An Algorithm for Jammer Localization in Wireless Sensor Networks

Tianzhen Cheng, Ping Li
Laboratory for Mechatronic Engineering and Control
BeiJing Institute of Technology
BeiJing, China 100081
{*czboss, liping85*}*@bit.edu.cn*

Sencun Zhu
Department of Computer Science and Engineering
and College of Information Sciences and Technology
The Pennsylvania State University, University Park, USA 16801
szhu@cse.psu.edu

***Abstract*—In wireless sensor networks (WSNs), jamming attacks have become a great concern recently. Finding the location of a jamming device is important so as to take security actions against the jammer and restore the network communication. In this paper, we take a comprehensive study on the jammer localization problem, and propose a simple while effective algorithm called *Double Circle Localization (DCL)*. DCL is based on minimum bounding circle (MBC) and maximum inscribed circle (MIC). We implement and evaluate DCL under different conditions, including different node densities, jammer's transmission powers and antenna orientations, and compare it with three existing jammer localization algorithms through both simulation and experiments. Our evaluation results have demonstrated that, compared with all other approaches, DCL achieves the best accuracy in jammer localization.**

***Keywords*-Jammer Localization; Jamming Attacks; Bounding Circle; Inscribed Circle; Wireless Sensor Networks;**

I. Introduction

In wireless sensor networks (WSNs), due to the shared nature and the open access to the wireless medium, an adversary can easily launch jamming attacks to paralyze the whole network [1]. Jamming attacks affects the network either by preventing the transmitters from sending messages due to the busy medium, or by dramatically decreasing the signal-noise ratio (SNR) at receivers to cause a large number of packet collisions. Although, some existing countermeasures against jamming attacks, such as channel surfing [2], frequency hopping[3], demonstrate a certain degree of resistance to jamming attacks, advanced devices and complex protocols are required. Furthermore, to keep working under the existence of the jammer, the power consumption of the whole WSN could be unacceptable.

We would take more active operations against the jammer, such as deactivating the jamming device, isolating the jammer, capturing, punishing or even destroying it. "Attack is the best form of defense", as the saying goes. To enable active strategies, jammer localization is important. In this work, we aim to solve the problem of how to localize jammers precisely. Determining the position of a jammer is more difficult than node localization in wireless sensor networks, due to the disrupted communication in portion of the network. Furthermore, a jammer does not comply with the jammer localization protocols, if not working against it. Especially, with all resource limitations of wireless sensor networks, many malicious device localization techniques [4], [5], [6] are not suitable in this scenario.

In this paper, we propose a jammer localization algorithm, called *Double Circle Localization (DCL)*. DCL is a new approach that uses two classic concepts in geometry, minimum bounding circle (MBC) and maximum inscribed circle (MIC), to solve the jammer localization problem. We then compare DCL with three existing algorithms, Centriod Localization (CL), Weighted Centriod Localization (WCL), Virtual Force Iterative Localization (VFIL) [7], and make a comprehensive comparison through simulation and experiments. Furthermore, in experiments, we not only perform experiments in isotropy jammer scenarios, but also change the direction of the jammer's antenna to imitate the anisotropy jammer scenario. To our best knowledge, we are the first one to do this comparison work through real experiments.

The rest of the paper is organized as follows. We begin this paper in Section II by discussing the related work. Section III describes our network models and adversary models that we will use in this paper. Then we describe the three existing algorithms and DCL in Section IV and V. After that, we present our simulation and experiments in Section VI and VII. Finally, Section VIII is our conclusion.

II. Related work

There are several algorithms proposed to cope with jamming attacks in wireless sensor networks. Noubir and Lin [8] combined error-correction codes and cryptographically strong interleavers to increase the likelihood of decoding corrupted packets. Xu et al. [2] presented two strategies, channel surfing and spatial retreats, to increase the resistance to jamming attacks by avoiding the interference as much as possible in the transmission frequency or physical location. Cagalj et al. [9] developed wormhole-based

The work of Sencun Zhu was supported in part by grants W911NF1120086-Z847707 from the Army Research Laboratory and NSF CAREER 0643906. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of ARL and NSF.

anti-jamming techniques to allow the delivery of important alarm messages. Additionally, conventional PHY-layer communication techniques, such as spreading techniques (e.g. frequency hopping), are commonly used to protect communication [10], which force the jammer to spend much more energy than the sender. However, such PHY-layer techniques require advanced transceivers, which may cost more power and bandwidth.

Few works have been done at jammer localization in WSNs. Pelechrinis et al. [11], based on packet delivery ratio (PDR) and gradient descent methods, designed and implemented a lightweight jammer localization algorithm. Their approach can find out the nearest node to the jammed area. Liu et al. [7] developed a jammer localization algorithm called Virtual Force Iterative Localization (VFIL). VFIL estimates the location of a jammer iteratively by virtual forces, which are derived from the node states and the network topology changes caused by jamming attacks. Liu et al. [12] proposed to localize jammers by exploiting nodes' hearing ranges. It works by estimating the change of hearing ranges before and after jamming attacks, and solving a least-squares problem. The assumption is the change of hearing ranges is only caused by jamming and the change is significant.

III. Jamming effects in wireless sensor networks

In this section, we analyze jamming effects on communications in wireless sensor networks, and outline our model formulations, network model and jammer model. Throughout our paper, all jammer localization algorithms will use these models.

A. *Wireless Sensor Network Model*

We assume all nodes in network are deployed randomly, and they do not change their locations. This is a common assumption used by existing works [7], [12]. No mobility will be considered in this work. Furthermore, we assume all nodes in the network have the same capability (e.g. transmission power, signal sensitivity), and they know their own locations. Many existing works have dealt with the problem of node localization in WSNs, and lots of localization technologies can be used [13], [14]. Finally, we assume that each node in WSNs can recognize its state of jammed or un-jammed, and discover the existence of the jammer [1], [15]. In this work we only focus on how to localize the jammer after jamming is detected.

B. *Jammer Model and Jamming Effects on Communications*

A jamming device may continuously emit electromagnetic energy on the medium, or keep staying quiet until it has sensed activities on the channel, and then it starts transmitting radio signals to corrupt ongoing messages. Despite the various attack strategies that a jammer may adopt to interfere with wireless communications [1], purposes and effects of strategies are the same – reducing the signal-to-noise ratio (SNR) of messages in a target area [12]. In this work, we assume a static jammer with isotropic influence, which keeps emitting jamming signals to disturb communications in WSNs. Only one jammer is considered in this work, and the jammer is assumed to be stationary. Our future work will investigate jammer localization under more complicated jamming scenarios, including comprehensive irregular jammed regions, jammers with directional antennas, and multiple jammers with overlapping jamming regions.

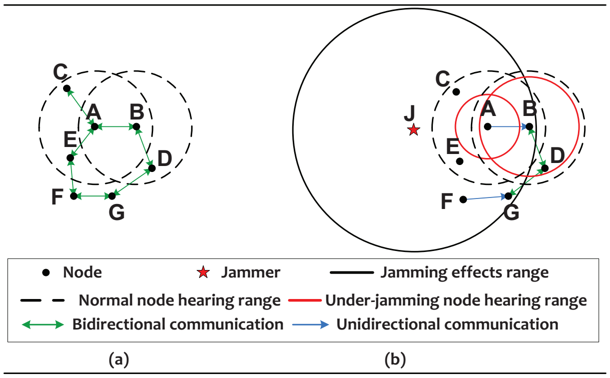
C
A
B
E
D
F
G
J
● Node
★ Jammer
Jamming effects range
Normal node hearing range
Under-jamming node hearing range
Bidirectional communication
Unidirectional communication
(a)
(b)

Figure 1. Jamming effects in wireless sensor network. (a) a part of the wireless sensor network, where hearing ranges of node A and B are represented by dashed circles. (b) a jammer in the network, which affects communications between sensor nodes.

In Figure 1, we show the effects of jamming attacks on communications in a wireless sensor network. Figure 1(a) shows a part of the wireless sensor network without jamming attacks. There are seven nodes $\{A, B, C, D, E, F, G\}$ in the field, and the *hearing ranges* of nodes A and B are shown by two dashed circles [12]. Here nodes A and B can send and receive messages from each other. All nodes in Figure 1(a) have bidirectional communications with adjacent nodes, which are represented by double-headed arrow lines. Figure 1(b) shows the scenario of jamming attacks in a wireless sensor network. The star J represents a jammer. Applying the free-space model to the jammer, jamming signals attenuate with distance, and they reduce to the normal ambient noise level at a circle centered at the jammer. We use this circle to denote the jamming effect range, which is the solid circle centered at the jammer in the figure. Under effects of jamming attacks, hearing ranges of nodes in the jamming effect range are reduced. As shown in Figure 1(b), the hearing ranges of node A and B are changed from original ranges, the dashed circles, to the new ranges, the smaller solid circles centered at themselves. According to the standard free-space propagation model, the power of jamming noise will be higher when nodes are nearer to the jammer, which makes the new hearing range of node A much smaller than that of node B. With the new hearing range, node A is within node B's hearing range, while node B is out of node A's hearing range. So node A and B can only have a unidirectional communication from nodes A to B, and communications between inside nodes are disrupted completely.

According to the influence of the jammer, nodes in a wireless sensor network could be divided into three types: jammed nodes, unaffected nodes and boundary nodes. As shown in Figure 1(b), nodes $\{A, C, E, F\}$ are jammed nodes. These jammed nodes can implement the jammer detection algorithms [1], and they can keep broadcast *jammed messages* to their neighbors [15], pulling the trigger of jammer localization algorithms. Unaffected nodes are far away from the jammer and not affected by the jammer at all, as node $\{D\}$ in Figure 1(b). Boundary nodes are not jammed, however, parts of its neighbors are jammed. Having normal communications with most neighboring nodes, these boundary nodes can be used to detect the existence of the jammer and measure some properties of the jamming messages, such as RSS. In Figure 1(b), nodes $\{B, G\}$ near the edge of jamming effects range are boundary nodes. As boundary nodes are close to jammed area, they may receive jammed messages and our jammer localization algorithms can be activated, e.g., nodes B and G may detect the jammed messages sent by nodes A and F, respectively, in Figure 1(b).

IV. Existing Algorithms

In this section, we provide an overview of three existing jammer localization algorithms: Centroid Localization (CL), Weighted Centroid Localization (WCL), and Virtual Force Iterative Localization (VFIL). We also analyze their advantages and disadvantages.

A. Centroid Localization

Centroid Localization [16] is derived from the idea of centroid, which is the geometric center in geometry. CL uses location information of all neighboring nodes, which are nodes located within the transmission range of the target node. In case of jammer localization, the target node is the jammer, and the neighboring nodes of the jammer are jammed nodes. CL collects all coordinates of *jammed nodes*, and averages over their coordinates as the estimated position of the jammer. Assuming that there are N jammed nodes $(X_1, Y_1), (X_2, Y_2), ..., (X_N, Y_N)$, the position of the jammer can be estimated by:

$$(\hat{X}_{jammer}, \hat{Y}_{jammer}) = (\frac{\sum_{i=1}^{N} X_i}{N}, \frac{\sum_{i=1}^{N} Y_i}{N}) \tag{1}$$

B. Weighted Centroid Localization

Weighted Centroid Localization [17] adds different contributions to the involved node coordinate information in estimating the location of the target node. We usually call the contribution as *weight*. One nature metric to be used as weight is the distance between the jammer to the boundary node. By adding the weighing factor into the centroid method, the jammer's position is estimated as:

$$(\hat{X}_{jammer}, \hat{Y}_{jammer}) = (\frac{\sum_{i=1}^{N} \omega_i X_i}{\sum_{i=1}^{N} \omega_i}, \frac{\sum_{i=1}^{N} \omega_i Y_i}{\sum_{i=1}^{N} \omega_i}) \tag{2}$$

The weight $\omega_i = \frac{1}{d_i^2}$, where d_i is the distance between the i-th neighboring node and the jammer node. One possible way to acquire a distance is measuring the received signal strength (RSS) of the incoming radio signal, which is inversely proportional to distance. In this paper, WCL only uses the boundary nodes' location information as samples for location estimation, and their RSS measurements as weight factors to indicate the distance between the jammer and neighboring nodes.

C. Virtual Force Iterative Localization

Virtual Force Iterative Localization (VFIL) [7] tries to improve CL by adjusting the estimation of CL according to the jammed nodes' distribution. VFIL first estimates the jammer's transmission range, then generates an estimated jammed region in a circle shape (This circle uses the estimation result of CL as the center and covers all jammed nodes while all boundary nodes fall outside of the region.), and after that, it changes the center of the estimated jammed region in the network iteratively in order to cover the most jammed nodes. VFIL assumes that when the estimated jammer's location equals to the true position, the estimated jammed region will overlap with the real jammed region. To move the estimated location to the real jammer's location, VFIL runs multiple times using two virtual force called *pull* and *push*. At each iterative step, the jammed nodes that are outside of the estimated jammed region should pull the jammed region toward themselves, which is the pull force, while the unaffected nodes that within the estimated jammed region should push the jammed region away from them, which is the push force.

Let (X_0, Y_0) be the estimated position of the jammer, (X_i, Y_i) be the position of a jammed node, and (X_j, Y_j) be the location of a affected node. The force F_{pull}^{i} and F_{push}^{j} as normalized vectors that point to/from the estimated jammer's position:

$$F_{pull}^{i} = [\frac{X_i - \hat{X}_0}{\sqrt{(X_i - \hat{X}_0)^2 + (Y_i - \hat{Y}_0)^2}}, \frac{Y_i - \hat{Y}_0}{\sqrt{(X_i - \hat{X}_0)^2 + (Y_i - \hat{Y}_0)^2}}],$$

$$F_{push}^{j} = [\frac{\hat{X}_0 - X_j}{\sqrt{(\hat{X}_0 - X_j)^2 + (\hat{Y}_0 - Y_j)^2}}, \frac{\hat{Y}_0 - Y_j}{\sqrt{(\hat{X}_0 - X_j)^2 + (\hat{Y}_0 - Y_j)^2}}] \tag{3}$$

Paper [7] chooses a threshold of 100 iterations as the stop point during the adjustment of virtual force. More details can be obtained from [7].

V. The Double Circles Localization Algorithm

A. Motivation

Both CL and WCL are sensitive to node distribution and network density, and VFIL has difficulties on jammer

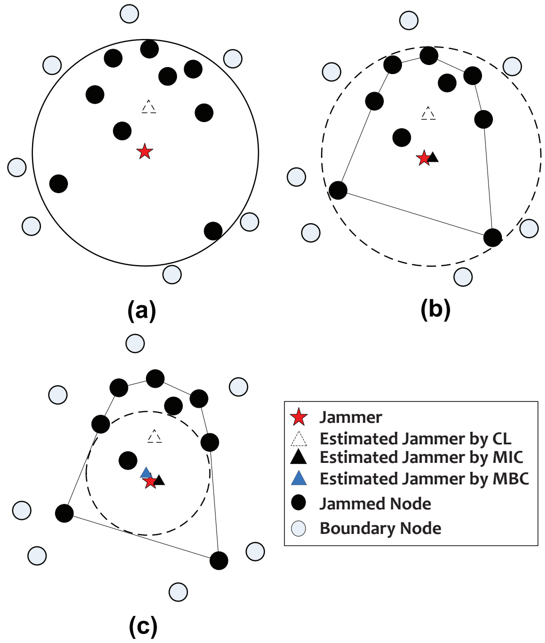

Figure 2. Double Circles Localization (DCL).

transmission range estimation. Firstly, as CL and WCL rely on the coordinates of jammed nodes and boundary nodes, respectively, they will be influenced by node distribution. VFIL uses a circle region to simulate the real jammed area and adjusts it iteratively according to node distribution on the edge of a jammed area. In this way, because the iterative adjustments of VFIL only rely on nodes near the jammed area while no inner jammed nodes could affect the estimation result, VFIL decreases the algorithm's dependence on node distribution. We find that a classic concept in geometry, the minimum bounding circle (MBC), could be used to overcome this problem. In geometry, MBC is the smallest circle that completely contains a set of points. In jammer localization, based on the topology of the peripheral jammed nodes, MBC can easily achieve the goal of VFIL, which is to find a circle that can cover all jammed nodes but no boundary nodes. MBC is easier to implement than VFIL, and works without the knowledge of jammer transmission range. Secondly, we also consider about the VFIL's drawback about the assumption that jammer has a circular jamming interference. In a real environment, due to the various environment effects on the jamming signal propagation at different directions, namely *radio irregularity* [18], we may not be able to simulate a circular jammed area to cover only all jammed nodes. The actual jammed area always is a shape based on a circle while its edge is irregular [18]. This irregularity is not considered by VFIL, and could result in errors. So we introduce another classic geometric concept, the maximum inscribed circle (MIC), to deal with effects of irregularity. MIC is the largest inscribed circle in the *convex hull* of a set of points. Using MIC, we can reduce the effects from jammer radio irregularity.

Thus, to improve existing algorithms, we develop the double circle localization algorithm (DCL), merely based on network topology without any other assumptions about the jammed area. Double circles refer to the minimum bounding circle (MBC) and the maximum inscribed circle (MIC). By combining the centers of the two circles as the estimated jammer location, taking advantages of both concepts, we get the estimation result in a better accuracy than the existing algorithms.

Figure 2 shows a simplified overview of our algorithm DCL. In Figure 2(a), we show that a wireless sensor network with the jammer represented by a star. The solid circle indicates the jammed area, where the black nodes inside it are jammed nodes, and the other nodes outside of the circle are all boundary nodes. We also show the estimated jammer by CL, the white dashed triangle, showing CL is sensitive to the distribution of the jammed nodes. In Figure 2(b), we show the MBC and its center in a black triangle. There is a polygon, called *convex hull*, which is used to calculate the MBC and MIC. In Figure 2(c), we show the MIC and its center in a blue triangle (It would be gray in the printed version). We can observe that through combination of the two circles' results, DCL can reduce the impact from the distribution of the jammed nodes, and achieve better accuracy in jammer localization. To our best knowledge, we are the first one to introduce the MBC and MIC into the area of jammer localization in WSNs, which improve the accuracy of jammer localization.

B. Algorithm

Next we describe our algorithm in more details. Assume that there are N jammed nodes (X_1, Y_1), (X_2, Y_2), ..., (X_N, Y_N). Algebraically, the convex hull of X can be characterized as the set of all of the convex combinations of finite subsets of points from X, as the following formula.

$$\begin{aligned} H_{convex}(X) \quad &= \quad \{\sum_{i=1}^{k} \alpha_i x_i \mid x_i \in X, \alpha_i \in R, \\ &\alpha_i \geq 0, \sum_{i=1}^{k} \alpha_i = 1, k = 1, 2, ...\} \end{aligned} \tag{4}$$

In mathematics, the convex hull, or convex envelope, for a set of points X in a real vector space V, is the minimal convex set containing X. In simple terms, a convex hull here is the polygon that completely encloses all jammed nodes with the fewest number of nodes on the perimeter, as shown in Figure 2(b). There are two main properties of convex hulls. One is that all of the nodes in the final polygon must be indented outwards, or more formally, convex. Another important property is that the most extreme point on any axis is part of the convex hull. In computational geometry, how to find out the convex hull for the finite nonempty set of points in the plane has been well studied. Unless the

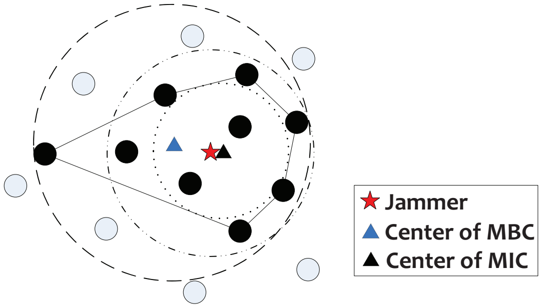

Figure 3. A scenario of jammed area irregularity.

points are collinear, the convex hull in this case is a convex polygon, typically represented by a sequence of its vertices ordered along its boundary. A number of algorithms (such as Incremental, Gift Wrap, Divide and Conquer, QuickHull) have been proposed for computing the convex hull of a finite set of points, with various computational complexities.

After having found out jammed nodes that locate on the convex hull,(X_1, Y_1), (X_2, Y_2), ..., (X_m, Y_m), we calculate the MBC and MIC with this convex hull (we don't show the details about the algorithms due to the page limt), as we show in Figure 2. Meanwhile, to achieve better resistance to the node distribution and the jammed area irregularity, DCL uses not only jammed nodes information but also boundary nodes information, assuming their coordinates are (X_1', Y_1'),(X_2', Y_2'),...,(X_k', Y_k'). we do the same processes to boundary nodes information as we do to jammed nodes information previously, finding out the convex hull of boundary nodes, getting another MBC and MIC. Then we set the average values of the two as the finial MBC and MIC values, using the following equations:

$$(X_{MBC}, Y_{MBC}) = ((X_{mbc} + X_{mbc}')/2, (Y_{mbc} + Y_{mbc}')/2),$$
$$(X_{MIC}, Y_{MIC}) = ((X_{mic} + X_{mic}')/2, (Y_{mic} + Y_{mic}')/2) \tag{5}$$

Finally we derive our result using the following equation:

$$(\hat{X}_{jammer}, \hat{Y}_{jammer}) = (\omega_1 X_{_{MBC}} + \omega_2 X_{_{MIC}}, \omega_1 Y_{_{MBC}} + \omega_2 Y_{_{MIC}}) \tag{6}$$

where (X_{mbc}, Y_{mbc}) and (X_{mic}, Y_{mic}) are the circle centers of MBC and MIC, the values for ω can be obtained by either an empirical approach under the condition of $\omega_1 + \omega_2 = 1$.

C. Discussion

The DCL algorithm uses classic geometric concepts, overcomes the weakness of the VFIL, and hence it shall be able to achieve better results. In DCL, the MBC is able to take the place of VFIL, finding out the circle covers all jammed nodes. Meanwhile, MIC can reduce the impact of jammed area irregularity, by making the estimated location closer to the main area of the jammed region. Figure 3 shows a scenario of jammed area irregularity, in which the jammer has an accidental stronger effect on its left. In Figure 3, the jammer represented by a star is supposed to have a circular jammed area in the network, which should be the middle dashed circular area. However, on the jammer's left side, probably due to environment effects, the jammer has a better interference performance than other directions, and it ends up jamming a node which is a little farther from it. This is a typical scenario of jammed area irregularity. We show the estimation results of both MBC and MIC, which are represents by the bigger dashed circle and the smaller dashed circle, respectively. The blue triangle is the center of MBC and the black one is the center of MIC. Figure 3 shows that the MIC is able to reduce the effects from jammed area irregularity and improve the overall estimation accuracy.

VI. Simulation Evaluation

In this section, we evaluate these jammer localization algorithms through simulation, compare their performance and analyze the elements affecting the algorithm performance. Advantages and disadvantages of these algorithms will also be discussed.

A. Methodology

Simulation Setup. We use MATLAB to generate the wireless network environment, which is a square field with a size of $100m^2$. All network nodes are uniformly distributed in this area with a transmission range of 10 meter. We place the jammer at the center of this simulation area so that the jammer is surrounded by multiple networks nodes. We evaluate the performance of localizing the jammer by running CL, WCL, DCL and VFIL under various network node densities and jamming powers. We change these network parameters to uncover their impacts on these algorithms. For every setup, we run these algorithms 1000 times for jammer localization to obtain the statistical evaluation of theirs performance. In this simulation, we establish the radio propagation channel model of the jammer with the well known and used formula, considering the path-loss and the shadowing. The ratio of received to transmitted power in dB is given by

$$\frac{P_r}{P_t}dB = 10\log_{10} K - 10\gamma \log_{10} \frac{d}{d_0} - \psi_{dB}, \tag{7}$$

where ψ_{dB} is a Gauss-distributed random variable with mean zero and variance $\sigma^2_{\psi_{dB}}$, K is a unitless constant that depends on the antenna characteristics and the average channel attenuation, d_0 is a reference distance for the antenna far field, and γ is the path-loss exponent[19].

Metrics. To evaluate the accuracy of jammer localization, we define *localization error* as the Euclidean distance between the estimated location of the jammer and the actual location of the jammer in the network. To capture the statistical characterization of the localization errors, we study the cumulative distribution function (CDF) of the localization errors for all 1000 rounds in each experimental setup.

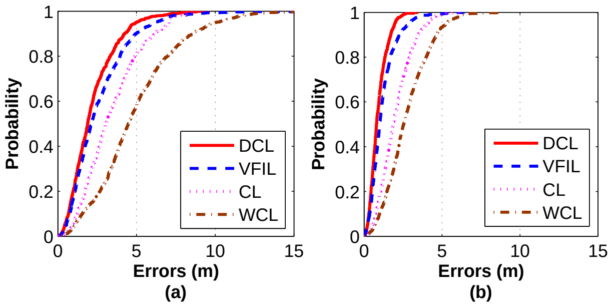

Figure 4. Impact of different node densities with the transmission range set to 20dbm : (a) N = 100; (b) N = 300.

B. Simulation Results

Sensitivity of Node Density. We first study the effects of various network node densities to localization accuracy. To adjust the network node density, we vary the total number of nodes N deployed in the simulation. Figure 4 presents the localization results across different algorithms when the total number of node is set to 100 and 300, respectively. We observe that all the algorithms under study are more or less sensitive to network node densities. Overall, the higher node density is, the better localization accuracy can be achieved. In Figure 4, DCL consistently achieves the best performance among all the algorithms under both node density setups. In both scenarios, we notice that WCL has worse performance than CL, which confirms our expectation in Section IV. That is, the WCL algorithm needs some information to represent the distance between a measuring node and the jammer. In the presence of jamming, we can only use the boundary nodes which are farther away from the jammer than the jammed nodes; hence, it introduces non-negligible errors into their distance measurements. Meanwhile, we observe that the VFIL also works well in both scenarios, only a little worse than DCL, but better than other algorithms. The latter is in accordance with the simulation results in [7].

Impact of Jammer's Transmission Power. We next examine the impact of different jamming ranges on the localization error. Figure 5 presents the localization performance of all algorithms where the transmission power of the jammer is set to 20 dbm, 30 dbm, and 40 dbm, respectively, and the number of network nodes is fixed at 200. In general, we observe the consistent localization performance: DCL achieves the best performance under different jamming ranges. Further, we observe that DCL and VFIL have a palpable improvement with the increase of the jammer's transmission power from 20 dbm to 40 dbm, which shows that both DCL and VFIL are sensitive to the jammer's transmission power. We also observe that the performance of CL is not impacted by the jammer's transmission power, whereas WCL has a palpable decline when the power is set to 40 dbm. This indicates larger jammed regions introduce more errors in the localization result of WCL.

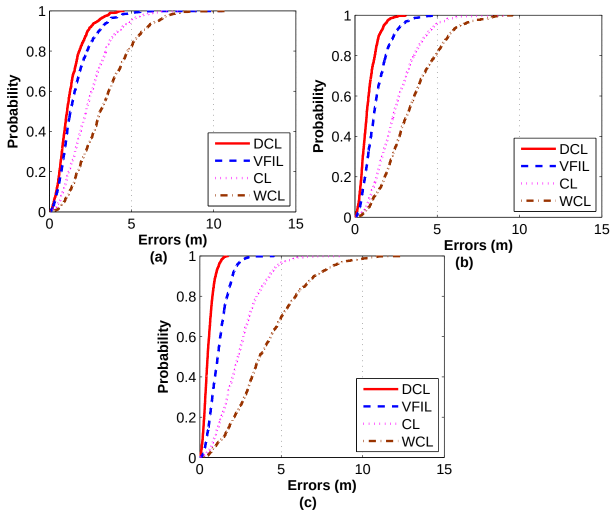

Figure 5. Impact of different jammer's transmission power when the network node density is 200:(a)20dbm, (b)30dbm,(c) 40dbm.

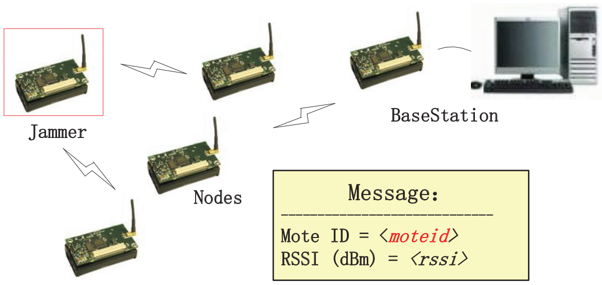

Figure 6. System architecture.

VII. Experiment evaluation

In this section, we establish a small wireless sensor network with a few MICAz motes and record all nodes' coordinate information and the RSS measurements under existing of a jammer in the middle. Then we run these algorithms with the raw data from the real environment, and compare their jammer-location estimation results. The goal of this experimentation is not only to validate our simulation results, but also to experiment with irregular jamming scenarios that are hard to be simulated.

A. Experimental setup

We used the MPR2400CA (2.4 GHz) MICAz motes, which are supplied by the Crossbow Technologies, for our experiments. Our experiments (Figure 6) consist of three modules: One mote is programmed as the jammer, which keeps sending interference signals. One mote is used as Base Station to collect all RSS data measured by all unjammed nodes for further analysis, and the other motes are randomly deployed on the ground, forming a small wireless sensor network. In this experimentation, the location of the jammer is fixed at (0,0) in the center of the network. Nodes of the network, 30 in all, are deployed around the jammer in

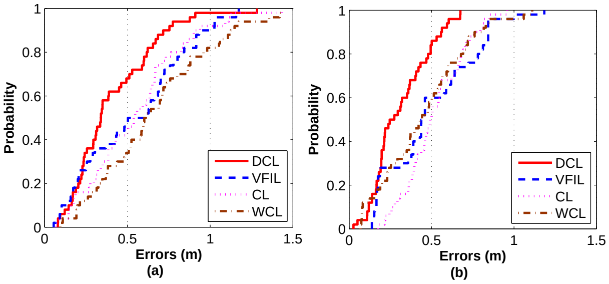

Figure 7. Impact of different node densities with the transmission range set to -11 dbm : (a) N = 30; (b) N = 50.

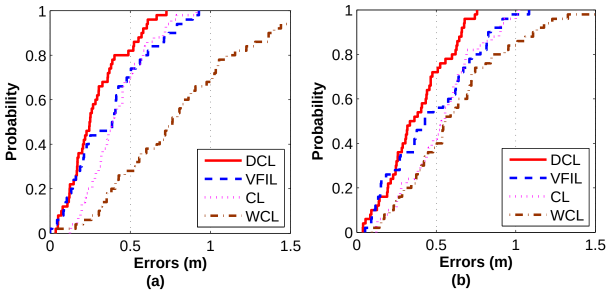

Figure 8. Impact of different jammer's transmission power: (a) -14dbm; (b) -11dbm.

a square field (10m×10m), while the base station connected to a computer is fixed outside of the network, as shown in Figure 6.

More specifically, the MICAz nodes, with transmission range set as 3 meter, are deployed around the jammer in a 2 meter of mean-distance between each other. For more convenience and accuracy in our experiment, no inter-node communication is introduced, and we let every node discover itself jammed or not by using the RSS information[1] to check the SNR threshold. After a fixed time, all un-jammed nodes will stop measuring and send messages, including the mote ID and the RSS information, to the base station node. After all messages are received, we just repeat these steps with different node distributions. In each experiment, we change the node distribution fifty times. For different experiments, we will change the place or jammer transmission power to compare our algorithms under various situations.

To evaluate the accuracy of jammer localization, we again show the cumulative distribution function (CDF) of the localization errors for all experiments.

B. Experiments Results

Impact of Various Node Density. We first study the effects of various network node densities to localization performance. Figure 7 presents the localization results across different algorithms, where total number of nodes is set to 30 and 50, respectively, and the transmission power of the jammer is fixed at -11dbm, corresponding to 3 meter transmission range of the jammer node. We observe, in this figure, all the algorithms are sensitive to network node densities in the real environment, which is consistent with our simulation result: the higher the node density, the better the localization accuracy. We also find that the DCL still performs the best here.

Impact of the Jammer's Transmission Power. Then, we study the effects of different jammer's transmission powers to the performance of these algorithms. we change the RF power parameter of the MICAz jammer from 8 to 10, corresponding to -14 dbm, and -11 dbm, while the node number is 30 with the same node density. Figure 8 shows the performance of these algorithms, where we can see that the CL is not impacted by the changes of the jammer's transmission power, which is accordant with the simulation result. DCL and VFIL are only slightly affected by the changes in jammer's power. This is because the power change is not as great as we did in simulation. We also observe that WCL has an upgraded performance when the power increases, which is opposite to the simulation result. That's probably because the change of 3 dbm does not increase the jammed region much (vs. the change of 10 dbm in simulation). Our conjecture is that the jammer's transmission power and jammed region may have different influences to WCL. This would be a future direction to figure out the relationship between these properties. Finally, DCL achieves the best performance among the four algorithms.

Impact of the Jammer's Antenna Orientation In general, the signal power received by a receiving antenna is dependent on the orientation of the receiver antenna with respect to the transmission antenna, and more loss is likely to be experienced if there is polarization mismatch [20]. This could make the jamming interfering range become irregular instead of a circle. Compared with the previous experiments, we only changed the jammer's antenna orientation, from perpendicular to horizontal to the ground. In Figure 9, we made the jammer antenna horizontal to the ground, pointing to the north (a) and east (b), respectively, in two experiments, while the jammer's transmission power was fixed at -14 dbm, and the number of nodes is 30, which is under the same conditions as in our previous experiments in Figure 8 (a). Because VFIL needs a circle-jammed region, it is not suitable for this kind scenario, so we do not show it in this evaluation. Comparing these two figures with the previous results 8, We can observe that the WCL algorithm has obvious improvement after the antenna is no longer perpendicular to the ground. This is probably because the number of the boundary nodes increases when the jammed area changes from a circular area to an irregular one. Meanwhile, we observe that the other two algorithms have slight improvements. This is due to the dissipated energy making jammed area becomes smaller than it does at the normal scenario, so that both DCL and CL get benefits from the changes. And we observe that DCL still have the best

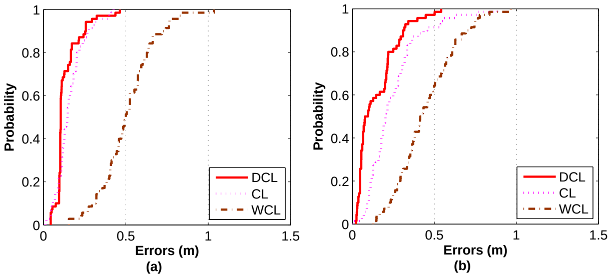

Figure 9. Impact of the jammer's antenna orientation: (a) horizontal-northward, (b) horizontal-eastward .

performance among all algorithms.

VIII. Conclusions and Future work

This paper introduces several jammer localization algorithms, including three existing algorithms, CL, WCL and VFIL, and one new algorithm, DCL. We then compare these algorithms through simulation and experiments, and show their performance under different conditions or situations. From previous sections, we observe that all these algorithms are sensitive to node density in both simulation and experiments, and we find out DCL always performs the best in all the situations.

In this paper, we only explored the one jammer localization scenario. The problem of directional jammer and multiple jammer localization would be our ongoing work. Also, all simulation and experiments were implemented without network background communication signals. We will improve our algorithm in the future.

Acknowledgement: We thank the reviewers for their valuable comments.

References

[1] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Mobihoc '05: Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2005, pp. 46–57.

[2] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference," in *IPSN '07: Proceedings of the 6th international conference on information processing in sensor networks*, 2007, pp. 499–508.

[3] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *SP'08: Proceedings of the 2008 IEEE Symposium on Security and Privacy*, 2008, pp. 64–78.

[4] E. F. Velez and M. G. Amin, "Improved jammer localization using multiple focusing," in *Advanced Signal Processing Algorithms, Architectures, and Implementations*, 1990, pp. 484–492.

[5] S. Coutts, "3-d jammer localization using out-of-plane multipath," in *RADARCON'98: Proceedings of the 1998 IEEE Radar Conference*, 1998, pp. 219 –224.

[6] L. Xiangqian, "Signal detection and jammer localization in multipath channels for frequency hopping communications." Defense Technical Information Center OAI-PMH Repository (US), 2005.

[7] H. Liu, W. Xu, Y. Chen, and Z. Liu, "Localizing jammers in wireless networks," in *PERCOM'09: Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications*, 2009, pp. 1–6.

[8] G. Noubir and G. Lin, "Low-power dos attacks in data wireless lans and countermeasures," in *ACM SIGMOBILE Mobile Computing and Communications*, 2003, pp. 29–30.

[9] M. Cagalj, S. Capkun, and J. Hubaux, "Wormhole-based antijamming techniques in sensor networks," in *IEEE Transactions on Mobile Computing*, 2007, pp. 100–114.

[10] B. Sklar, *Digital Communications, Fundamentals and Applications*, 2nd ed. Prentice-Hall, 2001.

[11] P. Konstantinos, K. Iordanis, I. Broustis, and S. V. Krishnamurthy, "Lightweight jammer localization in wireless networks: system design and implementation," in *GLOBECOM'09: Proceedings of the 28th IEEE conference on Global telecommunications*, 2009.

[12] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Wireless jamming localization by exploiting nodes' hearing ranges," in *DCOSS'10: Proceedings of the International Conference on Distributed Computing in Sensor System*, 2010, pp. 348–361.

[13] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. F. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *MOBICOM'03: Proceedings of the 9th International Conference on Mobile Computing and Networking*, 2003, pp. 81–95.

[14] G. Mao, B. Fidan, and B. Anderson, "Wireless sensor network localization techniques," in *Computer Networks*, 2007, pp. 2529–2553.

[15] A. D. Wood, J. A. Stankovic, and S. H. Son, "Jam: A jammed-area mapping service for sensor networks," in *RTSS'03: Proceedings of the 24th IEEE International Real-Time Systems Symposium*, 2003, pp. 286 – 297.

[16] N. Bulusu, J. Heidemann, and D. Estrin, "Gps-less low cost outdoor localization for very small devices," in *IEEE Personal Communications Magazine*, 2000, pp. 28–34.

[17] J. Blumenthal, R. Grossmann, F. Golatowski, and D. Timmermann, "Weighted centroid laocalization in zigbee-based sensor networks," in *WISP'07: Proceedings of the IEEE International Symposium on Intelligent Signal Processing*, 2007, pp. 1–6.

[18] Z. Gang, H. Tian, K. Sudha, and S. J. A., "Models and solutions for radio irregularity in wireless sensor networks," in *ACM Transactions on Sensor Networks*, 2006, pp. 221–262.

[19] A. Goldsmith, *Wireless Commulications*. Cambridge University Press, 2005.

[20] K. S. Jin, M. J.C., and S. G., "Rf characteristics of mica-z wireless sensor network motes," in *MWSCAS'06: Proceedings of the 49th IEEE International Midwest Symposium on Circuits and Systems*, 2006, pp. 100–104.