

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 obstacle through 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 circle centered at the transmitter are roughly the same. This observation serves as the fundamental basis of our error minimizing framework.

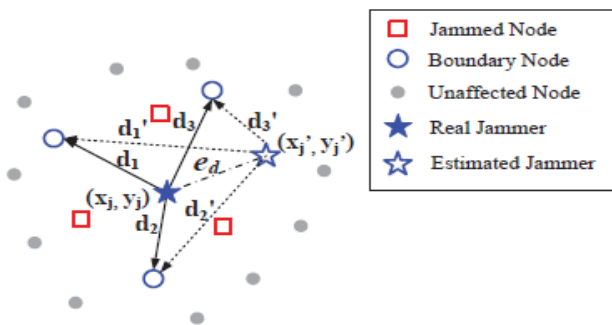


Figure 2: Illustration of jammer localization basis. When the estimated jammer location is e_d meters from the true location, the estimated random attenuation is biased and the corresponding standard deviation is larger than the real one.

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 (P_r)** in dBm at a distance of d can be modeled as the sum of P_f and a variance (denoted by X_σ) caused by shadowing and other random attenuation,

$$P_r = P_f + X_\sigma \quad (1)$$

$$P_f = P_t + K - 10\eta \log_{10}(d), \quad (2)$$

Where X_σ 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 X_σ is always 0.

5.2 Localization Evaluation Metric

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

5.2.1 The 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 e_z is. We define e_z as the estimated standard deviation of X_σ derived from the estimated jammers' locations. Considering the one jammer case, when the estimated jammer's location equals the true value, e_z is the real standard deviation of X_σ , which is relatively small. When there is an estimation error (the estimated location is e_d distance away from the true location), e_z will be biased and will be larger than the real standard deviation of X_σ . The level of bias is affected by e_d : the larger e_d is, the bigger the estimated standard deviation of X_σ 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 $\{(x_i, y_i)\}_{i \in [1, m]}$ become boundary nodes. To calculate e_z , each boundary node will first measure JSS locally, and we denote the JSS *measured* at boundary node i as P_{r_i} . Let the current estimation of the jammer J 's location and the transmission power be-

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

Algorithm 2 Evaluation feedback metric calculation.

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

Given $\hat{\mathbf{z}}$, we can estimate P_{f_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 $\hat{\mathbf{z}}$ is the standard deviation of estimated $\{\hat{X}_{\sigma_i}\}_{i \in [1, m]}$,

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

where \hat{X}_{σ} is the mean of \hat{X}_{σ_i} . One of the biggest advantages of this definition is that by subtracting \hat{X}_{σ} , e_z is only affected by (\hat{x}_J, \hat{y}_J) and is independent of the estimated jamming power $\hat{P}_J + \hat{K}$

2) Multiple Jammers:-

Similar to single jammer, we assume n jammers located at $\{(x_{J_i}, y_{J_i})\}_{i \in [1, n]}$ start to transmit at the power level of $\{P_{J_i}\}_{i \in [1, n]}$ separately at the same time, and m nodes located at $\{(x_i, y_i)\}_{i \in [1, m]}$ become boundary nodes. To calculate e_z , each boundary node measures JSS locally and we denote the JSS *measured* at boundary node i as P_{r_i} 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, P_{f_i} is the combined JSS from n jammers subject to path loss at a boundary node and can be calculated as

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

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

Where \hat{d}_{j_i} is the estimated distance between jammer j and boundary node i . Note that \hat{P}_{J_j} , \hat{K} and P_{f_i} are all in dBm.

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

```

1: procedure MEASUREJSS
2:    $s = \{s_1, s_2, \dots, s_n\} = \text{MeasureRSS}()$ 
3:   if  $\text{var}(s) < \text{varianceThresh}$  then
4:      $s_a = s$ 
5:   else
6:      $JssThresh = \min(s) + \alpha[\max(s) - \min(s)]$ ,  $\alpha \in [0, 1]$ 
7:      $s_a = \{s_i | s_i < JssThresh, s_i \in s\}$ 
8:   end if
9:   return  $\text{mean}(s_a)$ 
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

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 $\hat{\mathbf{z}}$ 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 \hat{X}_{σ_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 fingerprinting 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.

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

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

6.2 Estimating 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, and denote them as $\mathbf{s} = [s_1, s_2, \dots, s_n]$. The measurement set \mathbf{s} can be divided into two subsets ($\mathbf{s} = \mathbf{s}_a \cup \mathbf{s}_c$).

- 1) $\mathbf{s}_a = \{s_i | s_i = PJ\}$, the ambient noise floor set that contains the ambient noise measurements when only jammers are active, and
- 2) $\mathbf{s}_c = \{s_i | s_i = PJ + PC\}$, 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., $\text{mean}(\mathbf{s}_a)$. In most cases, $\mathbf{s}_c \neq \emptyset$ and $\mathbf{s}_a \subset \mathbf{s}$. In a special case where no sender has ever transmitted packets throughout the process of obtaining n measurements, $\mathbf{s}_c = \emptyset$ and $\mathbf{s}_a = \mathbf{s}$. 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 \mathbf{s}_a , which can be obtained by filtering out \mathbf{s}_c from \mathbf{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 by the fact that \mathbf{s}_a is not likely to be empty due to carrier sensing, and the JSS approximately equals to the average of \mathbf{s}_a . The key question is how to obtain \mathbf{s}_a . To do so, we set the upper bound (i.e., JSS_{Thresh}) of \mathbf{s}_c in Algorithm 3 as α percentage of the amplitude span of ambient noise measurements. We validate the feasibility of obtaining \mathbf{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. 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 $(X_1; Y_1); (X_2; Y_2); \dots; (X_N; Y_N)$, the position of the jammer can be estimated by:

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

6.4 Localizing Jammers by Average

Finally to localize the jammer with more accuracy we will take the average of (X_j, Y_j) with less e_z and $(X_{\text{jammer}}, Y_{\text{jammer}})$ calculated by centroids localization. By taking the average of these two values we can localize the jammer with high accuracy.

$$(X_j, Y_j) = \left(\frac{x_{\text{jammer}} + x_j}{2}, \frac{y_{\text{jammer}} + y_j}{2} \right)$$

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 lans and 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.