Catch the Jammer in Wireless Sensor Network

Yanqiang Sun[1], Refik Molva[2], Melek Önen[2], Xiaodong Wang[1], Xingming Zhou[1]
[1]College of Computer Science, National University of Defense Technology, Changsha, China
[2]Department of Networking and Security, EURECOM, Sophia Antipolis, France
Email: [1]{yq_sun, xdwang, xmzhou}@nudt.edu.cn, [2]{refik.molva, melek.onen}@eurecom.fr

***Abstract*—Jamming attacks can severely affect the performance of Wireless Sensor Networks (WSNs) due to their broadcast nature. The most reliable solution to reduce the impact of such attacks is to detect and localize the source of the attack. In this paper, we investigate the feasibility of localizing an omni-antenna jammer. We propose *Catch the Jammer* (*CJ*), an efficient jammer localization scheme whereby victim nodes at the border of the jammed region share their location information with their one-hop neighbor nodes which further collaborate to find the position of the jammer. This new localization technique first computes a convex hull for the set of victim nodes and further extracts the corresponding minimum covering circle. Simulation results show that *CJ* outperforms most of the existing localization algorithms depending on the variation of the jammer's transmission range and the position of the jammer.**

Keywords-wireless sensor network; jammer; localization; convex hull; minimum circle covering

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are vulnerable to radio interference attacks due to their broadcast nature. Such attacks, also known as jamming attacks, can easily be launched by any node and can cause serious damages on the performance and robustness of the network. Various mechanisms such as DSSS (Direct Sequence Spread Spectrum) or FHSS (Frequency Hopping Spread Spectrum), have been proposed to prevent jamming attacks at the physical layer [1-3]; however, unfortunately, such solutions are not realistic in the context of WSNs due to their high cost in terms of energy. Some further evasion strategies, such as wormhole-based anti-jamming techniques [4], channel surfing [5] and covert timing channel [6], have also been proposed to deal with such attacks in the upper layers.

Unlike jammer detection and prevention, the issue of determining the jammer's physical position, known as, the problem of jammer localization has attracted much less attention. Finding the location of the adversary or jamming attacker is of great importance for restoring the normal network operations and taking further security actions. Furthermore, the location of the jammer provides important information for network operations in various layers [7]. For example, a routing protocol can choose a path that does not traverse the jammed region to prevent packet delivery failures.

Localizing a jammer is not a trivial task. Indeed, existing localization techniques [8] cannot be used for jammer localization. For instance, many localization schemes require the wireless sensor to be equipped with specialized hardware, e.g., ultrasound or infrared, or use signals sent from sensors to perform localization. Unfortunately, the jammer will not cooperate and the jamming signal is usually embedded in the legal signal and is hard to be extracted, making the signal-based and special hardware-based approached unfeasible. Furthermore, such localization methods also require lots of energy and cannot directly be used in the context of energy-constrained sensor networks.

In this paper, we consider the problem of how to localize an omni-antenna jammer which has an isotropic effect in WSNs. We propose ***Catch the Jammer (CJ)***, an efficient jammer localization scheme where sensor nodes collaborate with each other to compute the coordinates of the jamming attacker. As opposed to existing localization techniques which locate jamming attacks based on the characteristics of the received signal, ***CJ*** only requires victim nodes' location information. Nodes located at the border of the jammed area will be able to exchange their location information and determine the jammer's coordinates thanks to the use of different computational geometry algorithms. Nodes first compute a convex hull for the set of victim nodes based on their coordinates. They further extract the corresponding smallest circle that covers all nodes in the convex hull in order to achieve a good accuracy on the coordinates of the adversary.

The remainder of this paper is organized as follows. In the next section, we provide a brief description of existing solutions. Section III introduces the network assumptions. The localization scheme and the proof of its correctness are described in section IV. Finally, in section V we evaluate the performance and accuracy of the proposed scheme through various simulation results.

II. RELATED WORK

Recently, jamming attacks in wireless ad hoc and sensor networks have been widely analyzed, and various solutions addressing the detection [3], the countermeasures [4-6], and game theory based defense strategies [10] have been proposed. However, only a few studies tackled the problem of jammer localization, which is the focus of this paper. Liu et al. [7] introduced a scheme called VFIL (Virtual Forces Iterative Localization), which uses the concept of virtual forces to estimate the jammer's position based on the changes in the network topology. The virtual forces are derived from the state of nodes and can help estimate the location of the jammer towards its true position in an iterative fashion. These localization solutions rely on iterative search which involves high computation overhead. In order to reduce the cost of

This work is supported by the National Natural Science Foundation of China under Grant No. 61070203 and the National Grand Fundamental Research 973 Program of China under Grant No. 2006CB303000

computation, measurement-based jammer localization schemes were proposed in [11-12]. However, these schemes are highly dependent on the wireless jamming models, and may suffer from inconsistencies with respect to the network environments.

Centroid Localization (CL) [13] uses position information of all neighboring nodes, which are located within the transmission range of the targeted node. For example, assume that there are N neighboring nodes $\{(X_1, Y_1), (X_2, Y_2), ..., (X_n, Y_n)\}$, the estimated position of the target node is:

$$(\bar{X}_{target}, \bar{Y}_{target}) = (\frac{\sum_{k=1}^{N} X_k}{N}, \frac{\sum_{k=1}^{N} Y_k}{N})$$

An enhanced version of CL is Weighed Centroid Localization (WCL) [13], which adds weight value into the process of estimating target node position. Both the CL and WCL can be used to localize the jammer. These two methods, however, are highly affected by the variation of the density and distribution of nodes in wireless sensor networks.

III. NETWORK ASSUMPTION

In this section, we outline the basic network models and jamming models that we use throughout the paper.

A. Network Model

Devising a generic approach that works across all kinds of sensor networks is impractical. We consider a wireless sensor network over a large area. As an initial work, we aim at tailoring our proposal to a category of sensor networks with the following characteristics.

- *Stationary*. We assume that once deployed, the location of each sensor node remains unchanged.
- *Location-Aware*. Each node knows its location coordinates. This is a reasonable assumption as many applications require location services, and the neighbor table can be maintained by most routing protocols.

In this paper, we focus on the issue of jammer localization after the jamming attack has been detected. The scheme of how to detect a jamming attack is not considered. The details of jamming detection can be referred in [3].

B. Attack Model

We assume a static jammer which has an isotropic effect, i.e., the jammed region can be modeled as a circular region centered at the jammer's location. Under jamming attack, the network nodes can be divided into three categories:

- *Unaffected node.* We define the nodes that are outside the jammed region as the unaffected nodes.
- *Border node.* The border nodes suffer from jamming attack, but still satisfy the demanding SINR (Signal to Interference and Noise Ratio), i.e., the border nodes are still in the hearing range as defined in [12].
- *Jammed node.* The jammed nodes are those that have been totally blocked by the jammer.

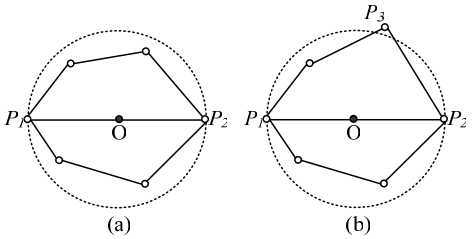


Fig.1. Example showing the covering scheme

Tab.1. Notation

n	Number of jammed nodes
Q	Set of jammed nodes
CH (Q)	Convex hull of *jammed* nodes
m	Size of convex hull CH (Q)
P_i	Sensor node i
P_iP_j	Diameter of CH (Q)
$\mathbb{C}$	Circle
O	Centre of circle
$d(A, B)$	Euclidean distance between A and B
$\overline{AB}$	Chord of circle $\mathbb{C}$
$\widehat{ACB}$	Angle of ACB
▲ABD	Triangle of ABD

IV. THE PROPOSED LOCALIZATION SCHEME

The notation used in the paper is summarized in Table 1.

The basic idea of ***Catch the Jammer (CJ)*** is two-fold: First, when detecting the jamming attack, nodes located at the border of the jammed area immediately broadcast an "I am jammed!" message to their one-hop neighbors that are just outside of the jammed region. Based on the Jammed Area Mapping (JAM) service [9], the neighbors that have received the messages communicate with each other to share the coordinates of the jammed nodes. One node is elected to collect all the border nodes' jammed information and to be in charge of localizing the jammer. Second, this node runs the localization algorithm ***CJ*** by first computing the convex hull of these jammed nodes and by further finding the smallest circle covering all nodes inside the convex hull. The details of these two phases are discussed in the following sections.

A. Construction of Convex Hull

In this section, we introduce the construction of a local convex hull which is formed by the nodes at the border of the jammed area. Our method is mainly based on the classical Jammed Area Mapping Service [9]. When a jamming attack occurs, the legitimate nodes which are close to the jammer are considered to be totally blocked. However, as discussed in Section III, the border nodes still are in the hearing range [12], and can successfully transmit packets.

When the jamming attack is detected, the jammed nodes at the border area broadcast "I am Jammed!" messages to their neighbors that are outside the jammed region. Each of these messages contains the jammed node's ID and physical location information. Neighbor nodes that are outside the jammed region exchange and aggregate these messages and a local leader is elected among these neighbors based on the maximal remaining energy or some other metric to calculate the convex hull that includes all the jammed nodes. Assume that there are

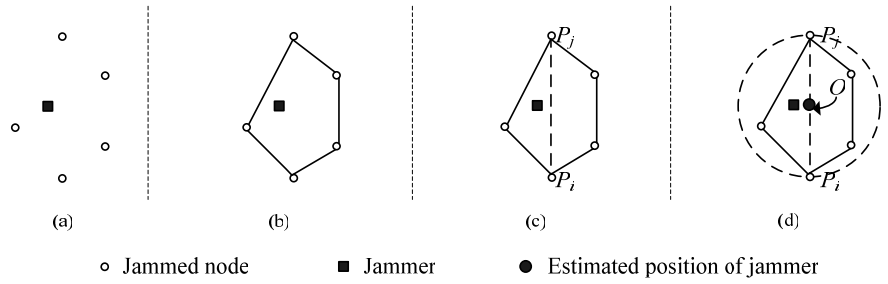


Fig.2. A simple case of algorithm ***CJ***

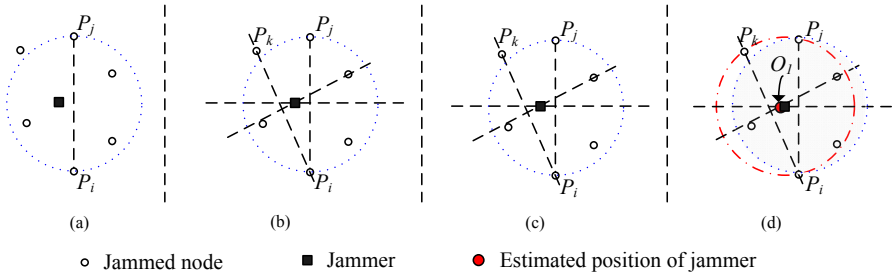


Fig.3. A more complicated case of algorithm ***CJ***

n jammed nodes in the border region. We denote the convex hull of these n nodes by $\mathrm{CH(Q)} = \{P_1, P_2, \ldots P_m\}$, where m is the size of the convex hull.

Once the convex hull is constructed, the diameter P_iP_j which is determined by selecting the pair of nodes that has the maximum [14]; the midpoint of the diameter is denoted by O. We consume that the jamming attack has an isotropic effect. Therefore, as illustrated in figure 1(a), if the circle centered at O with radius OP_i is able to cover all the nodes in CH(Q), then the estimated position of the jammer will be the center O (we assume that the jamming has an isotropic effect) as shown in figure 1(a). However, some of the nodes under jamming attack may not be covered by such a circle as shown in figure 1(b) (Node P_3 is not covered by the circle $\mathbb{C}$). Hence, the convex hull method alone is not always sufficient to determine the position of the jammer. The next section describes the following steps that compute the minimum covering circle.

B. Finding the minimum covering circle

Based on the constructed convex hull, we now describe the algorithm to find the smallest circle that covers all points inside the convex hull.

Step1: The first candidate circle $\mathbb{C}$ is the one obtained in the previous section, in which center O is the midpoint of the diameter P_iP_j of the convex hull. If all nodes are covered by this circle, ***CJ*** successfully ends (Fig. 2). If, on the contrary, there exists a node P_v outside the circle, then go to step 2. More formally, if there exists a node P_v such that $\mathrm{d}(O, P_v) \geq r$, where r denotes the radius of $\mathbb{C}$, then go to step 2.

Step2: Calculate the distance between every node in $\mathrm{CH(Q)} = \{P_1, P_2, \ldots P_m\}$ and the diameter P_iP_j, denoted by $\mathrm{d}(P_u, P_iP_j)$, where $P_u \in \{P_1, P_2, \ldots, P_m\}$, $u \in \{1,2,\ldots,m\}$.

Step3: Determine P_k such that:

$$\mathrm{d}(P_k, P_iP_j) = \max\{\mathrm{d}(P_u, P_iP_j)\}_{u=1, 2, \ldots, m}$$

Step4: Determine the circum-circle $\mathbb{C}_1$ of the triangle $\blacktriangle P_iP_jP_k$ which is defined as the circle passing through all vertices. The center O_1 of $\mathbb{C}_1$ is the intersection of the perpendicular bisectors of the triangle.

Step5: If $\mathbb{C}_1$ covers all nodes, then ***CJ*** successfully ends. Formally, if for all P_v where $v \in \{1, 2, \ldots, m\}$, $\mathrm{d}(O_1, P_v) \leq r_1$ (radius of $\mathbb{C}_1$), then ***CJ*** returns O_1 (Fig.3). If on the other hand, there exists $P_{k'}$ such that $\mathrm{d}(O_1, P_{k'}) > r_1$ then P_k becomes $P_{k'}$ and step 4 and step 5 are executed once again.

V. EVALUATION

A. Correctness

The correctness of ***CJ*** is proved based on the following two lemmas.

Lemma 1: *Let $\overline{AB}$ be a chord of circle $\mathbb{C}$. Suppose that point C is on the circle $\mathbb{C}$ and point D is outside the circle $\mathbb{C}$, C and D are on the same side of $\overline{AB}$. Then $\overset{\frown}{ACB} > \overset{\frown}{ADB}$.*

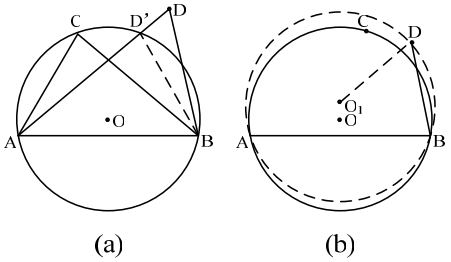
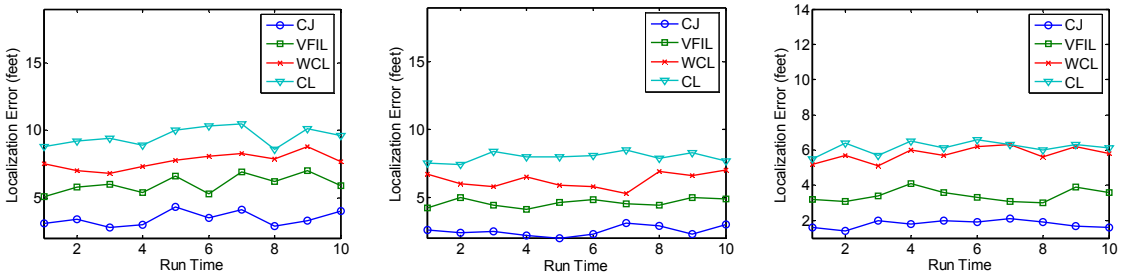


Fig.4. Case of Lemma 1(a), and Lemma 2 (b)

Proof: The lemma is illustrated in figure 4(a). Suppose the segment AD intersects with the circle $\mathbb{C}$ at D'. Connect D' with B. Based on the knowledge of plane geometry, the angles corresponding the same arc in one circle are equal,



(a) 30 feet (b) 45 feet (c) 60 feet

Fig.5. Impact of jammer's transmission range on localization error when N=200

therefore, $\widehat{AD'B} = \widehat{ACB}$. Since $\widehat{AD'B} = \widehat{ADB} + \widehat{D'BD}$, then $\widehat{ACB} > \widehat{ADB}$. Hence we have proved Lemma 1.

Lemma 2: *Let* $\overline{AB}$ *be a chord of circle* $\mathbb{C}$ *. Suppose that point C is on the circle* $\mathbb{C}$ *and point D is outside the circle* $\mathbb{C}$ *. If the distance between C and* $\overline{AB}$ *is larger than the one between D and* $\overline{AB}$ *, i.e.* $d(C,\overline{AB}) > d(D,\overline{AB})$ *, and* $AB > AD$ *, then the point C will be in the circum-circle of* ▲*ABD.*

Proof: As shown in figure 4(b)**,** from the assumption of **Lemma 2** and the conclusion made in **Lemma 1**, we have $\widehat{ACB} > \widehat{ADB}$, and draw the circum-circle $\mathbb{C}_1$ (with the centre O_1) of ▲*ABD*. We now can conclude that C must be in the circle $\mathbb{C}_1$. The reason of this claim is that if C is outside circum-circle $\mathbb{C}_1$, according to **Lemma 1**, we have $\widehat{ADB} > \widehat{ACB}$, which is a contradiction to our previous result.

The lemma 2 indicates that $\mathbb{C}_1$ is the smallest circle which covers the point A, B, C and D.

In ***CJ***, we try to determine the diameter of CH(Q), the midpoint of which will be treated as the estimated position of the jammer if all the jammed nodes fall into the midpoint-centered circle. If there are some nodes that are not in (on) that circle, then we try to find the node which is longest to the diameter. Then based on lemma 1 and lemma 2, we are also able to find out a smallest circle that covers all the jammed nodes. Thus, the correctness of ***CJ*** is proved.

B. Complexity

Algorithm Complexity: the time complexity of calculating the convex hull in the worst case is $O(nlogn)$ [14], where n is number of jammed nodes at the border. The local leader also needs to perform $m(m-1)$ multiplications and $(m(m-1)/2-1)$ comparisons to compute the diameter of circle, where m is the size of the convex hull. The remaining steps only require computation complexity of $O(m^2)$. Therefore the overall time complexity of the proposed algorithm is bounded and less than:

$$n\log n + n + m(m-1) + m(m-1)/2 - 1 \approx O(n\log n + m^2)$$

Normally, the size of the convex hull (m) is much smaller than the number of jammed nodes (n), so the time complexity of ***CJ*** is approximately $O(nlog(n))$, which is reasonable for resource-constrained sensor networks.

Message Complexity: the time complexity incurred by the 'I am jammed' messages which are broadcasted through the border nodes is less than $O(m^2L^2)$, where L refers to the size of the broadcast message.

C. Simulation Analysis

In order to evaluate the performance of ***CJ,*** we simulate a wireless sensor network scenario in a square field with a size of 300 feet by 300 feet. Sensor nodes are randomly distributed in this area with a transmission range of 30 feet. We evaluate the performance of locating the jammer by using ***CJ***, and compare our results with the ones proposed in VFIL [7], WCL [13] and CL [13] under different network densities and jammed regions. We place the jammer at the centre of the simulation area so that the jammer can be surrounded by multiple network nodes. We also randomly change the position of the jammer in order to investigate the effect of the jammer's position on ***CJ***'s performance.

1) Metrics

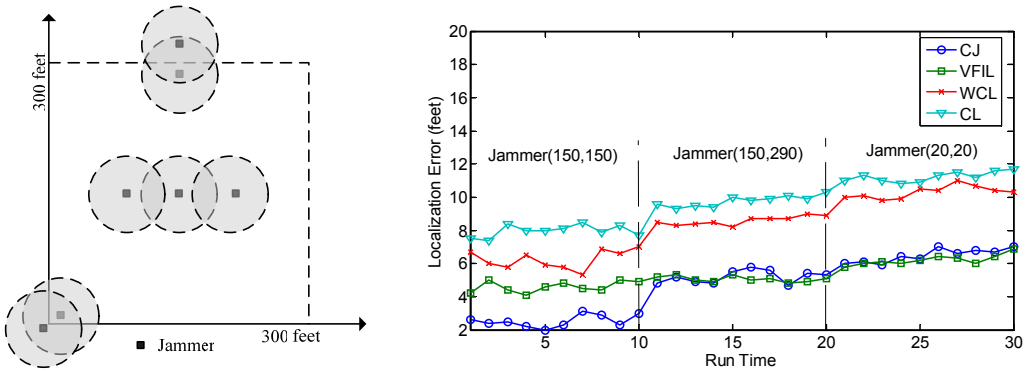
Localization error (Δ): The Euclidean distance between the estimated location of the jammer ($\tilde{X}_i, \tilde{Y}_i$) and the true location of the jammer (X_i, Y_i) in the network is defined as follows:

$$\Delta = \sqrt{(X_i - \tilde{X}_i)^2 + (Y_i - \tilde{Y}_i)^2}$$

We investigate the impact of the jammer's transmission range and the jammer's position, respectively.

2) Impact of the Jammer's Transmission Range

First, we consider the impact of the jammer's transmission range on the accuracy of the proposed scheme with a transmission range of 30 feet, 45 feet and 60 feet. Each algorithm is executed 10 times to obtain the estimated position of the jammer. Figure 5 shows the performance of 4 different localization algorithms in the scenario where 200 nodes are randomly distributed among the network. In general, CJ algorithm achieves the best localization accuracy, while CL performs worst in all cases. Furthermore, as the jammer's transmission range increases, the localization error becomes smaller, which indicates that all the algorithms are sensitive to the transmission range. The reason of this behavior is that when the jammer's transmission range becomes larger, more nodes in sensor networks will be blocked, which in turn leads to a larger number of nodes engaging into the estimation process of the jammer's position.



(a) Different Jammer Location (b) Impact of Jammer's Location on Localization error

Fig.6. Impact of Jammer's location on localization error when the transmission range is 45 feet

3) Impact of the Jammer's Position

As shown in figure 6(a), the jammer can be placed at any position. In our experiment, we place the jammer in three different regions: in the center of the network, at one of the corners and at the edge of the network. All the algorithms are sensitive to the change of the jammer's location. As figure 6(b) shows, when the location of the jammer changes from the center of the network to the edge or to the corner of the network, the localization error becomes larger. In general, ***CJ*** and VFIL outperform WCL and CL. The main reason of this result is that the boundary nodes play more important role in the process of estimation in ***CJ*** and VFIL than that in WCL and CL.

VI. CONCLUSION

In this paper, a jammer localization scheme ***CJ*** is proposed. ***CJ*** combines two computational geometric problems, namely the convex hull construction and the minimum covering circle. We proved the correctness of ***CJ***, and verified its efficiency through simulation. ***CJ*** can be adopted into localizing multiple jammers if different jammed regions (circle) incurred by different jammers are disjoint. We will study the more sophisticated scenario as future work. We also plan to exploit the feasibility to adapt our scheme into more sophisticated jamming attack models where the jammed region is not considered as a circular.

REFERENCES

[1] Mario Strasser, Christina. P, Srdjan Capkun, and Mario Cagalj. "Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping". In Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP '08). IEEE Computer Society, Washington, DC, USA, 64-78

[2] Liu. Y, Peng Ning, Huaiyu Dai, and An Liu. "Randomized differential DSSS: jamming-resistant wireless broadcast communication". In Proceedings of the 29th conference on Information communications (INFOCOM'10). IEEE Press, Piscataway, NJ, USA, 695-703.

[3] W. Xu, W. Trappe, Y. Zhang, and T.Wood. "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", ACM MobiHoc.2005. pp: 46-57

[4] M. Cagalj, S. Capkun, and J. P. Hubaux. "Wormhole-Based Anti-jamming Techniques in Sensor Network". IEEE TRANSACTIONS ON MOBILE COMPUTING, 2007, January. VOL. 6, NO. 1

[5] W. Xu, W. Trappe, and Y. Zhang. "Channel Surfing: Defending Wireless Sensor Networks from Interference. IPSN'07, April 2007. pp 499-508

[6] W. Xu, W. Trappe and Y.Zhang. "Anti-jamming Timing Channels for Wireless Networks. ACM WiSec'08. pp 203-213

[7] H. Liu, W. Xu, Y. Chen, and Z. Liu. "Localizing Jammers in Wireless Networks.In Proceedings of IEEE Percom. Texas. March 2009

[8] A. Savvides, C. C. Han, and M. B. Srivastava. "Dynamic fine-grained localization in ad-hoc networks of sensors". ACM MobiCom, 2001.

[9] A. D. Wood, J. A. Stankovic, and S. H. Son. "JAM: A Jammed-Area Mapping Service for Sensor Networks, Proc. 24th IEEE International Real-Time System Symposium. 2003. pp: 286-297

[10] Y. E. Sagduyu, R. Berry and A. Ephremides. "Jamming Games for Power Controlled Medium Access with Dynamic Traffic". In Proc. of IEEE International Symposium on Information Theory (ISIT), Austin, TX, June 2010

[11] Pelechrinis K, Koutsopoulos I, Broustis I. Lightweight jammer localization in wireless networks: system design and implementation. In: Proc. of the Globecom 2009. Hilton Hawallan Village, USA, 2009: 204-208

[12] Liu Z, Liu H, Xu W, Chen Y. Wireless jammer localization by exploiting nodes' hearing ranges. In Proc. of the DCOSS'2010. LNCS, Vol. 6131/2010: 348-361. DOI: 10.1007/978-3-642-13651-1_25

[13] J. Blumenthal, R. Grossmann, F. Golatowski, and D. Timmermann. "Weighted centroid localization in zigbee-based sensor networks. In Proceedings of the IEEE International Symposium on Intelligent Signal Processing, WISP 2007. pp 1-6

[14] Cormen, Thomas H, Leiserson, Charles E, Rivest, Ronald L and Stein, Clifford (2001). Introduction to Algorithms (2nd ed.). MIT Press and McGraw-Hill. ISBN 0-262-53196-8