is that with periodic messaging, use of directional antennas *(P-DA)* does not improve message latency in comparison to omni-directional *(P-OA)* ones. We found that this was because we maintained same communication range in both cases by reducing transmit power for directional antennas and while directional antennas allow more simultaneous transmissions, the fact that our reception is omni-directional caused collisions at some receivers resulting in slightly longer delays.

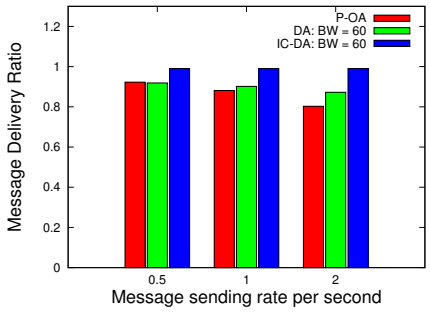

Fig. 4. Tradeoff between message delivery ratio and message sending rate

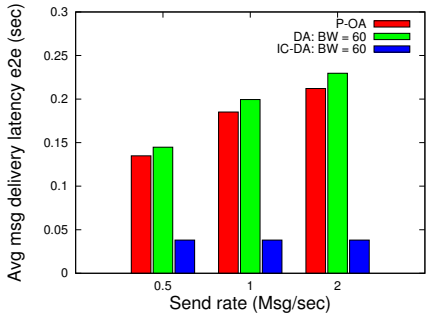

Fig. 5. Tradeoff between end to end message latency and message sending rate

Since energy consumption is a concern for sensor networks, we analyze it for different schemes with different antennas. We perform our energy calculation as follows: Let the event message size be *M* bits, total number of event messages sent in the network be N_T, number of times each message was forwarded before reaching the sink be F_T and the data rate be R *bits/sec*. The total energy consumed solely for packet transmissions can then be expressed as $E_{total} = P_t \frac{M \times N_T \times F_T}{R}$ *Joules*. Table. I shows the transmit energy consumption for *P-DA* ($BW = 30^o, 60^o$) and for *IC-DA* ($BW = 60^o$). The energy values are normalized by the corresponding consumption of *P-OA*. Once again, the huge potential for energy savings is evident from the numbers. The energy consumption for IC-DA is more than 10^5 times smaller than that for *P-OA*. These two values can be considered as opposite ends of the spectrum. With careful compression of information and highly directional antennas, a range of energy consumption possibilities can be exploited.

We remark here that in face of a distributed network of adversary nodes, all existing schemes with local overhearing adversary will at best provide same location privacy as our simple directional antenna based scheme but will experience longer message delays and also incur more overhead (flooding

TABLE I
TRANSMIT ENERGY CONSUMPTION NORMALIZED W.R.T P-OA

Message Sending Rate /sec	**P-DA**, $BW = 60^o$	**P-DA**, $BW = 30^o$	**IC-DA** $BW = 60^o$
0.5	0.07723	0.01598	0.00002527
1.0	0.08545	0.02352	0.000007739
2.0	0.08756	0.02546	0.000001798

in phantom routing [1], random walk, directed random walk). Our scheme's performance will also be better than those proposed for a global eavesdropping adversary since they all utilize some form of cover traffic (fake sources, dummy messages) that we do not heavily depend on. Both the idea of using directional antennas and of information compression can be employed on top of existing techniques also and it will improve both privacy and message transmission delays.

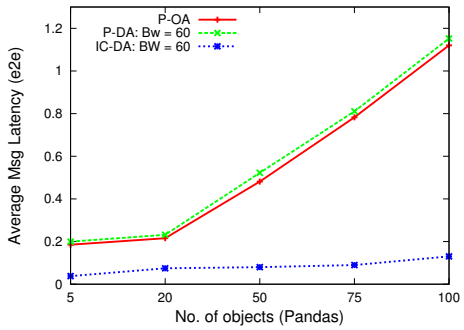

Fig. 6. End-to-end message latency with respect to number of objects

Next, in Fig. 6, we see how message latency varies as number of monitored objects increases in the network. Here again, the wide gap between *P-OA* and *IC-DA* shows potential for improvement possible with directional transmissions and intelligent information compression and/or prediction.

IV. Source Location Privacy: Observations and Conclusions

It is clear that if there is some node $n \in N_{adv}$ close to *every* sensor in the target network, it may be able to locate the sender in the schemes we discuss in this paper. But we note here that in the presence of such an adversary, leaving out the case where all nodes always send periodic messages whether or not they sense an event, all other existing techniques will also be unable to protect source location privacy. Consider for example, the scheme in [5]. If the adversary can overhear every message in the network, it can overhear the *first* message m_0 originated by the sender. It can also use timing correlation to conclude that this node has not received a message in a time interval τ before originating message m_0 and therefore must be originator of m_0. Moreover, privacy is also a function of how many fake sources are simulated *per* real object because if the adversary is so well-funded and determined as to achieve global eavesdropping, then it can also employ resources to check out all the suspected source locations simultaneously to find real objects. For example if adversary knows that there are close to N_r real objects in the monitored area and it can sense a total of $N_r + k$ sources in the network, then for reasonably small k compared to N_r, it can check out all suspected locations. We also point out that schemes which depend on using fake sources make an underlying assumption that fake sources are located where there are no real objects. Suppose a node has a token to act as fake source in the next round (or at boot-up). If this node observes an event at the start of the next round, it is no longer a fake source. This problem is hard to address without intelligent event prediction mechanisms.

Therefore, our understanding is that it will be more feasible to exploit practical constraints on adversary's capabilities rather than depend on expensive protocols that provide stronger protection against an idealistic adversary model. This is why we propose use of directional antennas since they degrade adversary's overhearing capability unless it spends more on its deployed network. However, a very dense network may make it infeasible for the adversary to gather information in a timely manner for processing and for making localization decisions. It may also expose adversary's own location which can further benefit the original network since the sensors can then avoid transmissions in directions where the adversary is suspected to be present. We understand that there may be additional practical issues with directional antennas and sending fewer messages. This is why we emphasize that our ideas outline newer options and practical tradeoffs need to be explored for more viable solutions. For example, if sending only one message (as in *IC-DA*) proves to be too optimistic, a small number $c > 1$ may be used. The resulting energy saving may then not be as high as that in Table. I, but it will certainly be a significant improvement.

As part of our future work, we plan to incorporate models for mobility of monitored objects and to see how prediction of motion can be utilized to the advantage of actual sources to achieve even stronger location privacy.

Acknowledgment

This research is supported in part by Army Research Office grant W-911-NF-0710287. Any opinions, findings, conclusions or recommendations expressed are those of authors and don't necessarily reflect views of funding agencies or U.S. govt.

References

[1] C. Ozturk and Y. Zhang, "Source-location privacy in energy-constrained sensor network routing," in *In ACM SASN*, 2004, pp. 88–93.
[2] Y. Yang, S. Zhu, G. Cao, and T. LaPorta, "An active global attack model for sensor source location privacy: Analysis and countermeasures." in *SecureComm*. Springer, 2009, pp. 373–393.
[3] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," ser. SECON'09, pp. 493–501.
[4] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, and T. L. Porta, "Cross-layer enhanced source location privacy in sensor networks," ser. SECON'09, pp. 324–332.
[5] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," *IEEE International Conference on Network Protocols*, vol. 0, pp. 314–323, 2007.
[6] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *In IEEE INFOCOM*, 2008.
[7] G. Giorgetti, A. Cidronali, S. Gupta, and G. Manes, "Exploiting low-cost directional antennas in 2.4 ghz ieee 802.15.4 wireless sensor networks," in *European Conference on Wireless Technologies*, 2007, pp. 217–220.
[8] P. Li, C. Zhang, and Y. Fang, "Asymptotic connectivity in wireless ad hoc networks using directional antennas," *IEEE/ACM Trans. Netw.*, vol. 17, pp. 1106–1117, 2009.
[9] H. N. Dai, "Throughput and delay in wireless sensor networks using directional antennas," in *International Conference on Intelligent Sensors Sensor Networks and Information Processing*, ser. ISSNIP, 2009.
[10] R. Ramanathan, "On the performance of ad hoc networks with beamforming antennas," ser. MobiHoc '01, 2001, pp. 95–105.