International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Effective Approach for Localizing Jammers in Wireless Sensor Network

Ashwini S. Chimankar[1], V. S. Nandedkar[2]

[1]PVPIT, Bavdhan, Pune, Savitribai Phule Pune University, India

[2]Professor, HOD (Information Technology) PVPIT, Bavdhan, Pune, Savitribai Phule, Pune University, India

Abstract: ***The communication in wireless network can be disrupted by jammers in the network. Jammers' position information allows the defender to actively eliminate the jamming attacks. In this paper, our aim is to design a framework that localizes one or multiple jammers with a high accuracy. Almost all of existing jammer-localization methods utilize indirect measurements (i.e. hearing ranges) affected by jamming attacks which does not localize jammers accurately. We use a direct measurement technique–the strength of jamming signals (JSS). Estimating JSS is challenging as jamming signals may be embedded in other signals. We used estimation scheme based on ambient noise floor. To further reduce estimation errors, we define an evaluation feedback metric to quantify the estimation errors and formulate jammer localization as a non-linear optimization problem, whose global optimal solution is close to jammers' true positions. Our simulation results show that our error-minimizing-based framework achieves better performance than the existing schemes .In this paper we took the average jammer location obtained by centroids based method and JSS based direct measurement technique. In addition to existing work, our error minimizing framework utilizes indirect measurements to obtain a better location estimation compared with prior work.***

Keywords: Localization, Jamming, Radio Interference, Strength of jamming signals

1. Introduction

Localizing jammers is very crucial task in wireless sensor network. The locations of jammers allow a better physical arrangement of wireless devices that cause unintentional radio interference, or enable a wide range of defense strategies for combating malicious jamming attackers. To overcome these challenges and increase the localization accuracy, we formulate the jammer localization problem as a non-linear optimization problem and define an evaluation metric as its objective function. The value of evaluation metric reflects how close the estimated jammers' locations are to their true locations, and thus we can search for the best estimations that minimize the evaluation metric. Because traditional gradient search methods may converge to a local minimum and may not necessarily yield the global minimum, we adopt several algorithms that involve stochastic processes to approach the global optimum..

This paper is organized as follows: section II consists of literature survey of existing work with comparisons. Some background details and formulation is given in section III. Section IV describes threat model. The localization formulation is described in Section V. Section VI describes our system and mathematical model. Section VII gives conclusion and Section VIII describes references.

2. Literature Survey

Methods used for localizing jammers in wireless sensor netwok are as follows:

A. Double Circle Localization

This algorithm is used to find the location of jammers in wireless networks. It uses two methods - Minimum bounding circle (MBC)[] and Maximum inscribed circle (MIC). It is implemented under different conditions including different node densities, jammers transmission power and antenna orientation. But this method deals with localizing a single jammer so this not sufficient because in a huge wireless network there will be need for localizing multiple jammers.

B. M Cluster Method

M-cluster method is used to localize single or multiple jammers which overcomes problem of double localization method. The M-cluster algorithm is based on the grouping of jammed nodes with a clustering algorithm, and each jammed-node group is used to estimate one jammer location. M-cluster algorithm, we consider the falsely covered boundary nodes and calibrate the result in a similar way. Second, we discover that when many bifurcation points belong to one jammer, the clustering technique may falsely divide them into two clusters, resulting in two jammers. This method is not efficient because it provide less accuracy for localizing jammers.

C. X-ray algorithm

The X-ray algorithm relies on the skeletonization of a jammed area, and uses the bifurcation points on the skeleton to localize jammers. In M-clustering algorithm it considers the falsely covered boundary nodes and calibrate the result in a similar way. Second we discover that when many bifurcation points belong to one jammer, the clustering technique may falsely divide them into two clusters, resulting in two jammers.

But in X-ray algorithm this error is discovered by using a filter that measures the distance between two estimated jammers.In literature new framework is proposed for localizing the jammers in wireless sensor network because the above given methods provide less accuracy in localizing jammers (1)Error mimimizing framework-

This framework includes three algorithms (a) a genetic algorithm (b) a generalized pattern search algorithm (c) a simulated annealing algorithm.This algorithms not only improve the estimation accuracy of localizing one jammer compared to prior work but also can estimate the positions of multiple jammers simultaneously, making it especially useful for identifying unintentional radio interference caused by multiple wireless devices or a few malicious and collaborative jammers.This methods provide the better result to locate the jammer in wireless network.

3. Problem Formulation

Given the definition of the feedback metric (ez), we generalize jammer localization problem as one optimization problem,

Problem :
Minimize **z**
e_z(**z**, **p**)
subject to **p** = {Pr_1, . . . , Pr_m};
where **z** are the unknown variable matrix of the jammer(s), e.g., **z** is defined as

$$\mathbf{z} = \begin{pmatrix} \hat{x}_{J_1} & \hat{y}_{J_1} & \hat{P}_{J_1} + \hat{K}_1 \\ \hat{x}_{J_2} & \hat{y}_{J_2} & \hat{P}_{J_2} + \hat{K}_2 \\ \vdots & \vdots & \vdots \\ \hat{x}_{J_n} & \hat{y}_{J_n} & \hat{P}_{J_n} + \hat{K}_n \end{pmatrix}$$

and {Pri}i∈[1,m] are the JSS measured at the boundary nodes {1, . . .,m}.
The estimated location(s) of the jammer(s) at which ez is minimized, matches the true location(s) of jammer(s) with small estimation error(s).

4. Threat Model

There are many attacking strategies, but we mainly focus on one common type of jammer –constant jammers**.** Constant jammers continually emit radio signals, regardless of whether the channel is idle or not .Such jammers can be unintentional radio interferers that are always active or malicious jammers that keep disturbing network communication .In proposed work the network nodes based on the level of disturbance caused by jammers, and identify the nodes that can participate in jammer localization, e.g., the ones that can measure and report the JSS. Essentially, the communication range changes caused by jamming are reflected by the changes of neighbors at the network topology level. Thus, the network nodes could be classified based on the changes of neighbors caused by jamming. We define that node B is a neighbor of node A if A can communicate with B prior to jamming. The network nodes can be classified into three categories according to the impact of jamming: *unaffected node*, *jammed node*, and *boundary node*.

1) **Unaffected node:** A node is unaffected if it can communicate with all of its neighbors. This type of node is barely affected by jamming and may not yield accurate JSS measurements.
2) **Jammed node:** A node is jammed if it cannot communicate with any of the unaffected nodes .We note that this type of node can measure JSS, but cannot always report their measurements.
3) **Boundary node:** A boundary node can communicate with part of its neighbors but not from all of its neighbors. Boundary nodes can not only measure the JSS, but also report their measurements to a designated node for jamming localization.

algorithm1: Jammer Localization Framework.

p = MeasureJSS()
z = Initial positions
whileTerminating Condition True **do**
e_z =EvaluateMetric(**z**, **p**)
ifNotSatisfy(e_z) **then**
z = SearchForBetter()
end if
end while
$Mine_z$= e_z
(x_j,y_j)=GetEstJammer(z);
(x_{jammer},y_{jammer}) = GetCentroid();
(x_{est},y_{est}) = Average(x_j,y_j,x_{jammer},y_{jammer});

5. Localization Formulation

Our jammer localization approach works as follows. Given a set of JSS, for every estimatedlocation, we are able to provide a quantitative evaluation feedback indicating the distance between the estimated locations of jammers and their true locations. For example, a small value of evaluation feedback indicates that estimated locations are close to the true ones, and vice versa. Although unable to adjust the estimation directly, it is possible, from a few candidate locations, to select the ones that are closest to the true locations with high probability, making searching for the best estimate feasible. Leveraging this idea,our jammer localization approach comprises two steps:

(a) ***JSS Collection:***Each boundary node locally obtains JSS.
(b) ***Best-Estimation Searching:***Based on the collected JSS, a designated node will obtain arough estimation of the jammers' positions. Then, it refines the estimation by searching for positions that minimize the evaluation feedback metric. The details are described in Algorithm 1. The search-based jammer localization approaches have a few challenging subtasks.

1) EvaluateMetric() has to define an appropriate metric to quantify the accuracy of estimatedjammers' locations.
2) MeasureJSS() has to obtain JSS even if it may be embedded in regular transmission.
3) SearchForBetter() has to efficiently search for the best estimation. In this section, we focus on formulating the evaluation feedback metric using collected JSS measurements. In particular, we model the jammer localization as an optimization problem.

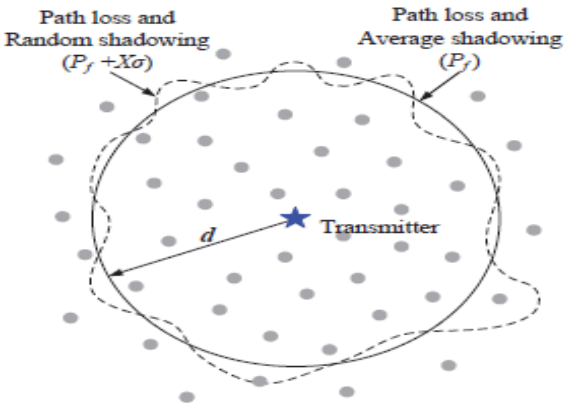

Figure 1: The contour of RSS subject to path loss is a circle centered at the transmitter, and the contour of RSS attenuated by both path loss and shadowing is an irregular loop.

5.1 Radio Propagation Basics

In wireless communication, the received signal strength attenuates with the increase of distance between the sender and receiver due to path loss and shadowing, as well as constructive and destructive addition of multipath signal components.Path loss can be considered as the *average* attenuation while shadowing is the *random* attenuation caused by obstaclesthrough absorption, reflections, scattering, and diffraction. Following Figure illustrates contours of received signal strength and the relationship between shadowing and path loss. The attenuation caused by shadowing at any single location, d meters from the transmitter, may exhibit variation; the average. Attenuation and average signal strength on the circlecentered at the transmitter are roughly the same .This observation serves as the fundamental basis of our error minimizing framework.

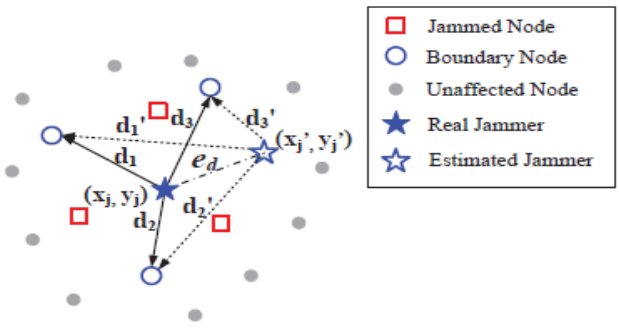

Figure 2: Illustration of jammer localization basis. When the estimated jammer location is ed meters from the true location, the estimated random attenuation is biased and the corresponding standard deviation is larger than the real one.

To illustrate our jammer localization approach, we use the widely-used log-normal shadowing model which captures the essential of both path loss and shadowing. Let P_f be the received signal strength subject to path loss attenuation only, and let the power of a transmitted signal be P_t. **The received signal power (Pr)** in dBm at a distance of d can be modeled as the sum of P_f and a variance (denoted by Xσ) caused by shadowing and other random attenuation,

$$Pr = Pf + X\sigma \quad (1)$$
$$Pf = Pt + K - 10\eta \log10(d), \quad (2)$$

WhereXσ is a Gaussian zero-mean random variable with standard deviation σ, K is a unitless constant which depends on the antenna characteristics and the average channel attenuation, and η is the Path Loss Exponent (PLE). In a free space, η is 2 and Xσ is always 0.

5.2Localization Evaluation Metric

We show the property of ez as well as its calculation.

5.2.1The property of e_z

The definition of e_z should have the following property: The larger the estimation errors of jammers' locations are, the larger ez is. We define ez as the estimated standard deviation of Xσ derived from the estimated jammers' locations. Considering the one jammer case, when the estimated jammer's location equals the true value, ez is the real standard deviation of Xσ, which is relatively small. When there is an estimation error (the estimated location is ed distance away from the true location), ez will be biased and will be larger than the real standard deviation of Xσ. The level of bias is affected by ed: the larger ed is, the bigger the estimated standard deviation of Xσ will likely be.

5.2.2 Calculation

1) Single Jammer: Assume a jammer J located at (x_J, y_J) starts to transmit at the power level of P_J, and m nodes located at {(xi, yi)}i∈[1,m] become boundary nodes. To calculate ez, each boundary node will first measure JSS locally, and we denote the JSS *measured* at boundary node i as Pr_i . Let the current estimation of the jammer J's location and the transmission power be-

$$\hat{z} = [\hat{x}_J, \hat{y}_J, \hat{P}_J + \hat{K}]$$

Algorithm 2 Evaluation feedback metric calculation.

1: **procedure** EVALUATEMETRIC($\hat{z}$, p)
2: **for all** $i \in [1, m]$ **do**
3: $\hat{X}_{\sigma_i} = P_{r_i} - P_{f_i}(\hat{z})$
4: **end for**
5: $e_z = \sqrt{\frac{1}{m}\sum_{i=1}^{m}(\hat{X}_{\sigma_i} - \hat{\bar{X}}_{\sigma})^2}$
6: **end procedure**

Given ˆ**z**, we can estimate Pf_i , the JSS subject to path loss only at boundary node i as

$$P_{f_i}(\hat{d}_i) = \hat{P}_J + \hat{K} - 10\eta \log_{10}(\hat{d}_i)$$
$$\hat{d}_i(\hat{\mathbf{z}}) = \sqrt{(\hat{x}_J - x_i)^2 + (\hat{y}_J - y_i)^2}$$

The random attenuation (shadowing) between the jammer J and boundary node i can be estimated as

$$\hat{X}_{\sigma_i} = P_{r_i} - P_{f_i}(\hat{d}_i)$$

The evaluation feedback metric for the estimation ˆ**z** is the standard deviation of estimated { ˆXσi}i∈[1,m],

$$e_z(\hat{\mathbf{z}}, \mathbf{p}) = \sqrt{\frac{1}{m}\sum_{i=1}^{m}(\hat{X}_{\sigma_i} - \hat{\bar{X}}_{\sigma})^2},$$

where ˆ¯Xσ is the mean of ˆXσi . One of the biggest advantages of this definition is that by subtracting ¯Xσ, ez is only affected by (ˆxJ , ˆyJ) and is independent of the estimated jamming power ˆ P_J + ˆK

2) Multiple Jammers:-

Similar to single jammer, we assume n jammers located at {(xJi, yJi)}i∈[1,n] start to transmit at the power level of {PJi}i∈[1,n] separately at the same time, and m nodes located at {(xi, yi)}i∈[1,m] become boundary nodes. To calculate ez, each boundary node measures JSS locally and we denote the JSS *measured* at boundary node i as Pri which is a combined JSS from multiple jammers .We can include all the variables to be estimated, i.e., current estimation of the n jammers' locations and the transmission powers, in a form of matrix written as

$$\mathbf{z} = \begin{pmatrix} \hat{x}_{J_1} & \hat{y}_{J_1} & \hat{P}_{J_1} + \hat{K}_1 \\ \hat{x}_{J_2} & \hat{y}_{J_2} & \hat{P}_{J_2} + \hat{K}_2 \\ \vdots & \vdots & \vdots \\ \hat{x}_{J_n} & \hat{y}_{J_n} & \hat{P}_{J_n} + \hat{K}_n \end{pmatrix}$$

In the case of multiple jammers, Pf_i is the combined JSS from n jammers subject to path loss at a boundary node and can be calculated as

$$P_{f_i}(\hat{\mathbf{z}}) = 10\log_{10}\left(\sum_{j=1}^{n}\frac{10^{\frac{\hat{P}_{J_j}+\hat{K}_j}{10}}}{\hat{d}_{ji}^{\eta}}\right)$$

$$\hat{d}_{ji} = \sqrt{(\hat{x}_{J_j} - x_i)^2 + (\hat{y}_{J_j} - y_i)^2}$$

Where ˆ dji is the estimated distance between jammer j and boundary node i. Note that ˆ PJj , ˆK and Pfi are all in dBm.

Algorithm 3 Acquiring the Ambient Noise Floor (ANF). ANF approximates the strength of jamming signals.

```
1: procedure MEASUREJSS
2:     s = {s_1, s_2, ..., s_n} = MeasureRSS()
3:     if var(s) < varianceThresh then
4:         s_a = s
5:     else
6:         JssThresh = min(s) + α[max(s) − min(s)]  ▷ α ∈ [0, 1]
7:         s_a = {s_i | s_i < JssThresh, s_i ∈ s}
8:     end if
9:     return mean(s_a)
10: end procedure
```

A naive approach of estimating the ANF could be sampling ambient noise when the wireless radio is idle (i.e., neither receiving nor transmitting packets).Such a method may not work in all network scenarios, since it may result in an overestimated ANF. For example, in a highly congested network, collision is likely to occur, and the collided signals may be treated as part of the ANF at the receiver, resulting

Then, the random attenuation between multiple jammers and the boundary node i can be estimated as

$$X_{\sigma_i} = P_{r_i} - P_{f_i}(\hat{\mathbf{z}}),$$

Thus, the evaluation feedback metric of ˆ**z** is

$$e_z(\mathbf{z}, \mathbf{p}) = \sqrt{\frac{1}{m}\sum_{i=1}^{m}(\hat{X}_{\sigma_i} - \hat{X}_{\sigma})^2}.$$

Where$\hat{X}$σ is the mean of ˆ$X\sigma_i$.

6. Measuring Jamming Signals

Received signal strength (RSS) is one of the most widely used measurements in localization. For instance ,a Wi Fi device can estimate its most likely location by matching the measured RSS vector of a set of Wi Fi APs with pre-trained RF finger printing maps [10] or with predicted RSS maps constructed based on RF propagation models [11]. However, obtaining signal strength of jammers (JSS) is a challenging task mainly because jamming signals are embedded in signals transmitted by regular wireless devices .The situation is complicated because multiple wireless devices are likely to send packets at the same time, as jamming disturbs the regular operation of carrier sensing multiple access (CSMA). For the rest of this paper, we refer the regular nodes' concurrent packet transmissions that could not be decoded as a collision .While it is difficult, if ever possible, to extract signal components contributed by jammers or collision sources, we discover that it is feasible to derive the JSS based on periodic ambient noise measurement. In the following subsections, we first present basics of ambient noise with regard to jamming signals, and then introduce our scheme to estimate the JSS. Finally, we validate our estimation schemes via real-world experiments.

6.1. Basics of Ambient Noise Floor

In theory, *ambient noise* is the sum of all unwanted signals that are always *present*, and the ambient noise floor (ANF) is the measurement of the ambient noise .In the presence of constant jammers, the ambient noise includes thermal noise, atmospheric noise, and jamming signals. Thus, it is

PN = PJ + PW,

where PJ is the JSS, and PW is the white noise comprising thermal noise, atmospheric noise, etc. Realizing that at each boundary node PW is relatively small compared to PJ , the ambient noise floor can be roughly considered as JSS. Thus, estimating JSS is equivalent to deriving the ambient noise floor (ANF) at each boundary node. In this work, we consider the type of wireless devices that are able to sample ambient noise regardless of whether the communication channel is idle or busy, e.g., MicaZ sensor platforms; and derive the ANF based on ambient noise measurements.

in an inflated ANF. This is exactly the situation we want to avoid.

6.2Estimating Strength of Jamming Signals

To derive the JSS, our scheme involves sampling ambient noise values regardless of whether the channel is idle or busy. In particular, each node will sample n measurements of ambient noise at a constant rate, an denote them as **s** = [s1, s2,. . ., sn]. The measurement set **s** can be divided into two subsets (**s** = **s**a∪ **s**c).
1) **s**a = {si|si = PJ}, the ambient noise floor set that contains the ambient noise measurements when only jammers are active, and
2) **s**c = {si|si = PJ + PC}, the combined ambient noise set that contains ambient noise measurements when both jamming signals (PJ) and signals from one or more senders (PC) are present. Calculating JSS is equivalent to obtaining the average of ANFs, i.e., mean(**s**a). In most cases, **s**c ≠ ϕ and **s**a⊂ **s**. In a special case where no sender hasever transmitted packets throughout the process of obtaining n measurements, **s**c = ϕand **s**a = **s**. The algorithm for calculating the ANF should be able to cope with both cases. As such, we designed an algorithm (referred as Algorithm 3) as follows:

A regular node will take n measurements of the ambient noise measurements. It will consider the ANF as the average of all measurements if no sender has transmitted during the period of measuring; otherwise, the ANF is the average of **s**a, which can be obtained by filtering out **s**c from **s**. The intuition of differentiating those two cases is that if only jamming signals are present, then the variance of n measurements will be small; otherwise, the ambient noise measurements will vary as different senders happen to transmit. The correctness of the algorithm is supported bythe fact that **s**a is not likely to be empty due to carrier sensing, and the JSS approximately equals to the average of **s**a. The key question is how to obtain **s**a. To do so, we set the upper bound (i.e., JssThresh)of **s**c in Algorithm 3 as α percentage of the amplitude span of ambient noise measurements. We validate the feasibility of obtaining **s**a using a filtering bound in the next experimental subsection.

6.3 Centroid Localization

Centroid Localization [16] is derived from the idea of centroid, which is the geometric center in geometry. CLuses 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 positionof the jammer. Assuming that there are N jammed nodes(X1; Y1); (X2; Y2); :::; (XN; YN), the position of the jammercan be estimated by:

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

6.4 Localizing Jammers by Average

Finall y to localize the jammer with more accuracy we will take the average of (Xj, Yj) with less e_z and (X_{jammer}, Y_{jammer}) calculated by centroids localization. By taking the average of these two values we can localize the jammer with high accuracy.

$$(Xj, Yj) = (\frac{x_{jammer} + x_j}{2}, \frac{y_{jammer} + y_j}{2})$$

7. Conclusion

We designed an error-minimizing-based framework to localize jammers. In particular, we combined the centroids based localization with the existing error minimizing framework. By combining these two methods we can achieve the better result to locate the jammer in wireless network.

References

[1] Geier J,2004,"the state of wireless lans technical support "
[2] Sampigethaya, K., Poovendran, R., and Bushnell, L., "Secure Operation, Control, and Maintenance of Future e-Enabled Airplanes," *Proc. IEEE*, Vol. 96, No. 12, Dec. 2008, pp. 1992–2007
[3] Rongqing Zhang, Lingyang Song, Zhu Han and Bingli Jiao "Physical Layer Security for Two-Way Un trusted Relaying with Friendly Jammers" IEEE 2012 |.
[4] Liu, H., Xu, W., Chen, Y., Liu, Z.: Localizing jammers in wireless networks. In: Proceedings of IEEE PerCom International Workshop on Pervasive Wireless Networking (IEEE PWN) (2009).
[5] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless lansand countermeasures," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7,no. 3, pp. 29–30, 2003\
[6] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise tolerant security mechanisms for wireless sensor networks," Selected Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 247 –260, Feb. 2006
[7] W. Xu, K. Ma, W. Trappe, and Y. Zhang. Jamming sensor networks:attacks and defense strategies. In IEEE Network, 2006.
[8] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.
[9] T. Rappaport, *Wireless Communications- Principles and Practice*. Prentice Hall, 2001.
[10] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proceedings of INFOCOM*, 2000.
[11] J. Yang, Y. Chen, and J. Cheng, "Improving localization accuracy of rss-based lateration methods in indoor environments,"*AHSWN*, vol. 11, no. 3-4, pp. 307–329, 2011. [12] P. V. Laarhoven and E. Aarts, *Simulated Annealing: Theory and Applications*. Springer, 1987.