Multi-node Coordinated Jamming for Location Privacy Protection

Sangho Oh
Electrical and Computer Engineering
WINLAB, Rutgers University
Rt 1 Tech Center, North Brunswick, NJ 08902, USA
Email: sangho@winlab.rutgers.edu

Marco Gruteser
Electrical and Computer Engineering
WINLAB, Rutgers University
Rt 1 Tech Center, North Brunswick, NJ 08902, USA
Email: gruteser@winlab.rutgers.edu

***Abstract*—In wireless sensor networks, adversaries can easily threaten the location privacy of sensor nodes using ordinary localization techniques. By collecting basic physical layer information, such as signal strength and time of arrival, adversaries can precisely locate the target nodes. Although basic anti-localization techniques based on power control and directional antennas are believed to mitigate such localization attacks in the radio physical layer, there has been little research on location privacy protection techniques by obfuscating physical layer information. In this paper, we propose a novel jamming technique that prevents adversaries from locating target nodes by mixing the jamming signal from neighboring nodes. We introduce this beneficial use of jamming technique, which uses single- or multiple- jammers, to improve location privacy while providing similar link throughputs. In addition, we introduce the Multi Cooperator Power Control (MCPC) algorithm to control jamming noise power, which further increases location privacy by actively controlling the strength of jamming noise.**

I. Introduction

In some applications, the location of sensor nodes is critical information that needs to be protected in wireless sensor networks. However, owing to the extensive research efforts that have focused on indirect mechanisms for inferring location information, adversary localization systems are able to threaten the location privacy of sensor nodes using the physical (PHY) layer information of the nodes [1], [2]. Particularly popular approaches are multilateration and RF finger printing methods using TOA (Time Of Arrival) or RSS (Received Signal Strength) measurements from the target node's transmission signal [3], [4].

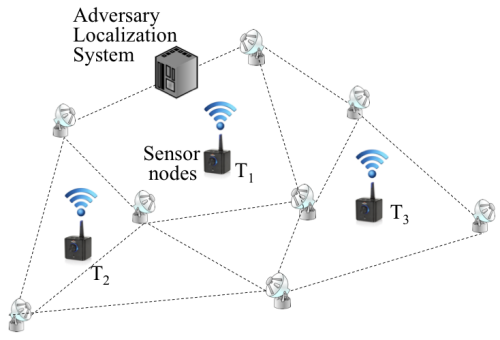


Fig. 1. Transmitter, receiver and adversary sensors.

We show an example scenario in Fig. 1, where an adversary localization system tries to find the location of the sensors nodes. Note that attacks from the adversary can be made in a completely passive manner using the information measured from the received signal. However, it is difficult to obfuscate PHY information without degrading the quality of wireless communications. Transmitting noise-like jamming signals from a third cooperative node can obviously help nodes obfuscate the PHY information, by inducing estimation errors to the adversary's localization systems. However, such a jamming technique has the problem of interfering with the communication between transmitters and receivers, thereby reducing the overall communication throughput of the network. Although applying beamforming antenna techniques or adding filterable pseudo-random noise can alleviate such interference problems, those techniques generally induce coordination problems or require encryption of the entire signal including pilots and preambles, which also degrade the radio performance.

In this paper, we design a simple but robust noise injection technique that is applicable to off-the-shelf commodity radio devices. The proposed privacy protection method utilizes friendly neighboring nodes as cooperative jammers that transmit jamming signals to obfuscate RSS or TOA information used by adversary sensors. While this jamming technique is quite intuitive, understanding the impact on radio link performance requires in-depth analysis. We first identify the trade-offs between throughputs and location privacy in wireless communication channels using the Cramer-Rao Lower Bound (CRLB), which determines the theoretical limits on the accuracy of localization attacks from adversaries. To the authors' knowledge, this is the first research paper that uses jamming to protect the location privacy of wireless nodes, and identifies the tradeoff between location-privacy and performance in wireless communications. Moreover, for efficient and reliable privacy gains against unknown adversary sensor locations, we introduce a novel Multi Cooperator Power Control (**MCPC**) technique exploiting distributed power-control mechanism, which considers the interference and throughput loss in the receiver node. Users can set a threshold for throughput loss, then cooperative jammers control their jamming signal strength within the threshold level while maximizing their

978-1-4673-0081-0/11/$26.00 ©2011 IEEE

aggregate jamming power. The algorithm is fully distributed and jammers do not transmit any coordination packet, which could disclose their locations.

The remainder of this article is organized as follows. In Section II we review existing location privacy protection techniques in the PHY layer. In Section III we propose multi-node cooperative jamming technique, and present simulation results. Then a conclusion is drawn in Section IV. The details on the simulation configuration and the analysis method based on CRLB are provided in the Appendix.

II. Related Work

Location privacy has been mostly discussed in the context of protection from an adversary system's inference attacks that are based on the knowledge acquired from location servers or proxies [5], [6]. In wireless communications, protecting location information in the PHY layer is a fundamental but difficult task compared to the approaches in application layers. As a result, relatively little research has been conducted on the protection of location privacy in the PHY layer.

Jiang et. al. [7] suggest a method that makes wireless nodes reduce transmission power to minimize the number of adversary sensors detecting their RSS values. On the other hand, El-badry et. al. have introduced a protocol where anchor nodes dynamically change their transmission powers to prevent unauthorized nodes localizing their locations [8]. They have also proposed a method where transmitters add noise to their transmitting signal to prevent the precise adversaries' RSS measurements while sacrificing their own link throughput. These approaches are simple but not effective when adversaries install a sufficient number of sensors for the detection and estimation of the signal transmitted from the target nodes.

Bauer et. al., conversely have used directional antennas made of tin-cans to prevent adversaries from collecting correct RSS information in [9], where they experimentally showed the performance of directional antenna on location privacy protection against RSS-based localization systems. However, it is not easy to apply directional antennas to wireless sensor nodes owing to their large size and difficulty in steering.

III. Collaborative Jamming for Location Privacy Protection

Self-jamming techniques, such as the transmitters randomly changing transmission power or lowering transmission power to minimum, can be easily detected or estimated by adversaries since all of their sensors are uniformly affected by the change of transmission power of a target transmitter node (TX). Hence, we propose a cooperative jamming method that exploits neighbor nodes of TX as cooperative jamming nodes (COP). Figure 2 shows an example scenario of cooperative jamming. In the figure, TX obfuscates its TOA and RSS information through the transmission of a jamming signal from one of its COPs. The jamming noise can be either white Gaussian noise like wide-band signal or low power dummy data packets, which decreases the received signal quality on adversary sensors $\mathbf{s} = \{s_1, s_2, \cdots, s_8\}$. Specifically for the adversaries using TOA information (TOA adversary), jamming noise from COPs lowers the estimation accuracy on the adversaries' TOA estimation since TOA estimations are largely dependent on the received signal quality. Also, the jamming noise induces estimation errors for RSS adversaries, who are localizing TX based on the measured RSS values from TX, by inducing errors to the adversaries' RSS measurements.

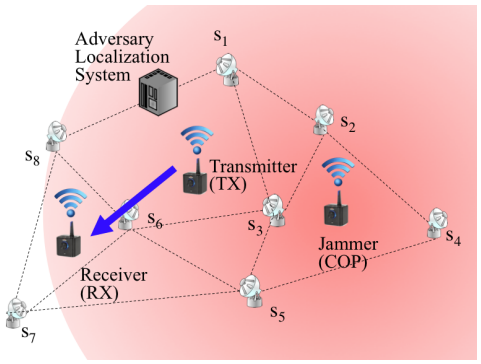


Fig. 2. Cooperative jamming for location privacy protection

We briefly explain how the jamming noise affects the location privacy of nodes, which is measured by the accuracy that the adversary can achieve on the location of target nodes. The accuracy of location estimations of adversary localization systems using TOA measurements depends on the Signal to Interference and Noise Ratio (SINR) of the received signal and Non-Line Of Sight (NLOS) signal components [10]. Hence, we use the CRLB, $||\sqrt{\sigma_{\hat{u}}}||[\mathrm{m}]$, on the target location, $u = \{x, y\}$, as a privacy measure at given topology and SINR conditions where $\sigma_{\hat{u}}$ is the CRLB on u. The *Fisher Information Matrix (FIM)*, J_u is used to find $\sigma_{\hat{u}}$, which can be induced from the probability density function, $f_u(r)$, on the observation, r, in (2) [11].

$$\sigma_{\hat{u}} \geq J_u^{-1}, \tag{1}$$

$$J_u = E_u \left\{ \frac{\partial}{\partial u} \log f_u(r) \cdot \left(\frac{\partial}{\partial u} \log f_u(r) \right)^T \right\}. \tag{2}$$

The FIM, J_u, depends on the precision of time estimation whose variance is bounded by the SINR, γ, of the received signal ($\sigma_{\tau^2} \geq \frac{1}{8\pi^2 f_b^2 \cdot \gamma}$)[10]. Jammers lower the SINR conditions at the adversary sensors, thereby inducing errors to their localization system.

The jamming noise from COPs also affects the RSS measurement of the adversary sensors. Typical radios find RSS by subtracting background noise power from the measured aggregate signal power, where the background noise power is measured in a calibrating process [12]. Therefore, the jamming noise increases RSS estimation values at adversary sensors since the energy of the received signal increases due to the added noise power. When adversary sensors measure wrong RSS information, their estimation on the location of TX will be incorrect. For RSS adversaries, FIM, J_u, depends on the variation of the RSS measurement which is heavily dependent on the channel variations due to fading. Typically

small scale fading can be averaged out, hence shadowing is a major factor that affects the accuracy of localization systems. The shadowing from terrain can be overcome by calibrating accurate RSS maps in the target area. However, the RSS variation induced from unknown COPs is hard to be filtered out. We define the level of location privacy using CRLB on the location estimation from the adversary. The details on the analysis method based on CRLB and the parameter values used in our simulations are presented in the Appendix.

A. Single- and Multi-node Jamming

Next, we explain the tradeoff relationship between throughput and location privacy, then show how single or multiple cooperative jamming technique improves the location privacy of wireless nodes. An example topology with 7 adversary sensors is shown in Fig. 3(a). Depending on the transmission signal power of TX and the jamming power of COPs, throughputs and location estimation errors from the adversary localization system change. The throughput of TX, $C = \log_2(1+\gamma)\,[bits/Hz/s]$, is determined from the SINR between TX and RX,$\gamma_0(\mathbf{p}) = \frac{p_{TX}h_{TX}}{\sum_i^M p_i h_i + N}$. We denote the transmission power of TX as p_{TX}, TX to RX channel gain as h_{TX}, the jamming powers from M COPs as $\mathbf{p} = \{p_1, p_2, \cdots, p_M\}$, i_{th} COP to RX channel gain as h_i, and noise floor as N.

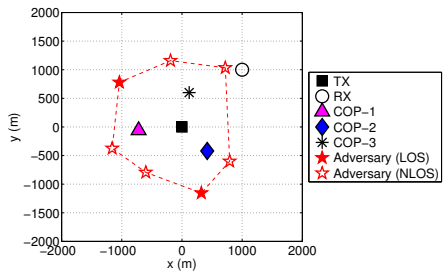
We first assume only one out of three COPs transmits jamming noise signal. In such a case, the location privacy of TX is dependent on the location of the COP transmitting a jamming signal.

In Fig. 3(b), we can find that using COP-1, which is close to adversary sensors and away from RX node, is the best strategy maximizing the privacy gain, which is measured by the location estimation error from the adversary. On the other hand, the performance of using all three COPs at the same time is not as good as using a single best COP. However, using multiple COPs can be more reliable since it can provide consistent location privacy gain, when the location of adversary sensors is unknown. Also, relying on a single COP may enable the adversary to trace back the location of the jamming signal source.

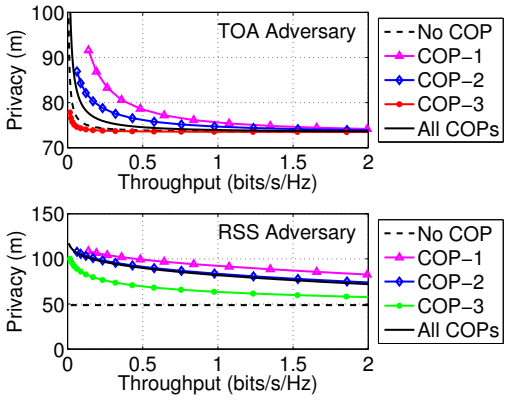
To minimize exposure to adversary sensors, all COPs have to know the precise transmission time and duration of message transmission of TX. We assume that the transmission time is pre-scheduled, and neighboring node lists are previously determined so that TXs and COPs synchronize their transmission time. Such information can be pre-configured before the nodes are deployed in the area, or it can be broadcast through a secured channel. During the time assigned, each node continuously transmits its message packets to its receiver node while its pre-assigned COPs transmit jamming signals.

B. Multi Cooperator Power Control (MCPC) Jamming for Location Privacy

The locations and jamming signal powers of COPs determine both the TX-RX link throughput, and the location privacy of TX. Although multiple low power jammers are



(a) Example topology.



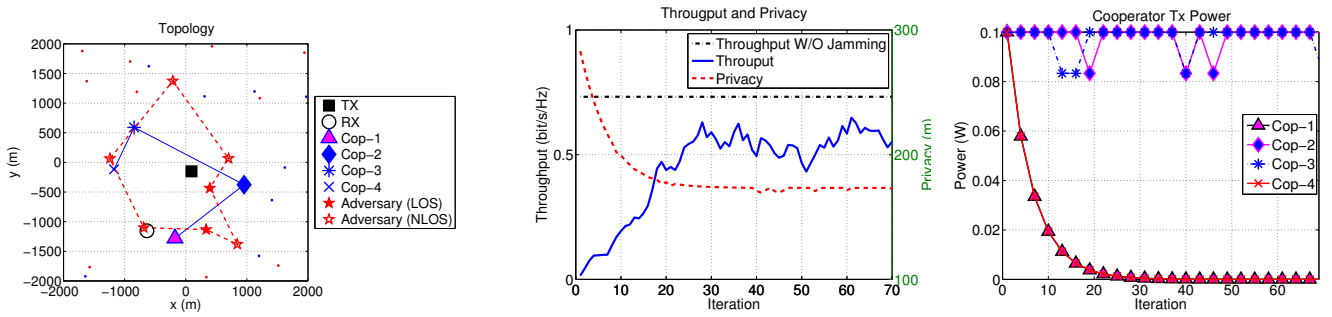
(b) Throughput and Privacy Tradeoff.

Fig. 3. Example of cooperator jamming scenario; path-loss exponent:$\eta = 3$, Receiver noise floor:$N = -101\text{dBm}$, Bandwidth:$f_b = 10\text{MHz}$.

used, some of them might be improperly located inducing too much interference noise to the RX node. However, it is not possible to determine the proper jamming signal strength without any message exchanging for the coordination among the nodes, which might expose the location of the message transmitter to the adversary.

We now propose the Multi Cooperator Power Control (*MCPC*) algorithm for an efficient jamming power control using a one-way single broadcast feedback channel from RX. Using the feedback information from RX, COPs adjust their jamming power to guarantee a certain level of link throughout for TX while maximizing their jamming efficiency to the adversary sensors. Although the feedback channel from RX can expose the location of RX, we can minimize the risks of revealing the location of RX through an asymmetrical feedback channel that is low rate and low power. One example scenario is that RX has a mobility, therefore less sensitive to the localization attacks from adversaries, e.g., RX is a ferry node collecting data from scattered stationary nodes.

For efficient location privacy protections, the jamming powers of COPs should be maximized while the link throughput C is guaranteed at certain level. To that end, a manually tunable parameter α, with ($\alpha < 1$), is introduced to allow COPs flexibly trade throughput for privacy. Specifically, α is a user-



(a) Example topology

(b) Throughput and privacy tradeoff

(c) Jamming power change at each COP

Fig. 4. NUM-based distributed jamming power control method; $p_{TX} = 20\text{dBm}$, $\alpha = 0.25$, Ricean fading.

defined threshold for acceptable throughput degradation due to jamming. We formulate this problem as a Linear Programing (LP) problem in (3), then apply the primal dual decomposition method to solve the problem in a distributed way [13].

$$\begin{aligned} \text{maximize} \quad & \sum_{i=1}^{M} p_i \\ \text{subject to} \quad & \gamma_0(p_{TX}, \mathbf{p}) \geq (1-\alpha) \cdot \gamma_0(p_{TX}, \mathbf{p}=0), \\ & 0 \leq \mathbf{p} \leq \bar{\mathbf{p}}. \end{aligned} \tag{3}$$

Using M cooperative jammers, the optimization variables are the jamming powers of COPs, $\mathbf{p}$, which are limited by maximum jamming signal transmission power $\bar{\mathbf{p}}$. We assume the transmission power of TX, p_{TX} is fixed, but the M COPs control their jamming power $\mathbf{p}$ to ensure that the SINR condition between TX-RX is larger than a certain throughput threshold set by α and SNR without a jamming signal ($\gamma_0(p_{TX}, \mathbf{p}=0)$). Then the constrain on SINR in (3) can be rewritten as $\sum_{i=1}^{M} p_i h_i \leq \alpha'$ for $\alpha' = N(\frac{\alpha}{1-\alpha})$.

We apply a Lagrangian multiplier λ and rewrite (3) as (4)

$$L(\mathbf{p}, \lambda) = \sum_{i=1}^{M} p_i - \lambda \left(\sum_{i=1}^{M} p_i h_i - \alpha' \right). \tag{4}$$

Then the dual problem can be solved by finding the minimum of $D(\lambda)$ in (3)

$$\begin{aligned} D(\lambda)_{(\lambda \geq 0)} &= \max_{\mathbf{p}} \left\{ \sum_{i=1}^{M} (1 - \lambda h_i) p_i \right\} + \alpha' \lambda \\ &= \sum_{i=1}^{M} \left\{ \max_{\mathbf{p_i}} (1 - \lambda h_i) p_i \right\} + \alpha' \lambda. \end{aligned} \tag{5}$$

Now the problem is decomposed into M sub-problems, and each COP can find the solution for (5) independently using the shadow price λ that is updated by RX using a feedback control channel. The shadow price λ is updated at each iteration by (6) using a gradient value $\frac{D(\lambda)}{\partial \lambda} = \sum_{i=1}^{M} h_i p_i - \alpha'$ where $[z]^+ = max\{0, z\}$ and δ is a small number adjusts the speed of convergence.

$$\lambda^{(n+1)} = [\lambda^{(n)} \left(1 + \delta (\sum_{i=1}^{M} h_i p_i - \alpha' \right)]^+. \tag{6}$$

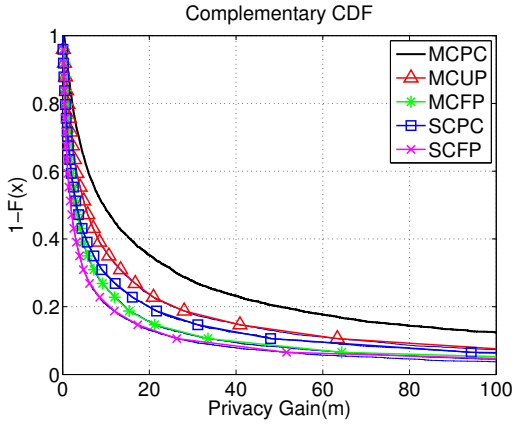
Using the updated price λ, each COP determines its jamming power p_i.

$$p_i^{(n+1)} = [arg \max_{p_i} (p_i - \lambda h_i p_i)]^+. \tag{7}$$

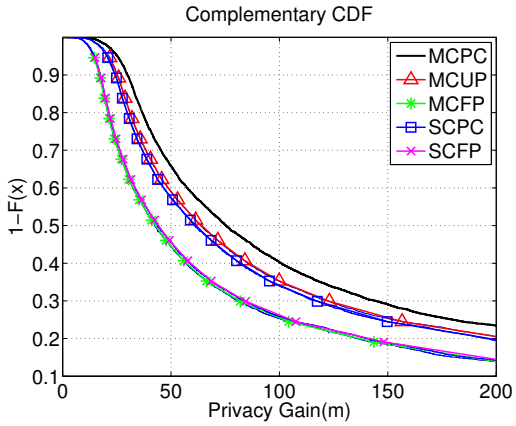
At each iteration, since each COP makes a greedy choice to maximize its own utility value $(p_i - \lambda h_i p_i)$, its transmission power abruptly changes between 0 and $\bar{p_i}$. Hence, we only allow a small power change of Δp in each iteration for slow but reliable convergence of power value considering unstable channel conditions due to fading.

Note that this distributed power control algorithm does not need any feedback from COPs. Since COPs passively estimate their channel gain to RX, h_i, from the feedback channel (from RX), their location privacy is preserved. In updating λ, RX only needs to know the sum of interference from COPs ($\sum_{i=1}^{M} h_i p_i$), which can be calculated from its SINR measurement, $\gamma_0(\mathbf{p}) = \frac{p_{TX} h_{TX}}{\sum_i^M p_i h_i + N}$. TX sends the values of p_{TX} and h_{TX} to RX, which can also be measured from the feedback channel from RX. Although RX has a mobility, the algorithm is fast (only 20 iteration is needed in the simulation) enough to catch up the variation of the channel.

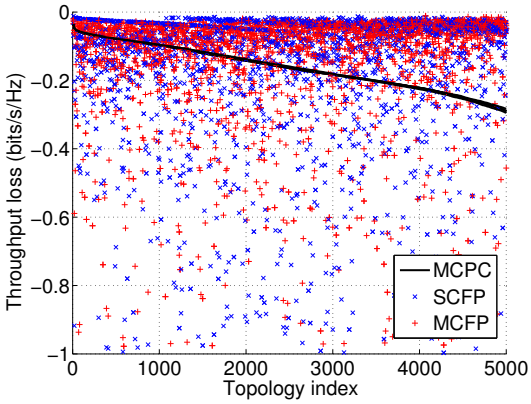
We show in Fig. 4 an example topology when $M = 4$ (4 COPs). COPs start with transmitting maximum jamming noise signal to protect the location privacy of TX in the initial stage of the algorithm, then gradually reduce their power at each iteration according to (7). Due to small scale channel fading, the channel conditions dynamically change over time, but as shown in Fig. 4(c), the jamming power in each COP gradually converges to a point that maximizes the sum of jamming powers while satisfying the constraints on the throughput loss. Note that the proposed distributed jamming power control algorithm automatically penalizes the jammers close to RX (COP-1 and COP-4) since their interference to RX is much stronger than other COPs (COP-2 and COP-3), which is better to achieve higher throughput. Therefore, in general cases where adversary locations are unknown, the proposed distributed power control algorithm performs better than other methods, such as randomly selecting a COP or uniformly changing jamming powers.



(a) Privacy performance for TOA adversary.



(b) Privacy performance for RSS adversary.



(c) Throughput comparison with fixed transmission power methods.

Fig. 5. Privacy performance measured by complementary cumulative distribution function; Jamming power for *SCFP* and *MCFP* are fixed as $9\mathrm{dBm}$ and $6\mathrm{dBm}$.

C. Performance of Multi-node Coordinated Jamming

Through simulations, we compare a number of jamming-based location privacy protection methods with the proposed *MCPC* jamming method. We run simulations for 5000 random topologies created with the sizes of $10\mathrm{km}$ by $10\mathrm{km}$ network. 100 nodes are uniformly located in every $1\mathrm{km}$ by $1\mathrm{km}$ grid with 2-dimensional random offset of $500\mathrm{m}$, and 100 adversary sensing nodes are also co-located in the same manner. TX is selected as the closest node to the center of the network, and its RX is randomly selected from the 5 closest nodes to TX, and the rest 4 nodes become COPs. Adversary sensors are the 7 closest nodes to TX among the 100 adversary sensors in the network, and 2 of them are assumed to have LOS link to TX. The throughput loss threshold set to be $\alpha = 0.25$.

The jamming-based location protection algorithms we simulated are summarized as follows;

- Multi Cooperator Power Control (*MCPC*): The jamming power of COPs are controlled by the proposed distributed multi-node power control algorithm satisfying the link throughput loss threshold α.
- Multi Cooperator Uniform Power (*MCUP*): The jamming power of COPs are uniformly adjusted according to the feedback from RX to guarantee the link throughput loss threshold α.
- Multi Cooperator Fixed Power (*MCFP*): The jamming power of COPs are fixed regardless of the link throughput.
- Single Cooperator Power Control (*SCPC*): Use a single COP. The closest node to TX is RX, and the next closest node is COP. The jamming power of COP is adjusted according to the feedback from RX to guarantee the link throughput loss threshold α.
- Single Cooperator Fixed Power (*SCFP*): RX and COP are same as *SCPC*. However, the jamming power of COP is fixed regardless of the link throughput condition.

For a fair comparison, the fixed transmission powers for *SCFP* and *MCFP* are selected as a value that provides the same average TX-RX link throughput with *MCPC* for overall topology conditions. We measure the privacy gain by calculating how much location privacy is improved compared with the cases without jammers. Figure 5 shows the simulation results. The performance is measured by a complementary cumulative distribution function $(1 - F(x))$, which indicates the probability that the privacy gain is above a particular privacy gain level. the proposed *MCPC* outperforms other baseline techniques. We can find that simple uniform power control methods marginally improve location privacy compared to fixed jamming power methods; even the fixed power values are reasonable well chosen to provide similar throughputs with *MCPC*. We can also find that multi-node jamming methods does not perform significantly better than single-node jamming methods for overall network environments.

Figure 5(c) shows the throughputs in fixed power methods compared to *MCPC*. Since fixed jamming methods do not consider the link throughputs, their throughput loss and privacy gain is very unstable depending on topological conditions. Therefore, they should be carefully calibrated before nodes are deployed in the target area considering the channel conditions

and the distances between nodes.

IV. Conclusion

In this paper, using theoretical analysis and simulations, we showed that the location privacy of wireless nodes and its communication throughput are negotiable parameters that can be traded off against one another. Moreover, we showed that by simply adding jamming noise from a third cooperator jamming node, it is possible to achieve better location privacy without sacrificing too much communication throughput. We also proposed a distributed jamming power control algorithm to find optimal jammers' transmission power in given topological conditions. The proposed algorithm significantly improves the location privacy while guaranteeing the throughput be above a user-defined threshold. Furthermore, the proposed algorithm leaves the cooperative jammers location privacy intact.

References

[1] Y.-C. Hu and H. J. Wang, "Location privacy in wireless networks," in *Proc. of ACM SIGCOMM Asia Workshop*, Apr. 2005.

[2] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, pp. 46 – 55, Jan. 2003.

[3] L. Doherty, K. Pister, and L. El Ghaoui, "Convex position estimation in wireless sensor networks," in *IEEE International Conference on Computer Communications*, vol. 3, pp. 1655–1663, Citeseer, 2001.

[4] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proc. of IEEE International Conference on Computer Communications*, 2000.

[5] J. Hightower and G. Borriello, "Location systems for ubiquitous computing," *IEEE Computer*, pp. 57–66.

[6] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis," *Mobile Networks and Applications*, vol. 10, no. 3, pp. 315–325, 2005.

[7] T. Jiang, H. J. Wang, and Y. C. Hu, "Preserving location privacy in wireless lans," in *Proc. of Mobile systems, applications and services (MobiSys)*, (New York, NY, USA), 2007.

[8] A. S. R. Elbadry and M. Youssef, "Hyberloc: providing physical layer location privacy in hybrid sensor networks," in *Proc. of IEEE Ad-Hoc, Sensor and Mesh Networking Symposium*, 2010.

[9] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker, "The directional attack on wireless localization: how to spoof your location with a tin can," in *Proc. of IEEE conference on Global telecommunications*, pp. 4125–4130, IEEE Press, 2009.

[10] H. Urkowitz, *Signal Theory and Random Processes*. Artech House, 1983.

[11] Y. Qi, H. Kobayashi, and H. Suda, "Analysis of wireless geolocation in a non-line-of-sight environment," *IEEE Transactions on Wireless Communications*, vol. 5, no. 3, pp. 672–681, 2006.

[12] Y. Chen and A. Terzis, "On the mechanisms and effects of calibrating rssi measurements for 802.15.4 radios," in *Proc. of European Conference on Wireless Sensor Networks (EWSN)*, pp. 256–271, 2010.

[13] S. wook Han, H. Kim, and Y. Han, "Distributed utility-maximization using a resource pricing power control in uplink DS-CDMA," *IEEE Communications Letters*, vol. 12, pp. 286 –288, Apr. 2008.

[14] J. Li, X. Sun, P. Huang, and J. Pang, "Performance analysis of active target localization using TDOA and FDOA measurements in WSN," in *Proc. of the Advanced Information Networking and Applications - Workshops*, pp. 585–589, 2008.

[15] I. J. Quader, B. Li, W. Peng, and A. G. Dempster, "Use of fingerprinting in Wi-Fi based outdoor positioning," in *Proc. of International Global Navigation Satellite Systems Society IGNSS Symposium*, 2007.

Appendix

We use the CRLB to estimate the limits in the precision of adversary localization systems trying to find the location of wireless mobiles sensors. CRLB for TOA and RSS based localization systems in mixed LOS and NLOS conditions is discussed in [11].

A. CRLB for TOA-based localization methods

The adversary localization system estimates the distance from target node TX by measuring TOA from the received signals, and then he applies triangulation techniques. Since the adversary does not know the exact timing of the transmitted signal, he has to use Time Different Of Arrival (TDOA) values instead. We considered that the accuracy of TDOA-based localization method is basically same as TOA-base system with doubled variances in time estimation [14].

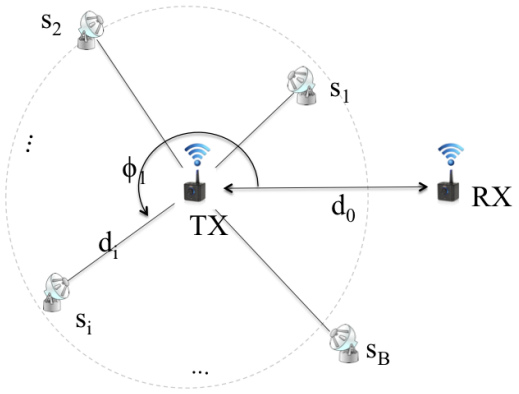


Fig. 6. Transmitter (TX), receiver (RX) and adversary sensors ($\mathbf{s}$).

Figure 6 depicts the adversary system localizing the target node TX using total number of B sensors, $\mathbf{s} = \{s_1, s_2, \cdots, s_B\}$. Let us assume M sensors are in NLOS conditions, and the rest $(B - M)$ sensors are in LOS conditions. Then, the values to be estimated are $\mathbf{v} = (u, l)$ for the location of T,$\mathbf{u} = \{x, y\}$, and NLOS path lengths, $\mathbf{l} = (l_1, l_2, \cdots, l_M)$. The CRLB for $\mathbf{v}$ is determined from *FIM* matrix $J_{\mathbf{v}}$ in (8),

$$Cov(\mathbf{v}) \geq J_{\mathbf{v}}^{-1}, \tag{8}$$

where $J_{\mathbf{v}}$ can be found from *FIM* for received signal delay τ in the following equation (9)

$$J_{\mathbf{v}} = H \cdot J_{\tau} \cdot H^T, \tag{9}$$

for H representing the geometric configuration of sensors in relation with the target transmitter location, where the angle to each sensor s_i is denoted as $\phi_{\mathbf{i}}$ referencing to the link to receiver RX.

$$H = \begin{pmatrix} \cos\phi_1, \cos\phi_2, \cdots, \cos\phi_M \\ \sin\phi_1, \sin\phi_2, \cdots, \sin\phi_M \end{pmatrix}. \tag{10}$$

Then, $J_{\mathbf{v}}$ can be rewritten as the following equation

$$J_{\mathbf{v}} = \frac{1}{c^2} \begin{pmatrix} H_{NL}\Lambda_{NL}H_{NL}^T + H_L\Lambda_L H_L^T & H_{NL}\Lambda_{NL} \\ \Lambda_{NL}H_{NL}^T & \Lambda_{NL} \end{pmatrix}, \tag{11}$$

where $c = 3 \times 10^8 \mathrm{m/s}$. H can be decomposed into NLOS

(denoted as "NL") and LOS (denoted as "L") components. Λ is a diagonal matrix of λ_i that represents the precision of time estimation for the TOA measurement at each sensor s_i. λ_i depends on the quality of the signal (SINR) and the delay spread of the channel, which can be expressed as (12).

$$\lambda = \frac{1}{\sigma_\tau^2 + \sigma_{\text{rms}}^2}, \tag{12}$$

where σ_{rms} is the delay spread of the channel, and $\sigma_{\tau^2} = \frac{1}{8\pi^2 f_b^2 \cdot \gamma}$ is the precision of time delay estimation, which depends on SINR of the received signal, γ, and the bandwidth of the signal, f_b. For the sensors in NLOS conditions, the delay spread in the received signal $\sigma_{\text{rms-NL}}$ is much larger than that of LOS sensors, $\sigma_{\text{rms-L}}$. Matrix λ can be decomposed into NLOS and LOS components in the same way as H. When jammers transmit jamming signals, the precision of location estimation of adversary localization system decrease as the SINR conditions in the received signals degrades.

CRLB for TOA adversary can be calculated from $J_{\mathbf{v}}$ in (11)

$$J_{TOA}^{-1} = [J_{\mathbf{v}}^{-1}]_{2\times 2}. \tag{13}$$

B. CRLB for RSS-based localization methods

Adversaries can also measure RSS from the target node TX to estimate the distance from the node. RSS at the receiver s_i depends on the path-loss between the TX and adversary sensors $\mathbf{s}$. A typical path-loss model is presented in (14), where the aggregate path-loss between TX and s_i, $\hat{z}_i$, consists of log-distance path-loss (z_i), log-normal shadowing (ω_i) , and small scale fading (ξ_i) components.

$$\hat{z}_i = z_i + \omega_i + \xi_i \quad [\text{dB}]. \tag{14}$$

The impact from small scale fading can be averaged out by collecting large number of samples since its variance can be significantly reduced by averaging the channel over time. CRLB for RSS-adversary is mostly bounded by the amount of the shadowing component ω_i since its variance is quite large. However, RF fingerprinting techniques [4] significantly reduce the effects from shadowing through an extensive calibrating process, which can also be applied to outdoor environments [15].

The path-loss z_i at distance d_i can be modeled by a log-distance path-loss model using a path-loss exponent η.

$$z_i = -10 \cdot \eta \cdot \log_{10} d_i \quad [\text{dB}]. \tag{15}$$

FIM for the location of TX can be found from

$$J_{\mathbf{v}} = \tilde{H} \cdot J_z \cdot \tilde{H}^T, \tag{16}$$

and

$$\tilde{H} = \frac{10\gamma}{\ln 10} \cdot \begin{pmatrix} \frac{\cos\phi_1}{d_1}, \frac{\cos\phi_2}{d_2}, \cdots, \frac{\cos\phi_B}{d_B} \\ \frac{\sin\phi_1}{d_1}, \frac{\sin\phi_2}{d_2}, \cdots, \frac{\sin\phi_B}{d_B} \end{pmatrix},$$

where $\tilde{H}$ is the geometric configuration for adversary sensors in RSS-base localization systems.

For large enough number of samples, $\bar{\xi}_i \approx 0$, then J_z is a diagonal matrix of the variance of shadowing components $\sigma_{\omega_i}^2$, which is often modeled by log-normal distribution of $N(\mu, \sigma_{\omega_i}^2)$. Sensors in NLOS conditions have larger $\sigma_{\omega_i}^2$ values that the sensors in LOS conditions.

$$J_z = \Lambda_B = [diag(\sigma_{\omega_1}^2, \sigma_{\omega_2}^2, \cdots, \sigma_{\omega_B}^2]^{-1}. \tag{17}$$

The RSS measurement value in adversary localization system interfered when jammers transmit jamming signals. We find σ_{c_i}, which is the variation of RSS induced by jamming signal at adversary sensor s_i, from simulations for 5000 different locations of COPs and adversary sensors. We put Λ'_B as the sum of the RSS variance due to shadowing and jamming noise, which can be decomposed into NLOS ($\sigma_{\omega-NL}^2$) and LOS ($\sigma_{\omega-L}^2$) components.

$$\Lambda'_B = [diag(\sigma_{\omega_1}^2 + \sigma_{c_1}^2, \sigma_{\omega_2}^2 + \sigma_{c_2}^2, \cdots, \sigma_{\omega_B}^2 + \sigma_{c_B}^2]^{-1}. \tag{18}$$

Then,

$$J_{\mathbf{v}} = \tilde{H} \cdot \Lambda'_B \cdot \tilde{H}^T. \tag{19}$$

CRLB in RSS adversary can be found from (20)

$$[J_{RSS}^{-1}] = [J_{\mathbf{v}}^{-1}]_{2\times 2}. \tag{20}$$

We summarize the parameter values used in the simulations in Table I.

TABLE I
SIMULATION PARAMETERS.

Parameter	Values
$\sigma_{\text{rms-L}}$	2×10^{-9} s
$\sigma_{\text{rms-NL}}$	2×10^{-8} s
$\sigma_{\omega-L}$	1 dB
$\sigma_{\omega-NL}$	3 dB