CrowdLoc: Wireless Jammer Localization with Crowdsourcing Measurements

Yanqiang Sun, Xiaodong Wang
Depart. of Computer Science
National University of Defense Technology
Changsha, 410073, China
{yq_sun, xdwang}@nudt.edu.cn

Melek Önen, Refik Molva
Depart. of Networking and Security
Institute Eurecom
Sophia Antipolis, 06904, France
{melek.onen, refik.molva}@eurecom.fr

ABSTRACT
Jamming attacks can severely affect the performance of wireless networks due to the broadcast nature. The most reliable solution to reduce the impact of such attacks is to detect and localize the jammer. In this paper, we propose our research into participatory sensing based scheme, named as ***CrowdLoc***, for the collection of measurements to collaboratively localize a jammer in wireless ubiquitous environments which are suffering from jamming attacks. ***CrowdLoc*** mainly contains three phases: 1) *Crowds as Sensor*. The sensor nodes at the boundary of jammer region are weakly impacted by the jamming attack, and conduct the sensing functions to record the information related to the jammer, such as received signal strength (RSS); 2) *Crowds as Network*. These boundary nodes cooperate with each other to share the recorded measurements of the jammer; and 3) *Crowds as Estimator*. Based on the crowdsourcing measurements of the jammer, we propose a novel localization scheme to estimate the position of the jammer: Range-based Jammer Localization (RJL). As opposed to existing solutions, RJL is independent of the propagation parameters, which are difficult to obtain in hostile jamming circumstance. The experimental results indicate that the localization accuracy of RJL is close to the Cramer-Rao Bound (CRB) for the RSS-based Localization in most area.

Author Keywords
Wireless network, jamming attack, jammer localization, crowdsourcing, RSS, linearization.

ACM Classification Keywords
C. Computer Systems Organization, C.2 Computer-Communication Networks, C.2.m Miscellaneous.

General Terms
Algorithm, design, security, performance

UbiCrowd'11, September 18, 2011, Beijing, China.

INTRODUCTION
Wireless networks, such as 802.11-based *WiFi* networks and 802.5.4-based sensor networks, are vulnerable to radio interference attacks due to their broadcast nature. Such attacks, also known as jamming attacks, can easily be launched by the malicious users 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]; Some 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 jamming detection and prevention, the issue of determining the jammer's physical position, known as 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 avoid wasting resources due to failed packet delivery.

In this paper, we focus on the omni-directional-antenna jammer localization. A participatory sensing based jammer localization scheme, which is named as ***CrowdLoc***, is proposed. ***CrowdLoc*** mainly consists of three phases: 1) *Crowds as Sensor*. The meaning of sensor here may be the users in mobile ad hoc networks, the sensing nodes in sensor networks, or even the mobile-phone-individuals in urban areas. The sensor nodes at the boundary of jammer region are weakly impacted by the jamming attack, and conduct the sensing functions to record the information related to the jammer, such as received signal strength (RSS); 2) *Crowds as Network*. These boundary nodes cooperate with each other to share the recorded measurements of the jammer; and 3) *Crowds as Estimator*. Based on the crowdsourcing measurements, the estimated position of the jammer is determined. Besides the application of crowdsourcing, we further design a Range-based Jammer Localization (RJL) which is independent of the propagation parameters. The experimental results

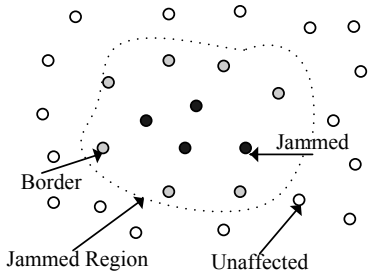
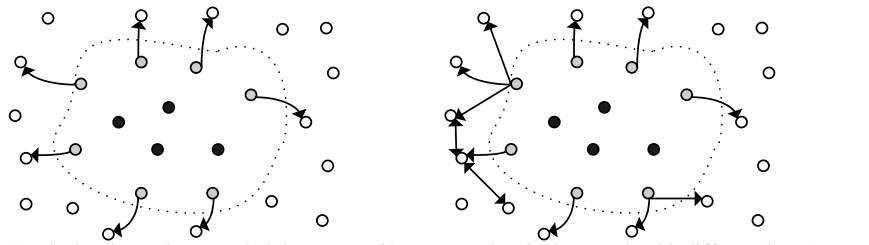


Fig 1. Jamming Scenario



(a) The border nodes recorded the RSS measurements and then broadcast

(b) Every node who has received k different(k>=4) RSS measurements can estimate the position of the jammer

Fig 2. Crowds as Sensor & Networks

indicate that the localization accuracy of RJL is close to the Cramer-Rao Bound (CRB) [11] for the RSS-based Localization in most area.

We first introduce the related work in brief, and then propose our jammer localization mechanism.

RELATED WORK

Liu et al. [7] introduced a scheme called Virtual Forces Iterative Localization (VFIL), which takes 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. Centroid Localization (CL) [13] uses position information of all neighboring nodes, which are located within the transmission range of the targeted node. And the centroid of these nodes is treated as the estimated position of the jammer. However, CL is highly sensitive to the varying of referred sensing nodes' position and the location of the jammer.

Logan Scott proposed a J911 system [8] to detect and localize the jammer incorporating GPS jam-to-noise ratio, which is the first work relying on crowdsourcing in jammer localization. Liu et al. [9] proposed a least-square jammer localization scheme by exploiting hearing range. Unfortunately, these solutions heavily depend on the knowledge of the radio propagation information such as transmitting power (TP) and the path loss exponent (λ). Although Krishna et al. [3] developed a general indoor localization scheme without the prior knowledge of TP and λ, yet it still involves iterative estimation of both parameters based on the measurements. In the sequel of this paper, we will show that ***CrowdLoc*** does not rely on additional devices (GPS, infrared devices, etc.), and is independent of the main propagation parameters (TP and λ) as well.

CROWDLOC DESIGN

Overview

Since it is very difficult, even sometimes unrealistic, to obtain accurate propagation parameters about the jammer, we aim at designing a RSS-based jammer localization scheme without depending on the radio propagation parameters, including transmitting power (TP) and path loss exponent (λ). As a first step, a relationship between the distance from a jammer to a sensing node and the RSS is established with the widely used log-distance path loss model [4]. Since this highly depends on the transmitting power and the path loss exponent, a linear approximation of this relationship is applied to generate independency with respect to TP and λ. Once this linearization equation is defined, crowdsourcing nodes collaborate with each other in order to be able to resolve a linear system of k (k is the number of sensing nodes) independent equations, and finally determine an estimated value of the jammer's position

Crowds as Sensor

This is the first phase of ***CrowdLoc***. Under jamming attack, the network nodes can be divided into three categories: unaffected nodes, border nodes and jammed nodes as shown in figure 1. Here we choose the border nodes as the crowds for the RSS measurements of the jammer. The rationale is that the border nodes suffer from jamming attack, yet still satisfy the demanding SINR (Signal to Interference and Noise Ratio), i.e., the border nodes can still transmit packets [9] [13].

Crowds as Network

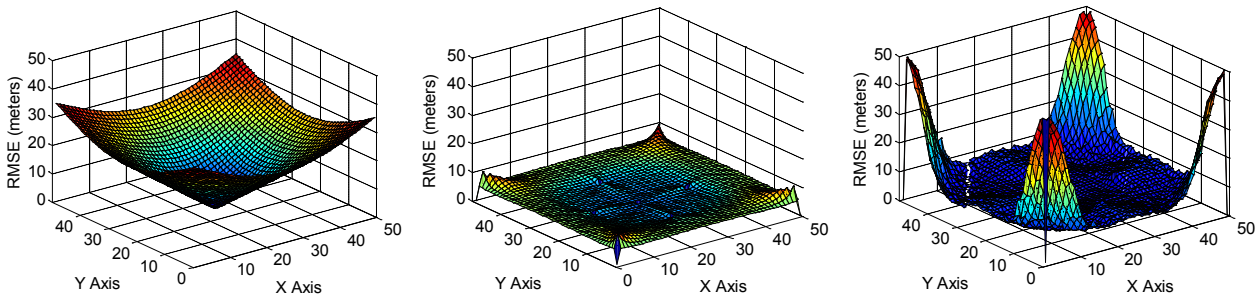
After recording the RSS measurements from the jammer, the border nodes begin to share this information with their neighbors as shown in figure 2. In the next section, we will show that every node who has received k different ($k \geq 4$) RSS measurements is able to estimate the possible position of the jammer by resolving a system of linear equations.

Crowds as Estimator

In the estimation phase, the first step of the proposed localization scheme is to establish a relationship between the distance to a jammer and the RSS information, using the widely adopted log-distance path loss model [11]. Formally, the estimated distance between the jammer and the sensing node is defined by the following equation:

$$d_i = 10^{(-r_i + PL_R + X_g)/10\lambda} \cdot d_R \qquad (1)$$

Here, r_i refers to the recorded RSS value at the ith sensing node, PL_R is the path loss at the reference distance d_R, and λ is the path loss exponent. X_g is a normal random variable with zero mean, reflecting the attenuation caused



(a)Centroid (b) CRB for RSS-based localization (c) ***CrowdLoc***

Fig.3 Performance Evaluation of Centroid， CRB and *CrowdLoc*

by flat fading. d_i refers to the estimated distance between the jammer and the *i*th sensing node, and is defined as follows:

$$d_i \cong \sqrt{(x_0 - x_i)^2 + (y_0 - y_i)^2} \quad (2)$$

where (x_0, y_0) and (x_i, y_i) are positions of the jammer and the *i*th sensing node, respectively.

Since this distance depends on unknown parameters, namely PL_R and λ, we propose to evaluate an approximation value of the distance by using the following well-known linear approximation:

$$10^x \cong \omega_0 + \omega_1 \cdot x \quad (3)$$

where ω_0 and ω_1 are the linear coefficients. In equation (1), x can be defined as

$$x = (-r_i + PL_R + X_g)/10\lambda\,, \quad (4)$$

Thus,

$$d_i \cong (\omega_0 + \omega_1 \cdot x) d_R\,. \quad (5)$$

By using this linearization technique, unknown parameters such as PL_R and λ, will not be needed for the second step where sensing nodes resolve a system of k independency equations. It is necessary to notice that the linearization accuracy has no impact on estimation process, which is proved in the remaining part.

Indeed, by combing equation (2) to (5) we obtain:

$$(x_0 - x_i)^2 + (y_0 - y_i)^2 \cong (\omega_0 + \omega_1 \cdot \frac{-r_i + PL_R + X_g}{5}) \cdot d_R^2 \quad (6)$$

Typically, d_R is set to 1 meter. During the second step of the proposed localization solution, sensing nodes collaborate with each other with the help of crowdsourcing techniques and hence build the following system of k equations (7):

$$\begin{cases} (x_0 - x_1)^2 + (y_0 - y_1)^2 = (\omega_0 + \omega_1 \cdot \dfrac{-r_1 + PL_R + X_g}{5}) \\ (x_0 - x_2)^2 + (y_0 - y_2)^2 = (\omega_0 + \omega_1 \cdot \dfrac{-r_2 + PL_R + X_g}{5}) \\ \quad \vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \\ (x_0 - x_k)^2 + (y_0 - y_k)^2 = (\omega_0 + \omega_1 \cdot \dfrac{-r_k + PL_R + X_g}{5}) \end{cases} \quad (7)$$

From the system of equations (7), we are able to obtain a linear system of x_0 and y_0 by subtracting the kth equation from the ith (i={1, 2, ..., k-1}) equation as shown in equation (8):

$$\begin{bmatrix} -x_1^2 - y_1^2 + x_k^2 + y_k^2 \\ -x_2^2 - y_2^2 + x_k^2 + y_k^2 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ -x_{k-1}^2 - y_{k-1}^2 + x_k^2 + y_k^2 \end{bmatrix} = \begin{bmatrix} -2x_1 + 2x_k & -2y_1 + 2y_k & \omega_1(r_1 - r_k)/5 \\ -2x_2 + 2x_k & -2y_2 + 2y_k & \omega_1(r_2 - r_k)/5 \\ \vdots & \vdots & \vdots \\ -2x_{k-1} + 2x_k & -2y_{k-1} + 2y_k & \omega_1(r_{k-1} - r_k)/5 \end{bmatrix} \begin{bmatrix} x_0 \\ y_0 \\ 1/\lambda \end{bmatrix} \quad (8)$$

The equation (8) can be denoted as $\beta = A\alpha$, and the being-estimated values of x_0 and y_0 only depend on the location of sensing nodes, the RSS value and the linear approximation coefficient ω_1. Hence, the jammer localization process does not rely on the radio propagation parameters (PL_R, λ) anymore. Only four or more RSS values from different sensing nodes are needed. More surprisingly, besides ω_0, we discover that the linear coefficient ω_1 does not have an impact on localization performance either. Assuming that we have four sensing nodes for jammer localization, then A is a 3x3 matrix in equation (8), and α equals $A^{-1}\beta$. $A^{-1} = adj(A)/det(A)$, and $det(A) = \omega_1 f_1(x, y, r)$, f_1 is linear functions of x, y, and r. Through simple deduction, the $adj(A)$ can be expressed by $\omega_1 A'$, where A' is a 3x3 matrix of which the first and second rows are independent of ω_1. So ω_1 does not affect the value of x_0 and y_0. That is, the linearization accuracy has no impact on estimation process.

We did not prove the higher-order matrix case when more than four nodes are involved. However, our experimental results in the next section indicate that the linear coefficients have no impact on localization accuracy even when the number of sensing nodes is larger than four.

PRELIMINARY EXPERIMENTAL RESULTS

We evaluated the feasibility and efficiency of our proposed scheme through simulation. In the circumstance setting, the network area is 50m x 50m square. RSSs are generated by

the log-distance path loss model. Five fixed referred sensing nodes (The coordinates are (1, 1), (1, 50), (50, 1), (50, 50), (25, 25), respectively) are involved into the process of jammer's location estimation, which was conducted in every meter grids. The root-mean-square error (RMSE) is used for the measure of differences between the estimated position and actual location of the jammer.

As Fig.3 shows, we compared our scheme with two representative algorithms. Centroid [12], which is a typical range-free localization method that is independent of the wireless propagation model, is highly sensitive to the varying of referred sensing nodes' position and the location of the jammer as shown in Fig.3.(a). The RMSE of Cramer-Rao Bound (CRB) [11] for RSS-based localization provides the accuracy bound of location estimation with RSS measurements. Fig.3.(b) illustrates this bound where PL_R was set to be -25dBm, and the path loss exponent λ was set to 4. Fig.3.(c) shows the performance of our proposed solution. In most of the simulated area, the localization error (RMSE) is close to the CRB, except at the corners. This is because of the poor geometric condition which is defined as the sum of areas of all triangles composed by a jammer and any set of two referred sensing nodes [11].

The impact of parameters are also investigated, including the transmitting power PL_R, the exponent λ, the number of sensing nodes, and the coefficient ω_1. Table 1 shows a fraction of simulation results. From these results, we observed that both PL_R and ω_1 have no impact on localization performance. The larger λ, the lower localization error, which further verifies the theoretical analysis mentioned in [11]. Localization error of our proposed scheme decreases as the number of referred sensing nodes increases.

CHANLLENGES & FUTURE WORK

The crowds as network

In this paper, we only consider the more simple case of RSS measurements sharing (broadcast). However, the way how to reduce the message overhead and protect the security and privacy of the users is still needed to be investigated. A reliable transmission protocol must be designed.

The higher-order matrix case

We verified the independency of ω_1 on the impact of localization accuracy in higher order matrix through simulation. In the future work, we need to prove the independency of ω_1 in all cases theoretically.

Conducting real experiments

The real network experiments have to be conducted to verify the efficiency of the proposed scheme.

ACKNOWLEDGEMENT

This work was partially done when Yanqiang Sun visited Eurecom, and was 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.

No. of sensing nodes	λ=2 ω_1=25 PL_R= -25	λ=4 ω_1=25 PL_R= -25	λ=4 ω_1=25 PL_R= -40	λ=4 ω_1=12 PL_R= -25
4	21.36	18.66	18.66	18.66
6	19.05	16.73	16.73	16.73
9	18.42	15.91	15.91	15.91

Tab 1. The impact of parameters (RMSE, in meters)

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. In *Proceedig of 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. In *Proceeding of IPSN'07*, April 2007. pp 499-508.

6.W. Xu, W. Trappe and Y.Zhang. Anti-jamming Timing Channels for Wireless Networks. In *Proceedings of 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'09*. Texas. March 2009.

8.Logan Scott. *J911: Fast JammerDetection and Location using Cell-Phone Crowd-Sourcing*. GPS World. Nov. 2010

9.Liu. Z, Liu. H, Xu.WY, and Chen. YY. Exploiting Jamming-Caused Neighbor Changes for Jammer Localization. *IEEE Transaction on Parallel and Distributed Systems*. 2011

10.Krishna. C, Anand. P.I, and Venkata. N.P. Indoor Localization without the pain. In *Proc. MobiCom'10*, ACM, New Your, NY, USA. 173-184

11.N. Ptwari, A. Hero, M. Pekins, N. S. Correal, and R. Dea. Relative location estimation in wireless sensor networks. *IEEE Trans. Signal Process*. 2003

12.J. Blumenthal, R. Grossmann, F. Golatowski, and D. Timmermann. Weighted centroid localization in zigbee-based sensor networks. In *Proc. WISP 2007*. pp 1-6.

13. Sun, Y.Q., Molva, R., Önen, M. and Wang, X.D. Catch the Jammer in Wireless Sensor Network. In *Proc. PIMRC'11*, IEEE Computer Society, Sep. 11-14.