Framework Creation for Reducing Errors and Jammers Localization in Wireless Networks

Shalini B.K
Department of Computer Science
T. John Institute of Technology

Prof. Srinvasa H.P
Associate Professor
Department of Computer Science
T. John Institute of Technology

***Abstract*— Jammers works as interfere to wireless local area networks. It can interrupt the communications in wireless networks, and position information allows to eliminate the jamming attacks. Our main goal is to design a framework that can find location of one or multiple jammers with a high accuracy. Existing jammer-location finding schemes uses indirect measurements (e.g., hearing ranges) affected by jamming attacks, using this measurements localizing jammers is difficult. Instead, this project uses strength of jamming signals (JSS) that is direct measurement . Estimating JSS is very much challenge as signals of jamming may be embedded in other signals. Estimation scheme is based on level of total noise in area and validate it with real-world experiments. To further reduce errors of estimation, we define a feedback metric to express the quantity of estimation errors and formulate jammer localization as a non-linear optimization problem, whose global maximal solution is close to true positions of jammers. This project includes searching algorithms for approaching the global maximal solution, and simulation show that framework for minimizing error gives better performance than the existing schemes. In addition, this error minimizing framework can utilize indirect measurements to obtain a better location estimation compared with previous work.**

Keywords*— Jammers,

1.INTRODUCTION

The wireless technologies by combining with the unlicensed bands, makes the radio environment packed, leading to unintentional radio interference across devices with different communication technologies. At the same time , the emerging of software defined radios has enabled adversaries to build intentional jammers to disturb network communication with little effort. Regardless whether it is unintentional interference or malicious jamming, one or multiple jammers/ interferers may co-exist and have a detrimental impact on network performance – both can be referred as jamming. To ensure the successful deployment of pervasive wireless networks, it is crucial to localize jammers, since 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 detecting malicious jamming attackers. We focus on finding one or multiple stationary jammers positions. Our goal is to extensively improve the accuracy of jammer localization. Present jammer-localization techniques mostly rely on parameters derived from the affected network topology, such as packet delivery ratios , neighbor lists , and nodes' hearing ranges . These indirect measurements from jamming attacks makes it difficult to accurately localize jammers' positions. Furthermore, they cannot work with multiple jammers localization. They help in detect single jammer localization. So to overcome the drawbacks of indirect measurements, we are using direct measurements of jamming signal strength(JSS) . Jamming signals are embedded in the regular network traffic. The commonly used received signal strength (RSS) measurement associated with a packet does not correspond to JSS. To overcome this challenge, we devise a scheme that can effectively estimate the JSS utilizing the measurement of the ambient noise floor. To increase the accuracy of localization , we formulate the jammer localization problem as a non-linear optimization problem and define an evaluation metric as its objective function. The evaluation metric value 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. Presenting localization error minimizing framework can improve the accuracy of estimation of localizing one jammer , 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.

.

2.THREAT MODEL

Several attack strategies can be performed by jammers in order to disturb wireless communications. we mainly focus on one common type of jammer –constant jammers. By the constant jammers, radio signals are continually emitted, 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. Every jammer has a similar jamming range in all directions. Jammers' positions identification will be done after the jamming attack is detected, and we assume the network is able to identify jamming attacks and obtain the number of jammers, leveraging the existing jamming detection approaches . We classify the network nodes based on the level of disturbance caused by jammers. 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.

- **Unaffected node.** If one node can communicate with all of its neighbors then the node is called as unaffected node . This type of node may not yield accurate JSS measurements.
- **Jammed node.** A node is jammed if it cannot communicate with any of the unaffected nodes. This type of node can measure JSS, but cannot always report their measurements.
- **Boundary node.** A boundary node can communicate with not from all of its neighbors. Boundary nodes can not only but part of its neighbors. It measures the JSS, also report their measurements to a designated node for jamming localization.

Prior to jamming, all the nodes could communicate with their neighbors,. Once the jammer became active, affected nodes lost their neighbors partially or completely.

In this work, the boundary nodes play an important role, and our jammer localization algorithms rely on them for sampling and collecting JSS for jammer localization.

3.FORMULATION OF LOCALIZATION

Our jammer localization approach comprises two steps: (a) JSS Collection. Each boundary node locally obtains JSS. (b) Best-Estimation Searching. A designated node will obtain a rough estimation of the jammers' positions based on the collected JSS. Then, it refines the estimation by searching for positions that minimize the evaluation feedback metric. The details are described in Algorithm 1.

Algorithm 1 Jammer Localization Framework.

```
p = MeasureJSS()
z = Initial positions
while Terminating Condition True do
    ez =EvaluateMetric(z, p)
    if NotSatisfy(ez) then
        z = SearchForBetter()
    end if
end while
```

The search-based jammer localization approaches have a few challenging subtasks:

1) EvaluateMetric() has to define an appropriate metric to quantify the accuracy of estimated jammers' 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.

Here we model the jammer localization as an optimization problem.

3.1 Localization Evaluation Metric

In this section, we discuss the definition of the evaluation metric ez, and we show the property of ez as well as its calculation. For the ease of reading, we summarize the frequently used notations in Table 1.

Description of variables	
Pri	JSS at a boundary node i
Pfi	Power component attenuated by path loss only
PJj	Transmission power of a jammer j
Xσi	Random attenuation at a boundary node i
z	Unknown variable vector of jammers
p	Vector of JSS at m boundary nodes
s	Vector of n ANF measurements at a boundary node
ez	Evaluation feedback metric
ed	Localization error (distance between the estimated location and the true location)

TABLE 1 : Frequently used notations.

3.1.1 The property of ez

The definition of ez 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.

Algorithm 2 Evaluation feedback metric calculation.

```
procedure EVALUATEMETRIC(ˆz, p)
    for all i ∈ [1,m] do
        ˆXσi = Pri − Pfi (ˆz)
    end for
end procedure
```

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

In the case of multiple jammers, pfi is the combined JSS from n jammers subject to path loss at a boundary node

4. MEASURING JAMMING SIGNALS

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 difficult because packets will be send at the same time by multiple wireless devices. It is difficult 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.

4.1 Ambient Noise Floor

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

$$PN = PJ + PW, \qquad (1)$$

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. A naive approach of estimating the ANF could be sampling ambient noise when the wireless radio is idle. Such a method may not work in all network scenarios, since it may result in an overestimated ANF.

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

```
procedure MEASUREJSS
    s = {s1, s2, ..., sn} = MeasureRSS()
    if var(s) < varianceThresh then
        sa = s
    else
        JssT hresh = min(s) + α[max(s) − min(s)] _ α ∈ [0, 1]
        sa = {si|si < JssT hresh, si ∈ s }
    end if
    return mean(sa)
end procedure
```

4.2 Strength of Jamming Signals Estimation

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 **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 ≠ Ø and **s**a ⊂ **s**. In a special case where no sender has ever transmitted packets throughout the process of obtaining n measurements, **s**c = Ø and **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 by the 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.
.

5.FINDING THE BEST ESTIMATION

The jammer localization problem can be modeled as a non-linear optimization problem and finding a good estimation of jammers locations is equivalent to seeking the solution that minimizes the evaluation feedback metric.
There are several heuristic searching algorithms to find the global minimum. In this work, these algorithms take the measured JSS as inputs; however, they are not limited to it.

5.1 Algorithm Description.

5.1.1 A Genetic Algorithm

A genetic algorithms (GA) searches for the global optimum by mimicking the process of natural selection in biological evolution. A GA iteratively generates a set of solutions known as a population. At each iteration, a GA selects a subset of solutions to form a new population based on their “fitness” and also randomly generates a few new solutions. As a result, the “fitter” solutions will be inherited. At the same time, new solutions will be introduced to the population, which may turn out to be “fitter” than ever. As a result, over successive generations, a GA is likely to escape from local optima and “evolves” towards an optimal solution.

5.1.2 A Generalized Pattern Search

A generalized pattern search algorithm (GPS) works similarly to the gradient descent algorithm. However, at each iteration, instead of making a step towards the steepest gradient, a GPS checks a set of solutions (called a mesh) around the current solution, looking for the one whose corresponding function value is smaller than the one at the current solution. If a GPS finds such a solution, the new solution becomes the current solution at the next step of the algorithm. By searching for a mesh of solutions, a GPS is likely to find a sequence of solutions that approach an optimal one without converging to a local minimum.

5.1.3 A Simulated Annealing Search

A simulated annealing algorithm (SA) searches for the optimal solutions by modeling the physical process of heating a material and then controlled lowering the temperature to decrease defects. At each iteration, the simulated annealing algorithm compares the current solution with a randomly-generated new solution. The new solution is selected according to a probability distribution with a scale proportional to the temperature, and it will replace the current solution according to a probability governed by both the new object function value and temperature. By accepting 'worse' solutions occasionally, the algorithm avoids being trapped in local minima, and is able to explore solutions globally. As the temperature decreases, the annealing algorithm reduces its search scale so that it converges to a global minimum with high probability.

6.CONCLUSION

In this work, we addressed the problem of localizing jammers in wireless networks, aiming to extensively reduce estimation errors. The jammers could be several wireless devices causing unintentional radio interference or malicious colluding jamming devices who co-exist and disturb the network together. Most of the existing schemes for localizing jammers rely on the indirect measurements of network parameters affected by jammers, e.g., nodes' hearing ranges, which makes it difficult to accurately localize jammers. In this work, we localized jammers by exploiting directly the jamming signal strength (JSS). Estimating JSS is considered challenging since they are usually embedded with other signals. Our estimation scheme smartly derives ambient noise floors as the JSS utilizing the available signal strength measuring capability in wireless devices. The scheme samples signal strength regardless whether the channel is busy or idle, and estimates the ambient noise floor by filtering out regular transmission (if any) to obtain the JSS. To further improve the estimation accuracy, we designed an error-minimizing-based framework to localize jammers. In particular, we defined an evaluation feedback metric that quantifies the estimation errors of jammers' positions. We examined several heuristic search algorithms (GA, GPS and SA . In particular, among the three searching algorithms, GPS can find the best estimation of multiple jammers' positions in the shortest duration.

REFERENCES

[1] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S. V. Krishnamurthy, "Lightweight jammer localization in wireless networks: System design and implementation," in Proceedings of IEEE GLOBECOM, 2009.

[2] H. Liu, Z. Liu, Y. Chen, and W. Xu, "Determining the position of a jammer using a virtual-force iterative approach," Wireless Networks (WiNet), vol. 17, pp. 531–547, 2010.

[3] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Exploiting jammingcaused neighbor changes for jammer localization," IEEE TPDS, vol. 23, no. 3, 2011.

[4] H. Liu, Z. Liu, Y. Chen, and W. Xu, "Localizing multiple jamming attackers in wireless networks," in Proceedings of ICDCS, 2011.

[5] T. Cheng, P. Li, and S. Zhu, "Multi-jammer localization in wireless sensor networks," in Proceedings of CIS, 2011.

[6] A. Wood, J. Stankovic, and S. Son, "JAM: A jammed-area mapping service for sensor networks," in Proceedings of RTSS.

[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proceedings of MobiHoc, 2005.

[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] D. Goldberg, Genetic algorithms in search, optimization and machine learning. Addison-Wesley, 1989.

[13] E. Polak, Computational Methods in Optimization: a Unified Approach. Academic Press, 1971.

[14] P. V. Laarhoven and E. Aarts, Simulated Annealing: Theory and Applications. Springer, 1987.

[15] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Wireless jamming localization by exploiting nodes' hearing ranges," in Proceedings of DCOSS, 2010.