# Exploiting Jamming-Caused Neighbor Changes for Jammer Localization

Zhenhua Liu, Hongbo Liu, Wenyuan Xu, and Yingying Chen

**Abstract**—Jamming attacks are especially harmful when ensuring the dependability of wireless communication. Finding the position of a jammer will enable the network to actively exploit a wide range of defense strategies. In this paper, we focus on developing mechanisms to localize a jammer by exploiting neighbor changes. We first conduct jamming effect analysis to examine how the communication range alters with the jammer's location and transmission power using free-space model. Then, we show that a node's affected communication range can be estimated purely by examining its neighbor changes caused by jamming attacks and thus, we can perform the jammer location estimation by solving a least-squares (LSQ) problem that exploits the changes of communication range. Compared with our previous iterative-search-based virtual force algorithm, our LSQ-based algorithm exhibits lower computational cost (i.e., one step instead of iterative searches) and higher localization accuracy. Furthermore, we analyze the localization challenges in real systems by building the log-normal shadowing model empirically and devising an adaptive LSQ-based algorithm to address those challenges. The extensive evaluation shows that the adaptive LSQ-based algorithm can effectively estimate the location of the jammer even in a highly complex propagation environment.

**Index Terms**—Jamming, radio interference, least squares, localization.

## 1 INTRODUCTION

The rapid advancement of wireless technologies has enabled a broad class of new applications utilizing wireless networks, such as patient tracking and monitoring via sensors, traffic monitoring through vehicular ad hoc networks, and emergency rescue and recovery based on the availability of wireless signals. To ensure the successful deployment of these pervasive applications, the dependability of the underneath wireless communication becomes utmost important. Among various threats that can undermine the normal wireless communication, jamming attacks are especially harmful toward achieving reliable wireless communication. As the wireless communication medium is shared by nature, an adversary may just inject false messages or emit radio signals to block the wireless medium and prevent other wireless devices from even communicating. Furthermore, the increasingly flexible programming interface of commodity devices makes launching jamming attacks with little effort. For instance, an adversary can easily purchase a commodity device and reprogram it to introduce packet collisions that force repeated backoff of other legitimate users and thus, disrupt network communications.

To ensure the dependability of wireless communication, much work has been done to detect and defend against jamming attacks. The existing countermeasures for coping with jamming include two types: the proactive conventional physical-layer techniques that provide resilience to interference by employing advanced transceivers [1], e.g., frequency hopping, and the reactive non-physical-layer strategies that defend against jamming leveraging medium access control (MAC) or network layer mechanisms, e.g., adaptive error correcting codes [2], channel adaption [3], spatial relocation [4], or constructing wormholes [5]

Few studies have been done in identifying the physical location of a jammer. However, localizing a jammer is an important task, which not only allows the network to actively exploit a wide range of defense strategies but also provides important information for network operations in various layers. For instance, a routing protocol can choose a route that does not traverse the jammed region to avoid wasting resources caused by failed packet deliveries. Alternatively, once a jammer's location is identified, one can eliminate the jammer from the network by neutralizing it. In light of the benefits, in this paper, we address the problem of localizing a jammer.

Although there has been active research in the area of localizing wireless devices [6], [7], [8], most of those localization schemes are inapplicable to jamming scenarios. For instance, many localization schemes require the wireless device to be equipped with specialized hardware [6], [9], e.g., ultrasound or infrared, or utilize signals transmitted from wireless devices to perform localization. Unfortunately, the jammer will not cooperate and the jamming signal is usually embedded in the legal signal and thus, is hard to extract, making the signal-based and special-hardware-based approaches inapplicable.

Recent work [10], [11] on jamming localization algorithms relies on metrics other than signals. Without presenting performance evaluation, gradient descent search method based on packet delivery rate (PDR) [11] has been

- *Z. Liu and W. Xu are with the University of South Carolina, Swearingen Engineering Center, 301 Main Street, Columbia, SC 29208. E-mail: {liuz, wyxu}@cse.sc.edu.*
- *H. Liu and Y. Chen are with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, 210 Burchard Building, Castle Point on Hudson, Hoboken, NJ 07030. E-mail: {hliu3, yingying.chen}@stevens.edu.*

*Manuscript received 20 July 2010; revised 3 Jan. 2011; accepted 29 Mar. 2011; published online 25 May 2011.*
*Recommended for acceptance by D. Turgut.*
*For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2010-07-0435.*
*Digital Object Identifier no. 10.1109/TPDS.2011.154.*

1045-9219/12/$31.00 © 2012 IEEE Published by the IEEE Computer Society

proposed to localize the jammer. In our prior work, we introduce the concept of virtual forces, which are calculated by examining the node state. Guided by virtual forces, the algorithm pushes or pulls the estimated location of the jammer toward its true position iteratively [10].

In this paper, we propose a noniterative algorithm to localize a jammer, which exploits a node's neighbor list changes caused by jamming attacks. We have discovered that a jammer may reduce the size of a node's hearing range, an area from which a node can successfully receive and decode the packet, and the level of changes is determined by the relative location of the jammer and its jamming intensity. Therefore, instead of searching for the jammer's position iteratively, we can estimate the hearing range by identifying neighbor changes and localize the jammer in one round, which significantly reduces the computational cost yet achieves better localization performance than prior work [10].

We organize the remainder of the paper as follows: we specify our jamming attack model and provide an analysis on jamming effects in Section 2 as well as Section 2 of the supplementary file, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TPDS.2011.154. Then, in Section 3, we discuss our basic least-squares (LSQ)-based algorithm. In Section 4 and Section 3 of the supplementary file, which can be found on the Computer Society Digital Library, we present our effort in building a realistic propagation model through empirical study, and introduce the adaptive LSQ-based algorithm that can address radio irregularity. We conduct simulation evaluation and present the performance results in Section 5 as well as Section 4 of the supplementary file, which can be found on the Computer Society Digital Library. Finally, we conclude in Section 6. The related work is discussed in Section 1 of the supplementary file, which can be found on the Computer Society Digital Library.

## 2 Analysis of Jamming Effects

In this section, we start by outlining basic wireless networks and jammers that we use throughout this paper and briefly reviewing the theoretical underpinning for analyzing the jamming effects. Then, we study the impact of one jammer with an omnidirectional antenna on the wireless communication at two levels: the individual communication range level and the network topology level.

### 2.1 Network Model and Assumptions

We target to design our solutions for a category of wireless networks with the following characteristics:

**Multihop.** We consider a large-scale network, which is densely deployed. We assume that each node has one transmission rate and communicates in a multihop fashion. One example of such a network could be a sensor network.

**Stationary.** Once deployed, the location of each node remains unchanged. Mobility will be considered in our future works.

**Neighbor aware.** Each node in the network maintains a table that stores the information of its neighbors, such as their locations or activeness. Such a neighbor table is supported by most routing protocols and can be easily implemented by periodically broadcasting beacons. Moreover, each node is able to track the change on its neighbor table.

**Location aware.** Each node is aware of its own location and its neighbors' locations. This can be achieved relatively easy as many applications already require localization services [7].

**Homogeneous.** Each node is equipped with an omnidirectional antenna and transmits at the same transmission power level.

**Adaptive-CCA.** Clear channel assessment (CCA) is an essential component of Carrier Sense Multiple Access (CSMA), the de-facto medium access control protocols in many wireless networks. In particular, each network node is only allowed to transmit packets when the channel is idle by using CCA as channel detection.

Typically, CCA works as follows: before transmitting, a wireless device samples the ambient noise floor for a short period and it will transmit only if the sampled value is larger than a threshold $\Upsilon$. Studies [12] have shown that adaptive-CCA, which adjusts the threshold $\Upsilon$ based on the ambient noise floor, can achieve better throughput and reduced latency than using a predetermined threshold $\Upsilon$. Therefore, we assume that each node employs an adaptive-CCA mechanism in our study.

In this work, we focus on locating a jammer after it is detected. Thus, we assume the network is able to identify a jamming attack, leveraging the existing jamming detection approaches [13], [14].

### 2.2 Jamming Model

There are many different attack strategies that a jammer can perform in order to disrupt wireless communications. In this work, we focus on a representative jammer with the following characteristics:

**Constant jammer.** We use a constant jammer that continually emits a radio signal, regardless whether the channel is idle or not.

**Omnidirectional.** Each jammer is equipped with an omnidirectional antenna and transmits at the same power level. Thus, every jammer has the same jamming range in all directions.

**Nonoverlapping.** We assume there are one or more jammers in the network, but none of their jamming regions overlap.

### 2.3 Communication in Nonjamming Scenarios

Before analyzing the impact of jamming on the communication range, we briefly review the key factors that affect packet deliveries. Essentially, the MAC layer concept, packet delivery ratio (PDR), is determined by the physical metric, signal-to-noise ratio (SNR). At the bit level, the bit error rate (BER) depends on the probability that a receiver can detect and process the signal correctly. To process a signal and derive the associated bit information with high probability, the signal has to exceed the noise by certain amount. Given the same hardware design of wireless devices, the minimum required surplus of signals over ambient noise is roughly the same. We use $\gamma_o$ to denote the *minimum SNR*, the threshold required to decode a signal successfully. We consider that Node $A$ is unable to receive messages from Node $B$ when $(SNR)_{B \to A} < \gamma_o$, where

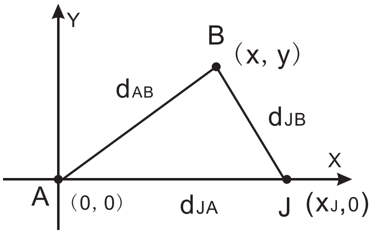


Fig. 1. The coordinate system for the hearing range and the sending range of Node $A$, wherein $A$ and $B$ are network nodes and $J$ is the jammer.

$(SNR)_{B\rightarrow A}$ denotes the SNR of messages sent by $B$ measured at $A$.

The communication range defines a node's ability to communicate with others, and it can be divided into two components: the *hearing range* and the *sending range*.

- ***The hearing range.*** Consider Node $A$ as a receiver, the hearing range of $A$ specifies the area within which the potential transmitters can deliver their message to $A$, e.g., for any Transmitter $S$ in $A$'s hearing range, $(SNR)_{S\rightarrow A} > \gamma_o$.

  潜在的发射器
- ***The sending range.*** Similarly, consider $A$ as a transmitter, the sending range of $A$ defines the region within which the potential receivers have to be located to assure receiving $A$'s messages, e.g., for any Receiver $R$ in $A$'s sending range, $(SNR)_{A\rightarrow R} > \gamma_o$.

Consider the standard free-space propagation model, the received power is

$$P_R = \frac{P_T G}{4\pi d^2}, \tag{1}$$

where $P_T$ is the transmission power, $G$ is the product of the sending and receiving antenna gain in the line of sight (LOS) between the receiver and the transmitter, and $d$ is the distance between them.

Given that in a nonjamming scenario, the average ambient noise floor $P_N$ is the same, both the hearing range and the sending range of Node $A$ will be the same, i.e., a circle centered at $A$ with a radius of $r_c = \sqrt{\frac{P_T G}{4\pi\gamma_o P_N}}$. This observation coincides with the common knowledge, that is, the communication between a pair of nodes is bidirectional when there are no interference sources.

We note that the hearing range and the sending range characterize a node's ability to receive and to deliver messages that are influenced by environmental factors (e.g., ambience noise or jammer signals) but not by in-network factors (e.g., interference from network nodes).

## 2.4 The Effect of Jamming on the Communication Range

Applying the free-space model to a jammer, the jamming signals also attenuate with distance, and they reduce to the normal ambient noise level at a circle centered at the jammer. We call this circle the *Noise Level Boundary (NLB)* of the jammer. Since jamming signals are nothing but interference signals that contribute to the noise, a node located within the NLB circle will have bigger ambient noise floor than the one prior to jamming.

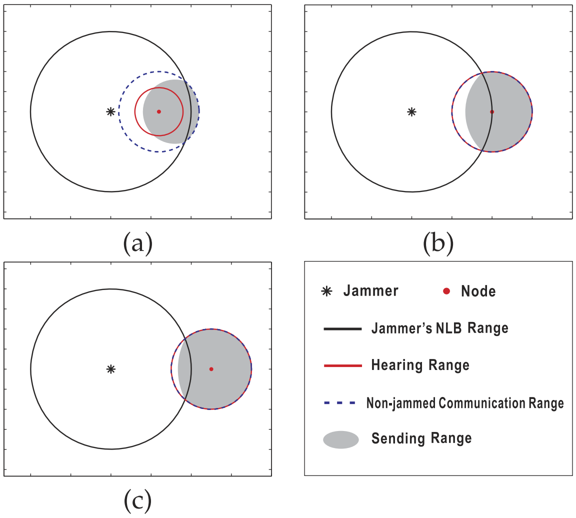


Fig. 2. The hearing range, the sending range, and the nonjammed communication range when the location of a jammer is fixed and a node is placed at different spots: (a) inside the jammer's NLB; (b) at the edge of the jammer's NLB; and (c) outside the jammer's NLB.

For simplicity, much work assumes that when a node is located inside the jammer's NLB circle, it loses its communication ability completely, e.g., both its sending range and hearing range become zero. Such assumptions may be valid for nodes that perform CCA by comparing the channel energy with a fixed threshold, since all nodes within the NLB will consider the channel busy throughout the duration that the jammer is active. However, in a network where adaptive-CCA is used, the nodes inside the jammer's NLB circle will still maintain partial communication ability yet weaker than the nodes outside the NLB circle.

To facilitate analyzing the hearing range and the sending range of Node $A$, we consider a simple network consisting of three players: Jammer $J$ interferes with the communication between Transmitter $B$ and Receiver $A$, as depicted in Fig. 1. The details on deriving both ranges are presented in the supplementary file, which can be found on the Computer Society Digital Library.

**The hearing range under jamming.** The hearing range of Node $A$ is a circle centered at $A$ with a radius of

$$r_h = \min\left(\frac{|x_J|}{\sqrt{\beta}}, \sqrt{\frac{P_T G}{4\pi\gamma_o P_N}}\right),$$

where $\beta = \frac{\gamma_o}{P_T/P_J}$.

**The sending range under jamming.** The sending range of Node $A$ is

$$\left(x - \frac{x_J}{1-\beta}\right)^2 + y^2 = \frac{\beta x_J^2}{(1-\beta)^2}, \tag{2}$$

a circle centered at $(\frac{x_J}{1-\beta}, 0)$ with a radius of $\frac{\sqrt{\beta}|x_J|}{|1-\beta|}$.

We depicted both the sending and hearing ranges in Fig. 2 when a node is located at various locations. From Fig. 2, we observed that for node A, because of jamming, the hearing range is no longer the same as the sending range, which can cause nonbidirectional links with its neighbors. In fact, interference can explain the commonly

非双向链接

observed nonbidirectional communications in wireless networks.

### 2.5 The Effect of Jamming on Network Topology

In this section, we extend our analysis of jamming impact from the individual node level to the network level, and classify the network nodes based on the level of disturbance caused by the jammer.

Essentially, the communication range changes caused by jamming are reflected by the changes of neighbors at the network topology level. We note that both the hearing range and the sending range shrink due to jamming. We choose to utilize the change of the hearing range and its effect on lost neighbors under jamming, since it can be easily estimated by examining receiving ability at each node.

We define that node $B$ is a neighbor of node $A$ if $A$ can *receive* messages from $B$, which is determined by the $(SNR)_{B\rightarrow A}$, i.e., the signal-to-noise ratio measured at node $B$ while node $A$ is transmitting. Let $Nbr\{n_i\}$ be the set of neighbors of node $n_i$ before any jammer becomes active. When jammers are present in the network, the network nodes can be classified into three categories according to the impact of jamming: *unaffected node* $N_U$, *jammed node* $N_J$, and *boundary node* $N_B$. Thus, we have

- **Unaffected node.**

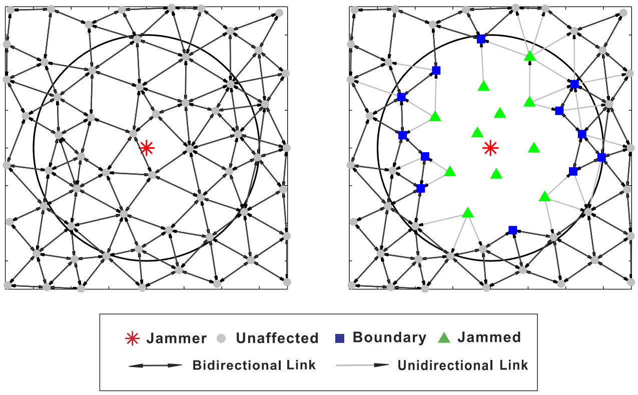
  $$N_U = \{n_u | \forall n_i \in Nbr\{n_u\}, (SNR)_{i\rightarrow u} > \gamma_0\}.$$

  A node is unaffected, if it can *receive* packets from all of its neighbors.
- **Jammed node.** $N_J = \{n_j | \forall n_i \in N_U, (SNR)_{i\rightarrow j} \leq \gamma_0\}$. Essentially, a node $n_j$ is jammed if it cannot *receive* messages from any of the unaffected nodes. We note that two jammed nodes may still be able to communicate with each other.
- **Boundary node.**

  $$N_B = \{n_b | (\exists n_i \in N_U, (SNR)_{i\rightarrow b} > \gamma_0) \text{ and } (\forall n_i \in Nbr\{n_b\} \cap N_J, SNR_{i\rightarrow b} \leq \gamma_0)\}.$$

  A boundary node can receive packets from part of its neighbors but not from all its neighbors.

Fig. 3 illustrates an example of network topology changes caused by a jammer. Prior to jamming, neighboring nodes were connected through bidirectional links. Once the jammer became active, nodes lost their bidirectional links either partially or completely. In the example depicted in Fig. 3, the nodes marked as triangles lost all their inbound links (receiving links) from their neighbors and became jammed nodes. Interestingly, some jammed nodes can still send messages to their neighbors, and they may participate in the jamming localization by delivering information to unaffected nodes as described in Section 3. The nodes depicted in rectangles are boundary nodes. They lost part of its neighbors but still maintained partial receiving links, e.g., at least connected to one of the unaffected nodes either directly or indirectly. Finally, the rest of nodes depicted in circles are unaffected nodes, and they can still receive from all their neighbors.



(a) Jammer is off (b) Jammer is on

Fig. 3. An example of the topology change of a wireless network due to jamming, where the black solid circle represents the jammer's NLB.

## 3 LSQ-Based Jammer Localization

### 3.1 Algorithm Description

In the previous sections, we have shown that the hearing range of a node may shrink and its neighbor list may change when a jammer becomes active. The levels of changes are determined by the distance to the jammer and the strength of the jamming signals. The basic idea of our LSQ-based algorithm is to localize the jammer according to the changes of a node's hearing range. To simplify the algorithm description, we start by assuming the node hearing range is known, and we delay the discussion of its estimation to Section 3.2.1.

Consider the example illustrated in Fig. 1, if $B$ happens to be located at the edge of $A$'s hearing range, then we have $(SNR)_{B\rightarrow A} \approx \gamma_o$, $d_{AB} = r_{h_A}$, and $(SNR)_{B\rightarrow A} \approx \frac{P_T/d^2_{AB}}{P_J/d^2_{JA}}$. Therefore, we can obtain the following formula:

$$(x_A - x_J)^2 + (y_A - y_J)^2 = \beta r^2_{h_A}, \tag{3}$$

where $r_{h_A}$ is the new hearing range of Node $A$, $\beta = \frac{\gamma_o}{P_T/P_J}$, and ($x_A$,$y_A$) and ($x_J$,$y_J$) are the coordinates of $A$ and Jammer $J$, respectively. In the above equation, the unknown variables include $x_J$, $y_J$, and $\beta$. To obtain those three variables, one equation is not enough. 求3个未知量，一个等式不够

Suppose that the hearing ranges of $m$ nodes have shrunk to $r_{h_i}$, $i = \{1, \ldots, m\}$ due to jamming. Then, we have $m$ equations:

除了A还有m个节点

$$\begin{aligned}
(x_1 - x_J)^2 + (y_1 - y_J)^2 &= \beta r^2_{h_1} \\
(x_2 - x_J)^2 + (y_2 - y_J)^2 &= \beta r^2_{h_2} \\
&\vdots \\
(x_m - x_J)^2 + (y_m - y_J)^2 &= \beta r^2_{h_m}.
\end{aligned} \tag{4}$$

Assume that we can obtain $r_{h_i}$ for each of $m$ nodes, then we can localize the jammer by solving the above equations. To avoid solving complicated nonlinear equations, we first linearize the problem by subtracting the $m$th equation from both sides of the first $m-1$ equations and obtain linear equations:

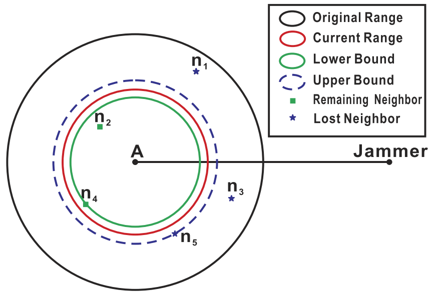


Fig. 4. An illustration of estimating the hearing range of Node $A$ leveraging the change of its neighbor list.

$$\begin{aligned}
&(x_1^2 - x_m^2) - 2(x_1 - x_m)x_J + (y_1^2 - y_m^2) - 2(y_1 - y_m)y_J \\
&\qquad = \beta(r_{h_1}^2 - r_{h_m}^2) \\
&(x_2^2 - x_m^2) - 2(x_2 - x_m)x_J + (y_2^2 - y_m^2) - 2(y_2 - y_m)y_J \\
&\qquad = \beta(r_{h_2}^2 - r_{h_m}^2) \\
&\qquad \vdots \\
&(x_{m-1}^2 - x_m^2) - 2(x_{m-1} - x_m)x_J + (y_{m-1}^2 - y_m^2) \\
&\qquad - 2(y_{m-1} - y_m)y_J = \beta(r_{h_{m-1}}^2 - r_{h_m}^2).
\end{aligned} \tag{5}$$

Then, it can be written in the form of $\mathbf{Az} = \mathbf{b}$ with

$$\mathbf{A} = \begin{pmatrix} x_1 - x_m & y_1 - y_m & \frac{1}{2}\left(r_{h_1}^2 - r_{h_m}^2\right) \\ \vdots & \vdots & \vdots \\ x_{m-1} - x_m & y_{m-1} - y_m & \frac{1}{2}\left(r_{h_{m-1}^2} - r_{h_m}^2\right) \end{pmatrix}$$

and

$$\mathbf{b} = \begin{pmatrix} (x_1^2 - x_m^2) + (y_1^2 - y_m^2) \\ \vdots \\ (x_{m-1}^2 - x_m^2) + (y_{m-1}^2 - y_m^2) \end{pmatrix}.$$

We can estimate the location of the jammer and $\beta$ by using the least-squares method,

$$\mathbf{z} = [x_J, y_J, \beta]^T = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}. \tag{6}$$

## 3.2 Algorithm Challenges

To localize a jammer using LSQ-based method, two questions have to be answered: 1) How to estimate the radius of a node's hearing range (aka the hearing radius)? and 2) what are the criteria of selecting nodes as candidates to form equation groups?

### *3.2.1 Estimating the Hearing Radius*

To estimate the hearing radius of Node $A$ after a jammer becomes active, Node A should examine its neighbor list and identify two specially located nodes: its furthest neighbor that Node $A$ *can* still hear from and its closest node that Node $A$ *cannot* hear from. Since the distances to those two special nodes provide the lower bound and the upper bound of $A$'s hearing radius, $A$'s hearing radius can be estimated as the mean value of those bounds.

Consider the example illustrated in Fig. 4, before the jammer started to disturb the network communication, Node $A$ had a neighbor list of $\{n_1, n_2, n_3, n_4, n_5\}$. Once the jammer became active, $A$'s neighbors reduced to $\{n_2, n_4\}$ and we call this set the *Remaining Neighbor Set*. At the same time, $A$ can no longer hear from $\{n_1, n_3, n_5\}$, the *Lost Neighbor Set*. The estimated upper bound of $A$'s hearing radius $r_u$ equals the distance to $n_5$, the nearest node in the lost neighbor set; the estimated lower bound $r_l$ equals the distance to $n_4$, the furthest node in the remaining neighbor set. As a result, the true hearing radius $r_{h_A}$ is sandwiched between $[r_l, r_u]$ and can be estimated as $\hat{r}_{h_A} = (r_u + r_l)/2$.

The estimation error of the hearing radius $e_h$ depends on $(r_u - r_l)$ and can be any value in $[0, (r_u - r_l)/2]$. When the distances between any two nodes are uniformly distributed, the estimation error $e_h$ follows uniform distribution with the expected value as $\frac{r_u - r_l}{4}$.

### *3.2.2 Selecting $m$ Nodes*

The nodes that can contribute to the jamming localization have to satisfy the following requirements: 1) they have a reduced hearing range and their neighbor list has changed; 2) the new hearing range under jamming attacks can be estimated; and 3) they are able to transmit their new hearing radius out of the jammed area.

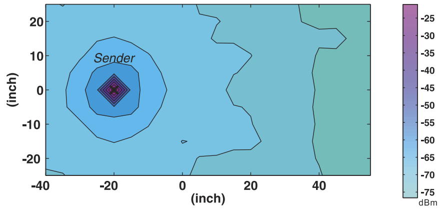
Although an unaffected node may have a slightly reduced hearing range, its neighbor list remains unchanged. Therefore, its hearing radius cannot be estimated and neither can it contribute an equation to localize the jammer. Likewise, although a jammed node's hearing range is decreased severely, its remaining neighbor set may be empty, preventing it from estimating the up-to-date hearing radius accurately. Even in the cases when they may estimate their hearing ranges with the help of "Jammed Cluster," they may not be able to transmit their estimations out of the jammed area due to communication isolation. In short, most of the jammed nodes are not suitable for jamming localization. Only those that can estimate their reduced hearing ranges and are able to send out messages to unaffected nodes can be used.

Finally, with regard to boundary nodes, the hearing range of a boundary node is reduced. Leveraging their reduced neighbor lists, their hearing radii can be estimated. More importantly, they can still communicate with unaffected nodes within finite steps. Therefore, all boundary nodes shall be used to participate the jamming localization.

In summary, we use the following nodes to form the equation group for jamming localization: all the boundary nodes and the jammed nodes that can estimate their reduced hearing ranges and are able to send out messages to unaffected nodes.

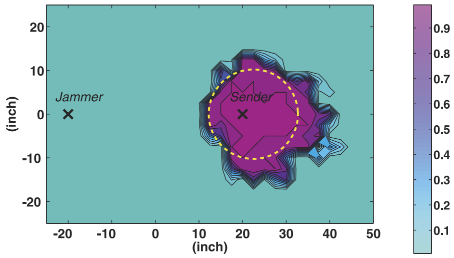
## 4 Localizing a Jammer in Reality

The previous analysis that exploits the free-space model provides insights in understanding the jamming effect and underlying theoretical basis for our localization algorithms. However, real wireless communication operates in complex propagation environments full of absorption, reflection, scattering, and diffraction, and it cannot be accurately modeled by the free-space model. Because of those characteristics associated with realistic radio propagation, several challenges arise when implementing our localization algorithm in practice. Thus, in this section, we first performed experimental measurements in a real environment to understand radio propagation in practice and then, selected a



Real measurements

Fig. 5. RSS contours with a transmitter located at $(-20, 0)$.



Real measurements

Fig. 6. PDR contours with a stationary sender at $(20, 0)$ and a jammer at $(-20, 0)$, where the dash circle is the sending contour derived using free-space model.

虚线圆

model that can represent realistic radio propagation. Finally, we modified the LSQ-based algorithm to address challenges induced by the complex radio propagation.

In practice, we envision that each node periodically samples the PDRs from all its neighbors and delivers them to a designed node that is unaffected. Once the jammer is detected, the designated node runs the LSQ-based algorithm. In other words, the data are acquired distributively but the localization is performed at one node.

## 4.1 Empirical Study

We conducted experiments in a 50 ft $\times$ 50 ft basement with 9-feet ceiling and several columns supporting the ceilings, using micaZ sensor nodes [15]. Due to space limitation, we tuned the transmission power to $-15$ dBm or $-25$ dBm to reduce the communication range of sensors. We have measured the Received Signal Strength (RSS) and Packet Delivery Ratio. Fig. 5 shows the resulted RSS contours, which appear to be approximate concentric circles yet with irregular edges. Fig. 6 depicts the measured PDR contours over the rectangular grid of $[-25, 50] \times [-25, 25]$ inches. The area where $PDR > 0$ actually maps to the sending range, and exhibits irregularity that coincides with common observations in wireless communication. The detailed experiment setup and discussions are presented in the supplementary document, which can be found on the Computer Society Digital Library.

同心圆
不规则的切边

## 4.2 Log-Normal Shadowing Model

To prepare for the extensive performance study, we targeted at discovering a realistic propagation model that can help to build our simulation tools. To balance the trade-off of modeling, we chose a simple model that captures the essential of signal propagation without using computer-aided modeling tools: log-normal shadowing model. The log-normal shadowing model captures both path loss versus distance along with the random attenuation due to blockage from objects in the signal path [16], and it has the following form:

$$PL(d) = PL(d_0) - 10 \cdot \eta \cdot \log\left(\frac{d}{d_0}\right) + X_\sigma, \tag{7}$$

where $PL(d)$ is the path loss at distance d, $PL(d_0)$ is the known path loss at a reference distance $d_0$, $\eta$ is the Path Loss Exponent (PLE), and $X_\sigma$ is a Gaussian zero-mean random variable with standard deviation $\sigma$. When $\eta = 2$ and $\sigma = 0$, Eq. (7) regresses to

高斯0均值分布的变量标准偏差

$$PL(d) = PL(d_0) - 20 \cdot \log\left(\frac{d}{d_0}\right), \tag{8}$$

which is the log-normal form of the standard free-space propagation model listed as Eq. (1).

There are two unknown parameters in the log-normal shadowing model: PLE $\eta$ and the standard deviation $\sigma$. We determined those parameters based on our experimental measurements: $\eta = 2.11$ and $\sigma = 1.0$. Details are presented in the supplementary file, which can be found on the Computer Society Digital Library.

## 4.3 Dealing with Signal Irregularity

The irregularity of the hearing range caused by random attenuation and multipath propagation in a complex radio environment can create much larger estimation errors of hearing radii than the one obtained assuming the free-space model. The larger estimation errors, in turn, can impair the localization accuracy, especially in the cases when not enough equations are available to "cancel out" those large estimation errors. Thus, the estimated location of the jammer could be very far away from its true location, even out of the jammed region.

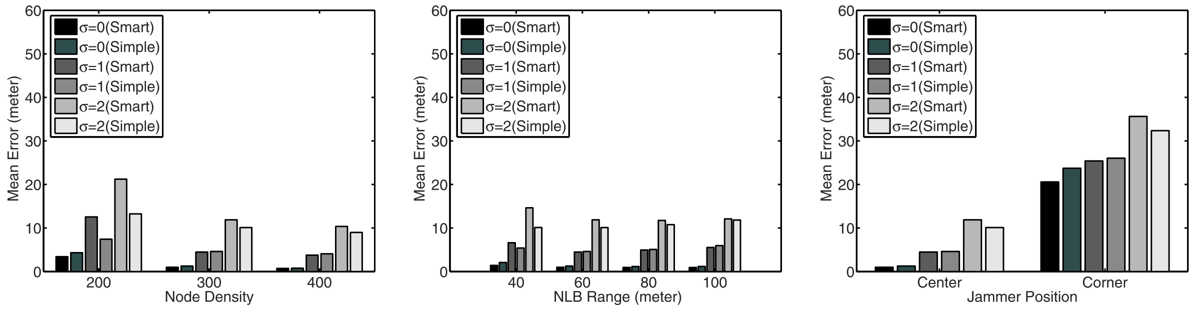
To assure that the estimated location of the jammer is inside the jammed region, we utilize centroid-based localization (CL) algorithm, which estimates the position of the jammer by averaging over coordinates of all boundary nodes. Formally, consider that there are $m$ boundary nodes $\{(x_i, y_i)\}_{i=1\ldots m}$, the position of the jammer can be estimated by

$$\hat{J} = (\hat{x}_J, \hat{y}_J) = \left(\frac{\sum_{k=1}^{m} x_k}{m}, \frac{\sum_{k=1}^{m} y_k}{m}\right). \tag{9}$$

Although CL is extremely sensitive to the distribution of boundary nodes and does not provide accurate estimation consistently [10], it always produces a position surrounded by all boundary nodes and can serve as correction when the LSQ-based algorithm fails to perform.

```
Algorithm: Adaptive_LSQ_localization
S: the set of boundary nodes
$\hat{J}_L = LSQ\_localization()$
$\hat{J}_C = Centroid\_localization()$
$d_m = \max_{Z_i, Z_j \in S} ||Z_i - Z_j||_2$
if $||\hat{J}_L - \hat{J}_C||_2 < a \times d_m$ then
    return $\hat{J}_L$
else
    return $\hat{J}_C$
end
```

**Algorithm 1.** The adaptive LSQ-based localization algorithm which incorporates the Centroid method with the original LSQ method. We empirically selected $a = 0.4$



(a) (b) (c)

Fig. 7. The impact of various factors on the performance of the Adaptive-LSQ algorithm under the shadowing model: (a) node density; (b) jammer's NLB range; and (c) jammer's position in the network.

Thus, we proposed an adaptive LSQ-based localization algorithm that combines the CL method with the LSQ algorithm, as shown in Algorithm 1. We note the name difference between the *adaptive* LSQ-based algorithm and the *pure* LSQ-based algorithm, as the latter does not integrate the CL method. In the `Adaptive_LSQ_localization` algorithm, the jammer's position is first estimated using both CL (`Centroid_localization`) and LSQ (`LSQ_localization`) independently. We note that `LSQ_localization` returns *infinity*, when the number of equations is less than the unknown variables. We estimated the span of the jammed region as the maximum distance between all boundary nodes. When the difference of both estimations is larger than $a$ times the span of the jammed region, indicating abnormally large estimation errors, the estimation using CL is returned. Otherwise, the estimation using LSQ algorithm is preferred. We selected $a$ to be 0.4, as it produces the best performance empirically.

We note that `Adaptive_LSQ_localization` algorithm does not work well when the jammer is indeed located outside the network and all affected nodes. However, such cases do not impose much concern in practice, as a jammer is less likely to place itself outside of the network, afraid of not fulfilling its objective to disrupt the communication ability of as many nodes as possible. Even if such cases do happen, such situations can be detected by examining the positions of affected nodes with regard to the network edges and then, one can choose to localize the jammer using LSQ-based algorithm instead of CL method.

## 5 Experiment Validation

In this section, we highlighted our evaluation results on the performance of the LSQ-based localization algorithm using the log-normal shadowing model. Detailed evaluations are presented in the supplementary file, which can be found on the Computer Society Digital Library.

### 5.1 Performance under the Shadowing Model

We evaluated the performance of the adaptive LSQ-based localization algorithms by emulating a real environment. Particularly, we adopted the log-normal model and tuned the parameters obtained from our empirical study, e.g., $\eta = 2.11$ and $\sigma = 1.0$. As such, we utilized the advantages of simulation methodology, e.g., flexibility, low cost, and no physical space limitation yet captured major characteristics of real-world implementation. Furthermore, we can tune the parameters of log-normal model slightly to mimic various radio environments.

We studied the localization accuracy of the adaptive LSQ-based algorithm under shadowing model in various network configurations, including node densities, jammer's NLB ranges, and jammer's positions in the network, as well as the standard deviation $\sigma$. We note that when $\sigma = 0$, the shadowing model with $\sigma = 0$ regresses to the free-space model.

**Impact of the node density.** We investigated the impact of the node density on the adaptive LSQ-based localization algorithm by setting the $N$ to $\{200, 300, 400\}$ while fixing the jammer's NLB range to 60 m. We plotted the mean estimation errors with $\sigma = \{0, 1.0, 2, 0\}$ in Fig. 7a. As $N$ increases, the performance of the adaptive LSQ-based algorithm improves for all $\sigma$.

Additionally, for the same $N$ and jammer's NLB range, we observed that as $\sigma$ increases, the performance of adaptive LSQ-based algorithm decreases. This is caused by the increasing degrees of the hearing range's irregularity.

**Impact of the jammer's NLB range.** We measured the mean localization errors of 300-node networks when changing the jammer's NLB radius to 40, 60, 80, and 100 m, respectively, and plotted the results in Fig. 7b. Again, we observed that as $\sigma$ increases, the performance of the adaptive LSQ-based algorithms decreases. However, as the jammer's NLB range increases, the accuracy of the estimated jammer's location does not change much.

**Impact of the jammer's position.** We placed jammer at the corner $(130, -130)$ and at the center $(0, 0)$, respectively, and depicted the mean errors of the adaptive LSQ-based algorithm when setting the jammer's NLB range to 60 m and $N$ to 300 in Fig. 7c. We observed that when the jammer is located at the center, the adaptive LSQ-based algorithm can localize the jammer with an accuracy better than 12 m on average. However, when the jammer is located at the corner, the mean estimation errors become around 30 m. The increase in estimation errors is because of the usage of CL. The performance of CL algorithm depends on the distribution of the affected nodes and a jammer located at the network corner produces a biased distribution of the affected nodes.

## 6 Conclusion

In this work, we addressed the problem of localizing a jammer in wireless networks and proposed an LSQ-based localization algorithm that estimates the jammer's location by utilizing the changes of neighbor nodes caused by jamming. We have analyzed the impact of a jammer on both a node's hearing range and sending range. And we have shown that the levels of a node's hearing range changes are determined quantitatively by the distance between the node to the jammer. The change of a node's hearing range can be estimated by exploiting the changes of its neighbors. Therefore, we can localize the jammer by examining the neighbor list changes of multiple nodes and constructing a least-squares problem. Our approach does not depend on measuring signal strength inside the jammed area, nor does it require to deliver information out of the jammed area. Thus, it works well in the jamming scenarios where network communication is disturbed.

We analyzed and evaluated our LSQ-based jammer localization algorithms in both the free-space and the shadowing model that represent the real radio environment. Under the free-space model, we compared our LSQ-based jammer localization algorithm with our prior work, i.e., the virtual force iterative localization (VFIL) algorithm that involves searching for the location of the jammer iteratively. Since the LSQ-based approach finishes the location estimation in one step, it significantly reduces the computation cost while achieving better performance. We have shown that our LSQ-based approach outperforms the VFIL regardless of node distributions, network node densities, jammer's transmission ranges, and jammer's positions by simulation.

To address the irregularity that exists in real systems, we studied our LSQ-based algorithm in the shadowing model. Particularly, we extended the pure LSQ-based localization scheme to an adaptive version by combining it with the centroid method. To evaluate the adaptive LSQ-based algorithm, we built our simulation environment based on the shadowing model and used the parameters obtained empirically from our experiments. Our extensive simulation results have confirmed that the adaptive LSQ-based algorithm is effective in localizing jammers in all experiment configurations, even in a highly complicated radio environment.

## REFERENCES

[1] J.G. Proakis, *Digital Communications,* fourth ed. McGraw-Hill, 2000.

[2] G. Noubir and G. Lin, "Low-Power DoS Attacks in Data Wireless Lans and Countermeasures," *ACM SIGMOBILE Mobile Computing and Comm. Rev.,* vol. 7, no. 3, pp. 29-30, 2003.

[3] W. Xu, W. Trappe, and Y. Zhang, "Channel Surfing: Defending Wireless Sensor Networks from Interference," *IPSN '07: Proc. Sixth Int'l Conf. Information Processing in Sensor Networks,* pp. 499-508, 2007.

[4] K. Ma, Y. Zhang, and W. Trappe, "Mobile Network Management and Robust Spatial Retreats via Network Dynamics," *Proc. First Int'l Workshop Resource Provisioning and Management in Sensor Networks (RPMSN '05),* 2005.

[5] M. Cagalj, S. Capkun, and J. Hubaux, "Wormhole-Based Anti-Jamming Techniques in Sensor Networks," *IEEE Trans. Mobile Computing,* vol. 6, no. 1, pp. 100-114, Jan. 2007.

[6] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The Active Badge Location System," *ACM Trans. Information Systems,* vol. 10, no. 1, pp. 91-102, Jan. 1992.

[7] P. Bahl and V.N. Padmanabhan, "RADAR: An In-Building RF-Based User Location and Tracking System," *Proc. IEEE INFOCOM,* pp. 775-784, Mar. 2000.

[8] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, "A Practical Approach to Landmark Deployment for Indoor Localization," *Proc. Third Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON),* Sept. 2006.

[9] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System," *Proc. ACM MobiCom,* pp. 32-43, Aug. 2000.

[10] H. Liu, W. Xu, Y. Chen, and Z. Liu, "Localizing Jammers in Wireless Networks," *Proc. IEEE PerCom Int'l Workshop Pervasive Wireless Networking (IEEE PWN),* 2009.

[11] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S.V. Krishnamurthy, "Lightweight Jammer Localization in Wireless Networks: System Design and Implementation," *Proc. IEEE Conf. Global Telecomm. (GLOBECOM),* Dec. 2009.

[12] J. Polastre, J. Hill, and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," *SenSys '04: Proc. Second Int'l Conf. Embedded Networked Sensor Systems,* pp. 95-107, 2004.

[13] A. Wood, J. Stankovic, and S. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks," *Proc. 24th IEEE Real-Time Systems Symp.,* pp. 286-297, 2003.

[14] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," *MobiHoc '05: Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing,* pp. 46-57, 2005.

[15] Crossbow Technology, http://www.xbow.com/, 2011.

[16] A. Goldsmith, *Wireless Communications.,* Cambridge Univ. Press, 2005.

**Zhenhua Liu** received the bachelor's degree in electronics and information engineering from the Department of Information Science and Technology in Central South University, Hunan, China, in 2006. He is working toward the PhD degree at the Computer Science and Engineering Department in the University of South Carolina. He is currently working in the Arena for Research on Emerging Networks and Applications (ARENA) Lab with Prof. Wenyuan Xu. His research interests include antijamming defense and location privacy in sensor networks.

**Hongbo Liu** received the bachelor's degree from the Department of Communication and Information Engineering of the University of Electronic Science and Technology of China, China, in 2005, and the master's degree in communication engineering from the same department in 2008. He is working toward the PhD degree at the Electrical and Computer Engineering Department in Stevens Institute of Technology. He is currently working in the Data Analysis and Information SecuritY (DAISY) Lab with Prof. Yingying Chen. His research interests include information security and privacy, wireless localization and location-based services (LBS), and wireless and sensor networks.

**Wenyuan Xu** received the PhD degree in electrical and computer engineering from Rutgers University in 2007. She is currently an assistant professor in the Department of Computer Science and Engineering, University of South Carolina. Her research interests include wireless networking, network security, and privacy. She is a coauthor of the book *Securing Emerging Wireless Systems: Lower-layer Approaches* (Springer, 2009). She received the US National Science Foundation (NSF) Career Award in 2009. She has served on the technical programs for several IEEE/ACM conferences on wireless networking and security.

**Yingying Chen** received the PhD degree in computer science from Rutgers University. She is currently an assistant professor in the Department of Electrical and Computer Engineering at Stevens Institute of Technology. Her research interests include wireless and system security and privacy, wireless networking, and distributed systems. She is the coauthor of the book *Securing Emerging Wireless Systems* (Springer, 2009). Prior to joining Stevens Institute of Technology, she was with Bell Laboratories and the Optical Networking Group, Lucent Technologies. She received the IEEE Outstanding Contribution Award from IEEE New Jersey Coast Section each year from 2000 to 2005. She is the recipient of the Best paper Award of the Sixth International Conference on Wireless On-demand Network Systems and Services (WONS) in 2009 and the Best Technological Innovation Award from the Third International TinyOS Technology Exchange in 2006.