A Study Analysis on Jammer Localization Schemes and Proposing an Optimized Error-Minimizing Framework for Localizing Jammers in Wireless Networks

P. Priya*, R. Brindha*, S. Manosownthari*, S. Udhayakumar**
*(M.E Applied electronics, Sri Eshwar college of engineering, Coimbatore
** (Assistant Professor,Sri Eshwar college of engineering,Coimbatore

***Abstract* - Jammers can severely disrupt the communications in wireless networks by intentionally emitting radio frequency interference signals aiming at disturbing transceivers' operation. Jamming attacks may be viewed as a special case of Denial of Service (DoS) attacks which may be defined as any event that diminishes or eliminates a network's capacity to perform its expected function. The information about position of jammers allows the defender to actively eliminate the jamming attacks. Thus the main objective of this article is to provide a general overview on various jammer localization techniques currently existing in the wireless networks and proposing an optimized error-minimizing framework for localizing jammers with high accuracy. A brief overview on various jamming models is also reviewed.**

Keywords–Ambient noise floor, Denial of Service, Jamming, Radio interference, Localization.

1. INTRODUCTION

The rapid development in wireless technologies has enabled a broad class of new applications utilizing wireless networks, which often include the monitoring and recording of sensitive information using sensor networks, traffic monitoring through vehicular ad hoc networks, and emergency rescue and recovery based on the availability of wireless signals. As these networks gain popularity, providing security will become an issue of critical importance. Wireless networks, however, are susceptible to many security threats. One serious threat that is especially harmful is jamming attacks. Jamming is defined as the act of intentionally emitting electromagnetic energy towards a communication system to disrupt or prevent signal transmission. To ensure the successful deployment of wireless networks, localizing the jammers becomes utmost important. Most of the existing jammer localization approaches rely on utilizing indirect measurements such as packet delivery ratios [1], neighbour lists [2], and nodes' hearing ranges [3]. These parameters derived from jamming effects make it difficult to accurately localize jammers' positions. Moreover, they mainly localize one jammer and cannot cope with the cases if multiple jammers are located close to each other.

The main goal of this article is to provide a general overview on existing jammer localization schemes and cover all the relevant work, providing the interested researcher pointers for open research issues in this field and to provide a better optimization in jamming detection.

The remainder of this article is organized as follows: Section 2 comprises an overview on various jamming attack models. Section 3 specifies how a hearing range i.e. the area from which a node can successfully receive and decode the packet, alters with jammer's location and transmission power. Further, how to solve the jammer location estimation by our basic least-squares (LSQ)-based scheme is also discussed. Section4analysesdesign and implementation of simple, lightweight and generic localization algorithm. Section 5 specifies two enhanced detection protocols that employ consistency checking. In this section we examine the feasibility and effectiveness of schemes. In Section 6, an experimental analysis on direct measurement- the strength of jamming signals shows an optimized error-minimizing framework for jammer localization. Section 7 summarizes the relevant advantages and shortcomings of jammer localization schemes. Finally Section 8 concludes the paper.

2. JAMMING ATTACK MODELS

In this section, we first define the characteristics of a jammer's behaviour, and then enumerate metrics that can be used to measure the effectiveness of a jamming attack. These metrics are closely related to the ability of a radio device to either send or receive packets. We then introduce four typical jammer attack models that have proven to be effective in disrupting wireless communication.

2.1. Characteristics of a Jammer

A common assumption is that a jammer continuously emits RF signals, so that legitimate traffic will be completely blocked. The common behaviour of all jamming attacks is that their communications are not compliant with MAC protocols. The objective of a jammer is to interfere the wireless communications by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets.

2.2 Metrics

2.2.1 Packet Send Ratio (PSR)
The PSR can be easily measured by a wireless device by keeping track of the number of packets that are successfully sent out by the source and the number of packets that it intends to send out at the MAC layer. If P intends to send out *n* messages, but only *m* of them go through, the PSR is *m/n*.

2.2.2 Packet Delivery Ratio (PDR)
The PDRcan be easily measured by a wireless device by the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. If no packets are received, then the PDR is defined to be 0.

2.3 Jamming Attack Models

There are four typical jammer attack models.

2.3.1 Constant Jammer
The constant jammer continuously emits a radio signal i.e. sends out random bits to the channel without following any MAC-layer etiquette. Moreover, the constant jammer does not wait for the channel to become idle before transmitting. The MAC protocol determines whether a channel is idle or not by comparing the signal strength measurement with a fixed threshold, which is usually lower than the signal strength generated by the constant jammer. Thus , a constant jammer can effectively prevent legitimate traffic sources from getting hold of channel and sending packets.

2.3.2 Deceptive Jammer
The deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions. Thus a normal communicator will be deceived into believing there is a legitimate packet and will be duped to remain in the receive mode. Hence, even if a node has packets to send, it cannot switch to the send mode because a constant stream of incoming packets will be detected.

2.3.3 Random Jammer
A random jammer alternates between sleeping and jamming. After jamming for *tj* units of time, it stops emission and enters a sleeping mode for a period of t_s units of time. It will resume jamming after sleeping for *ts* time.*tj* and *ts* can be either fixed or random values. A special feature about this model is that it tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply.

2.3.4 Reactive Jammer
The three models discussed above are active jammers which are usually effective because they keep the channel busy all the time. The reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets to disrupt the reception of a message. The fact about the model is that a reactive jammer does not necessarily conserve energy because the jammer's radio must continuously be on in order to sense the channel. Another fact is that active jammers are relatively easy to detect whereas reactive jammers maybe harder to detect.

3. JAMMER LOCALIZATION BY EXPLOITING NODES' HEARING RANGE

In this section, we studied that a node'saffected communication range can be estimated purely by examining its neighbor changes caused by jamming attacks. Further we discussed that LSQ-based scheme can effectively estimate the location of the jammer even in a highly complex propagation environment.

3.1 Communication in Nonjamming Scenarios

The communication range defines a node's ability to communicate with others, and it comprises the following two components: the hearing range and the sending range.

3.1.1 The hearing range
Consider Node P as a receiver, the hearing range of P specifies the area within which the potential transmitters can deliver their message to P, e.g., for any Transmitter S in P's hearing range, $(SNR)_{S\to P} > \gamma_{\,o}$.

3.1.2 The sending range
Consider P as a transmitter, the sending range of P defines the region within which the potential receivers have to be located to assure receiving P's messages, e.g., for any Receiver R in P's sending range,$(SNR)_{P\to R} > \gamma_{\,o}$.

The notation $\gamma_{\,o}$ is used to denote the minimum SNR, the threshold required to decode the signal successfully. In a nonjamming scenario, the average ambient noise floor P_N is the same, both the hearing range and the sending range of Node P will be the same.

3.2 Effect of Jamming on the Communication Range

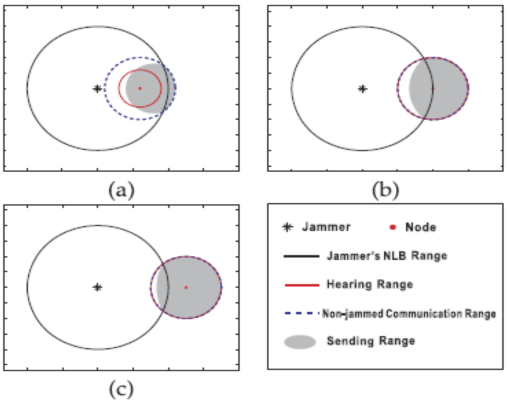


Fig.1 The hearing range, the sending range, and the nonjammed communication range when the location of a jammer is fixed and a node is placed at different spots: (a) inside the jammer's NLB; (b) at the edge of the jammer's NLB; and (c) outside the jammer's NLB.

The jamming signals attenuate with distance, and they reduce to the normal ambient noise level at a circle centered at the jammer which we call as Noise Level Boundary (NLB) of the jammer.

3.3 Effect of Jamming on Network Topology

The communication range changes caused by jamming are reflected by the changes of neighbors at the network topology level. When jammers are present in the network, the network nodes can be classified into three categories based on the impact of jamming as unaffected node N_U, jammed node N_J , and boundary node N_B.

3.3.1 Unaffected node

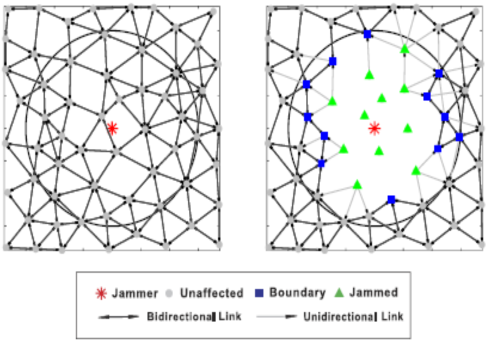
A node is unaffected, if it can receive packets from all of its neighbors.

3.3.2 Jammed node

A node is jammed if it cannot receive messages from any of the unaffected nodes. The fact is that two jammed nodes may still be able to communicate with each other.

3.3.3 Boundary node

A boundary node can receive packets from part of its neighbors but not from all its neighbors.



(a) Jammer is off (b) Jammer is on

Fig. 2.An example of the topology change of a wireless network due to jamming, where the black solid circle represents the jammer's NLB.

Fig.2, illustrates that prior to jamming effect, neighboring nodes were connected through bidirectional links but when the jammer became active, nodes lost their bidirectional links partially or completely.

In Fig. 2, the nodes marked as triangles lost all their receiving links from their neighbors and became jammed nodes. Interestingly, a fact is that some jammed nodes can still send messages to their neighbors, and they may participate in the jamming localization by delivering information to unaffected nodes. The nodes depicted in rectangles are boundary nodes. They lost part of its neighbors but still maintained partial receiving links. Ultimately, the rest of nodes depicted in circles are unaffected nodes because they can still receive from all their neighbors.

3.4 LSQ-Based Jammer Localization

In the previous sections, we have studied that the hearing range of a node may shrink and its neighbor list may change when a jammer becomes active.

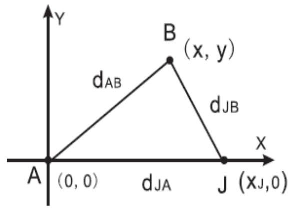


Fig. 3. The coordinate system for the sending range and the hearing range of Node A, wherein A and B are network nodes and J is the jammer.

The levels of changes are determined by the distance to the jammer and the strength of the jamming signals. The basic idea of LSQ-based algorithm is to localize the jammer according to the changes of a node's hearing range. Consider the example illustrated in Fig. 3, if B happens to be located at the edge of A's hearing range, and then we can obtain the following formula:

$$(x_A - x_J)^2 + (y_A - y_J)^2 = \beta r_{hA}^2 \quad (1)$$

where r_{hA} is the new hearing range of Node A, and $\beta = \frac{\gamma_o}{P_T/P_J}$ and (x_A,y_A) and (x_J,y_J) are the coordinates of A and JammerJ, respectively. Suppose that the hearing ranges of m nodes have shrunk to r_{hi} where i={1,2,3,…m}due to jamming. Assume that we can obtain r_{hi} for each of m nodes, then we can localize the jammer by solving the following equations:

$$\begin{gathered}(x_1 - x_J)^2 + (y_1 - y_J)^2 = \beta r_{h1}^2 \\ (x_2 - x_J)^2 + (y_2 - y_J)^2 = \beta r_{h2}^2 \\ \vdots \\ (x_m - x_J)^2 + (y_m - y_J)^2 = \beta r_{hm}^2\end{gathered}$$

We could linearize the problem by subtracting the mth equation from both sides of the first m-1equations and obtain linear equations to avoid solving complicated nonlinear equations. Thus, we can localize the jammer by examining the neighbor list changes of multiple nodes and constructing a least-squares problem.

4. LIGHTWEIGHT JAMMER LOCALIZATION

This scheme is based on the principles of gradient descent minimization algorithm. The key observation is that the Packet Delivery Ratio (PDR) has lower values as we move closer to the jammer.

4.1 Gradient Descent Minimization

Gradient descent is a unique optimization method for real valued functions. The idea of this technique is that starting from a point, we greedily move towards the direction of the maximum decrease of the function at the neighbourhood of this point using a step of γ_n at every iteration. After a series of iterations, the algorithm will converge to the minimum of the function. In order to find the minimum of this function, one may start from a point $\vec{x}_0 \in R^n$ and continue finding a series of points using:

$$\vec{x}_{n+1} = \vec{x}_n - \gamma_n * \nabla f(\vec{x}_n) \qquad (2)$$

where$\nabla f(\vec{x}_i)$ is the gradient of f.

We can modify the above gradient descent method in order to localize the jammer. Function f is the PDR while the next candidate points $\vec{x}_{n+1}$ are the neighbors of the node under consideration. Every node will try to find its neighbor node with the largest decrease in PDR. The Pseudocode for localizing the node i is

```
Data: Neighbor's PDR
Result: Next node n closer to the jammer
begin
Pick $k$: $(PDR_i - PDR_k) > (PDR_i - PDR_j)\forall_j \neq k$
            $\Delta = (PDR_i - PDR_k)$
                $if\ \Delta > 0\ then$
    $n = k$
    $else$
        $n = i$
    $end$
$end$
$return$
$end$
```

In order to calculate PDR_i we use the average value of PDR of the link between node i and its neighbors as follows:

$$PDR_i = \frac{\sum_{m=1}^{|NS|} PDR_{im}}{|NS|} \qquad (3)$$

whereNS the set of neighbors of i, PDR_{im} is the PDR on link $i - m\ and\ |NS|$ is the cardinality of NS, the numbers of neighbors of node i.

5. FEASIBILITY OF DETECTING JAMMING ATTACKS

Detection of jamming attacks can be done by the measurements of signal strength and carrier sensing time. But the fact is that both signal strength and carrier sensing time, under certain circumstances, can only detect the constant and deceptive jammers. Consequently, compared to signal strength and carriersensing time, PDR is a powerful statistic in that it can be used to differentiate a jamming attack from a congested network scenario, for different jammer models.

5.1 Jamming Detection With Consistency Checks

A node's weak reception capability (i.e. alow PDR) can be caused by several factors besides jamming, such as a low link quality due to the relatively large distance between the sender and the receiver. Since PDR is a powerful measurement that is capable of discriminating between jammed and congested scenarios, we will examine two strategies that build upon PDR to achieve enhanced jammer detection.

5.2 Signal Strength Consistency Checks

We employ measurements of the PDR between a node and each of its neighbors and signal strength as a consistency check in order to combat false detections due to legitimate causes of link degradation. Specifically, we check to see whether a low PDR value is consistent with the signal strength that is measured.

In a normal scenario, where there is no interference or software faults, a high signal strength corresponds to a high PDR. However, if the signal strength is low, which means the strength of the wireless signal is comparable to that of the ambient background noise, the PDR will be also low. On the other hand, a low PDR does not necessarily imply a low signal strength. It is the relationship between signal strength and PDR that allows us to differentiate between the following two cases, which were not able to separate using just the packet delivery ratio.

First case would be from the point of view of a specific wireless node, it may be that all of a node's neighbors have moved beyond a reliable radio range or it may be that all of its neighbors have died. A second case would be the case that the wireless node is jammed. The key observation here is that in the first case, the signal strength is low, which is consistent with a low PDR measurement. While in the jammed case, the signal strength should be high, which contradicts the fact that the PDR is low.

Jamming detection algorithm that checks the consistency of PDR measurements with observed signal strength readings is given below.

```
PDRSS_Detect_Jam
{PDR(N): N∈ Neighbors} = Measure_PDR()
MaxPDR = max{PDR(N): N∈ Neighbors}
If MaxPDR< PDRThresh then
SS = Sample_Signal_Strength()
 CCheck = SS_ConsistencyCheck(MaxPDR,SS)
If CCheck== False then
Post NodeIs Jammed()
End
End
```

In the PDRSS_Detect_Jam algorithm, a wireless node will decide that it is not jammed if at least one of its neighbors has a high PDR value. However, if all neighbors' PDR values are low then the node mayor may not be jammed so we need to further differentiate the possibilities by measuring the ambient signal strength. The function Sample_Signal_Strength() reactively measures the signal strength values for a window of time after the PDR values fall below a threshold and returns the maximum value of the signal strengths denoted as SS during the sampling window. It is noticed that the duration of the sampling window should be carefully tuned based upon the jamming mode, the traffic rate, the measuring accuracy ,and the desired detection confidence level.

The function SS_ConsistencyCheck() takes the maximum PDR value of all the neighbors, denoted as *MaxPDR* and the signal strength reading SS as inputs. To see whether the low PDR values are consistent with the signal strength measurements, a consistency check is performed. If *SS* is too large to have produced the observed *MaxPDR* value, then SS_ConsistencyCheck() returns False, else it returns True.

5.3 Location Consistency Checks

The LOC_Detect_Jam algorithm employs location information and uses a proactive consistency check. The LOC_Detect_Jam protocol requires the support of a localization infrastructure, such as GPS [6],a localization technique which provides location information to wireless devices. In the LOC_Detect_Jam protocol, we use PDR as the metric indicating link quality.

A node will decide its jamming status by checking its PDR whether the observed PDR is consistent with the location of its neighbor nodes. Most probably, neighbor nodes that are close to a particular node should have high PDR values, and if we observe that all nearby neighbors have low PDR values, then we conclude that the node is jammed. Jamming detection algorithm that checks the consistency of PDR measurements with location information is given below.

```
LOC_Detect_Jam
{PDR(N): N∈ Neighbors} = Measure_PDR()
(n,MaxPDR) = (arg max, max) {PDR(N): N∈ Neighbors}
If MaxPDR< PDRThresh then
P$_0$ =(x$_0$,y$_0$) = GetMyLoc()
P$_n$= (x$_n$,y$_n$) = LookUpLoc(n)
d= dist(P$_0$, P$_n$)
CCheck= LOC_ConsistencyCheck(MaxPDR,d)
If CCheck== False then
Post NodeIs Jammed()
End
End
```

The function LOC_ConsistencyCheck() operates in a similar manner as SS_ConsistencyCheck(). To represent the profile of normal radio operation for node *A*, a table of (*PDR*, *d*) values are gathered. We may define a jammed-region and a benign-region using either a binning procedure or regression to obtain lower bounds on the PDR that should be observed for a given distance under benign radio conditions using measured data as in SS_ConsistencyCheck(). The node declares that it is jammed if the point (*MaxPDR*, *d*) falls in the jammed-region. Therefore the above discussed consistency checking schemes can be effectively implemented to improve detection of jamming in the wireless networks.

6. DIRECT MEASUREMENT OF JAMMER LOCALIZATION

To overcome the limitation caused by indirect measurements of the jamming effect, we propose to use the direct measurement of the strength of jamming signal (JSS). As the jamming signals may be embedded with the other signals in the regular network traffic, estimating strength of the jamming signals is yet challenging. One way to overcome this challenge is to utilize the measurement of the ambient noise floor (ANF), which is readily available from many commodity devices (e.g., MicaZ motes). This can effectively estimate the JSS.

6.1 Jammer Localization Framework

Our jammer localization approach comprises the following tasks:

- JSS collection at each boundary node.
- Best estimation searching. Based on the collected JSS, a designated node will obtain a rough estimation of the jammers' positions which is then refined by searching for positions that minimize the evaluation feedback metric

6.1.1 Estimating Strength of Jamming Signals

Ambient noise is the sum of all unwanted signals that are always present in the channel. The ANF is the measurement of the ambient noise which in the presence of jammers includes thermal noise, atmospheric noise, and jamming signals. Thus it is given by:

$$P_N = P_J + P_W \quad (4)$$

where P$_J$ is the JSS, and P$_W$ is the white noise comprising thermal noise, atmospheric noise, and so on. Realizing that at each boundary node P$_W$ is relatively small compared to P$_J$, the ANF can be roughly considered as JSS. Thus, estimating JSS is equivalent to deriving the ANF at each boundary node. To derive the JSS, our scheme involves sampling ambient
noise values regardless of whether the channel is idle or busy.

6.1.2 Acquiring Ambient Noise Floor

ANF approximates the strength of jamming signals by the following Algorithm.

```
procedure MEASUREJSS
$s = \{s_1, s_2, s_3 \ldots . s_n\} = MeasureRSS()$
ifvar(s) <varianceThreshthen
                        $s_a = s$
else
JssThresh = $min(s) + \alpha[\max(s) - \min(s)]$ ⊳
$\alpha\epsilon$ [0,1]
          $s_a = \{s_i | s_i < JSSThresh, s_i \epsilon\, s\}$
end if
return mean($s_a$)
end procedure
```

The measurement set*s* can be dividedinto two subsets ($s = s_a \cup s_c$) where

- $s_a = \{s_i | s_i = P_J\}$, the ANF set that contains theambient noise measurements when only jamming signals are active.

- $s_c = \{s_i | s_i = P_J + P_C\}$, the combined ambient noise set that contains ambient noise measurements when both jamming signals (P_J) and signals from one or more transmitters (P_C) are present.

6.2 Error-Minimizing Based Algorithms for Localizing Jammers

6.2.1 Single jammer

Assume single jammer J located at (x_J,y_J) starts to transmit at the power level of P_J , and m nodes located at$\{(x_i, y_i)\}_{i\in[1,n]}$become boundary nodes.

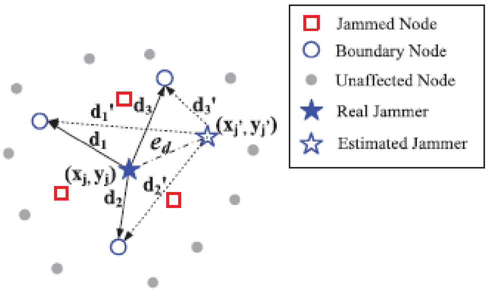


Fig.4. Illustration of jammer localization basis

To calculate e_z, each boundary node will 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 position and the transmission power be:

$$\hat{z} = [\hat{x}_J, \hat{y}_J, \hat{P}_J + \hat{K}] \qquad (5)$$

6.2.2Algorithm for Jammer Localization Framework

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

The subtasks that has to be carried out are as foilows:
Step 1: Collection of JSS at each boundary nodes.
Step 2: Calculating average channel attenuation.
Step 3: Calculating JSS subject to path loss only.
Step 4: Random Attenuation is calculated by subtracting JSS subject to path loss from JSS at each boundary node.
Step 5: Calculating evaluation feedback metric(e_z) which is the standard deviation of estimated random attenuation.
Step 6: If the estimation errors of jammer's location is larger, then larger will be $e_{z..}$
Step 7: Searching for minimum e_z utilizing gradient pattern search which is similar to gradient descent minimization will finally reaches its minimum at a location close to jammer's position.

6.2.3 Algorithm for Evaluation Feedback Metric Calculation

```
**procedure** EVALUATEMETRIC ($\hat{\boldsymbol{z}}, \boldsymbol{p}$)
**for all**$i \in [1, m]$**do**
$\hat{\hat{X}}_{\sigma i} = P_{r_i} - P_{f_i}(\hat{z})$
**end for**
        $\boldsymbol{e_z} = \sqrt{\frac{1}{m}\sum_{i=1}^{m}\left(\hat{\boldsymbol{X}}_{\sigma i} - \hat{\hat{\boldsymbol{X}}}_{\sigma}\right)^2}$
**end procedure**
```

For given $\hat{z}$, we can estimateP_{f_i}, the JSS subject to path loss only at boundary node i as:

$$P_{f_i}(\hat{d}_i) = \hat{P}_J + \hat{K} - 10\eta \log_{10}(\hat{d}_i) \qquad (6)$$

$$\hat{d}_i(\hat{z}) = \sqrt{(\hat{x}_J - x_i)^2 + (\hat{y}_J - y_i)^2} \qquad (7)$$

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

$$\hat{X}_{\sigma i} = P_{ri} - P_{fi}(\hat{d}_i) \qquad (8)$$

Similar to single jammer, multiple jammers can also be located by measuring the JSS locally and we denote the JSS measured at boundary node i as P_{ri} that is a combined JSS from multiple jammers.

We define e_z as the estimated standard deviation of $X_\sigma$derived from the estimated jammers'locations. Considering single -jammer case, when the estimated jammer's location equals the true value, e_z is the real standard deviation of X_σ which is probably small. When there is an error in estimation (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 larger the e_d is, the bigger the estimated standard deviation of X_σ will likely be.

The frequently used notations are summarized in TABLE 1.

Table 1: Frequently used Notations

Description of variables	
p	Vector of JSS at m boundary nodes
P_{r_i}	JSS at boundary node i
P_{j_i}	Power component attenuated by path loss only
P_{j_j}	Transmission power of a jammer j.
K	Unitless constant which depends on the characteristics of antenna and average attenuation of the channel.
$X_{\sigma i}$	Random attenuation at a boundary node i
s	Vector of n ANF measurements at a boundary node.
z	Unknown variable vector of jammers.
σ	Standard deviation of random attenuation.
e_z	Evaluation feedback metric
e_d	Distance between estimated location and true location.
(x_i, y_i)	Coordinates of a boundary node i.
(x_{j_j}, y_{j_j})	Coordinates of jammer j.

6.3 Best Estimation

Finding a good estimation of jammers' locations is equivalent to seeking the solution that minimizes the evaluation feedback metric

e_z. A GPS algorithm [7] works in a similar manner as the gradient descent algorithm. However, a GPS checks a set of solutions around the current solution, looking for the one whose corresponding function value is smaller than the one at the current solution instead of making a step toward the steepest gradient, during each iteration. If such a solution is found by GPS, the new solution becomes the current solution at the next step of the algorithm. By searching for a set of solutions, a GPS is likely to find a sequence of solutions that approach an optimal one without converging to a local minimum.

6.4 Experimental Validation

To verify jammer localization utilizing the direct measurements, we conducted experiments on a network topology which has 83 nodes including two jammers.

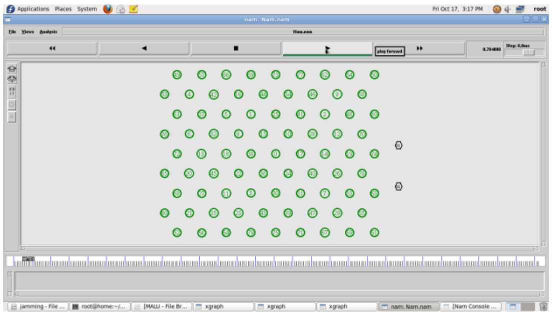
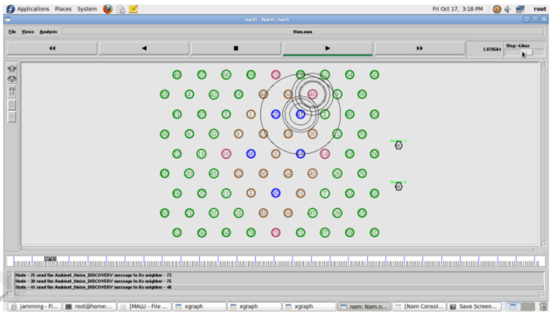
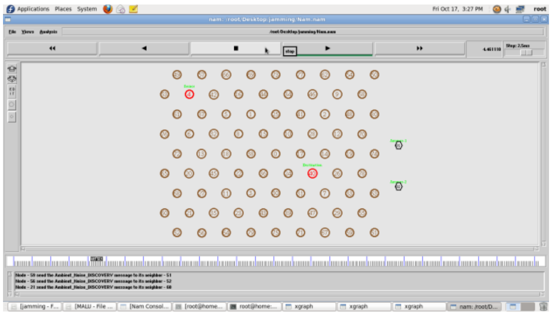


Fig.5.Initial node deployment before ANF discovery



```
Node - 25 send the Ambient_Noise_DISCOVERY message to its neighbor - 73
Node - 30 send the Ambient_Noise_DISCOVERY message to its neighbor - 75
Node - 41 send the Ambient_Noise_DISCOVERY message to its neighbor - 46
```

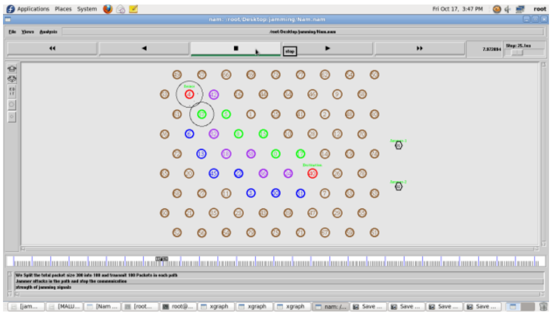
Fig.6. Discovery of ANF messages



```
Node - 59 send the Ambient_Noise_DISCOVERY message to its neighbor - 51
Node - 56 send the Ambient_Noise_DISCOVERY message to its neighbor - 53
Node - 21 send the Ambient_Noise_DISCOVERY message to its neighbor - 68
```

Fig.7. Nodes Deployment after ANF discovery

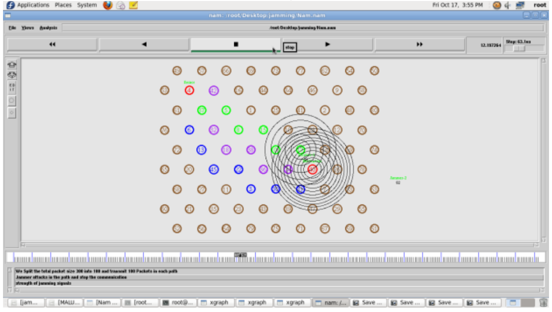
Each and every node collects the ambient noise floor messages from all of its neighbor nodes before initiating transmission. Routing is based on the type of reactive routing protocol. In reactive routing protocol, a source node initiates route discovery process within the network only when it requires a route to a destination.



We Split the total packet size 300 into 100 and transmit 100 Packets in each path
Jammer attacks in the path and stop the communication
strength of jamming signals

Fig.8. Packet transmission before Jammer attack

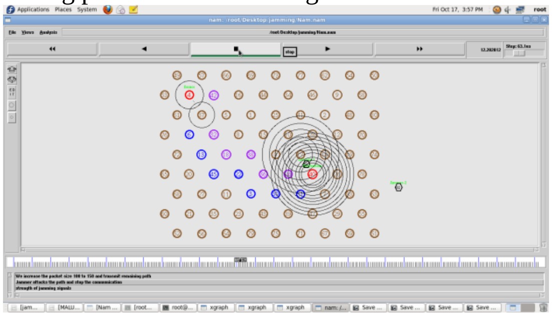
In Fig.8, packets are transmitted from source to destination using Dynamic source routing protocol(DSR). Initially it transmits using three different paths i.e. multipath routing when the network is free from jammer attacks.



We Split the total packet size 300 into 100 and transmit 100 Packets in each path
Jammer attacks in the path and stop the communication
strength of jamming signals

Fig.9. Single jammer attack

In Fig.9, packet forwarding is disturbed in the path due to the presence of jammer. This could be identified by the source when it fails to receive any acknowledgement for a certain period of time from the destination. Instead it receives route error message from the intermediate node indicating jamming in the path of the transmission preventing packets from reaching destination.

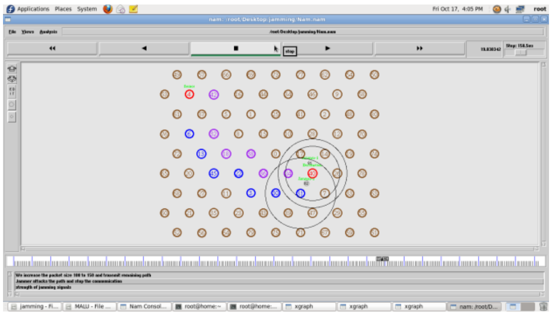


We increase the packet size 100 to 150 and transmit remaining path
Jammer attacks the path and stop the communication
strength of jamming signals

Fig.10. Single jammer detection

Jammer location is identified by utilizing the periodic ANF discovery and error-minimizing algorithms. Initially, the location information of the jammer is broadcasted to all the nodes so that they could avoid that routing path in their future transmissions.

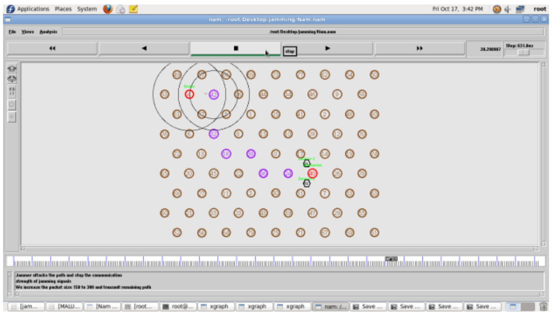
Then the source node will continue its transmission with the remaining two paths that reaches the destination securely. Jamming-aware traffic allocation is implemented.



We increase the packet size 100 to 150 and transmit remaining path
Jammer attacks the path and stop the communication
strength of jamming signals

Fig.11. Multiple jammer attack

In Fig.11, packet transmission is again interrupted in another routing path due to the presence of another jammer.



Jammer attacks the path and stop the communication
strength of jamming signals
We increase the packet size 150 to 300 and transmit remaining path

Fig.11. Multiple jammer detection

Multiple jammers are also identified in a similar manner by which the single jammer is identified. As soon as the jammer locations are identified, the location information is broadcasted to all the nodes to avoid further delay in packet transmission.

Then the source node will continue its transmission with the remaining single path that reaches the destination securely. Jamming-aware traffic allocation is implemented. If the source node has lost all its route to destination then it repeats initiating route discovery process which involves transmission of route request message and reception of route reply message and transmission of packets through the discovered route or routes to destination.

This process is repeated until it completes the transmission of entire packets.

6.4 Performance Validation

Various performance metrics like Packet delivery ratio, Throughput and Packet drop evaluation shows jammer localization approaches using direct measurements improves the accuracy of localizing jammers in wireless networks.

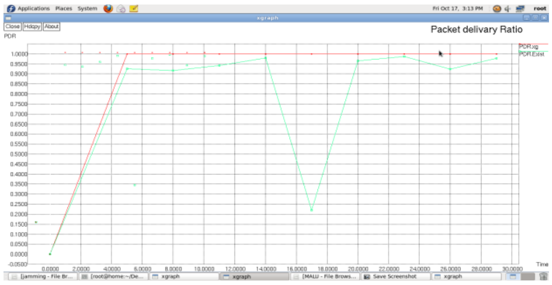


Fig.12. Packet delivery ratio

Packet Delivery Ratio (PDR) is defined by the ratio between number of bits transferred and number of bits received. Simulation result shows improved PDR values

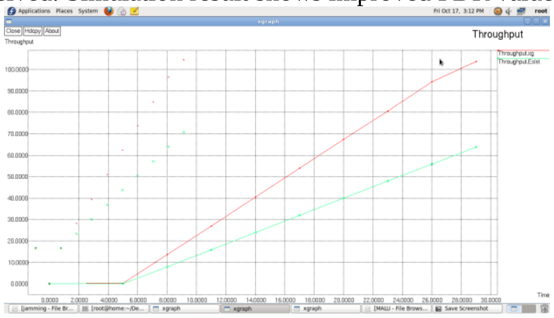


Fig.13. Throughput

Throughput shows the total performance, it also represents number of bits transferred per second. Simulation result shows increased throughput.

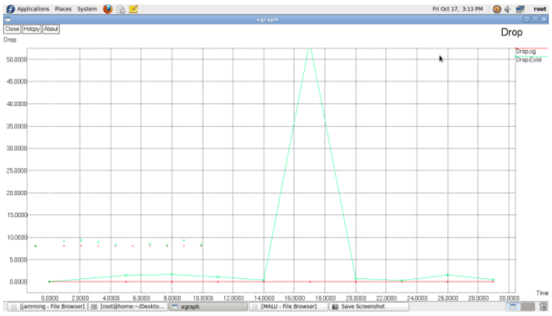


Fig.14. Packet drop

Packet drop indicates measure of packet loss during transmission. This value should be negligible for achieving successful transmission. The performance shows packet loss is zero which indicates efficient packet transmission.

6. RELATED WORK

In this section, we have summarized the behavior of four typical jammer attack modelsand have discussed about the advantages and shortcomings of the above analysed localization and detection schemes. The main focus of this work is to provide an overview on jammer localizing schemes.

The following TABLE 2 summarizes the behaviour of four typical jammer attack models in the wireless networks.

Table 2: Characteristics of Jamming Models

Jamming Attack Models	**Characteristics**
Constant Jammers	• Active jammer. Keeps the channel busy all the time. • Continuously emit radio signals. • Effectively prevent legitimate traffic sources from getting hold of channel and sending packets. • Easy to detect.
Deceptive Jammers	• Active jammer. Keeps the channel busy all the time. • Constantly injects regular packets and a normal communicator will be duped to remain in the receive state. • Easy to detect.
Random Jammers	• Active jammer. Keeps the channel busy all the time. • Alternates between jamming and sleeping. • Special feature is that it takes energy conservation into consideration. • Easy to detect
Reactive Jammers	• Jammer stays quiet when the channel is idle and starts interruption as soon it senses activity on the channel. • Hard to detect.

The following TABLE 3 summarizes the characteristics of various jammer localization schemes in wireless networks.

Table 3: Features of various Jammer Localization Schemes

Jammer Localization Schemes	**Characteristics**
Hearing Range Based • Localize a jammer by examining network topology changes caused by jamming attacks.	**Advantages** • Lower computational cost. • Localization accuracy is high. • Works well in the jamming scenarios. **Disadvantages** • Not efficient in idle network.
Lightweight Jammer Localization • Principle of gradient descent minimization algorithm is implemented. • Key observation is the PDR which has lower values as we move closer to the jammer.	**Advantages** • Does not require any special hardware support. • Relies on PDR which is readily available on each node. **Disadvantages** • Local minima sensitivity. • Less effective in the presence of multiple jammers.
Feasibility of Jamming and Detection Schemes • Examining radio interference attacks by observing signal strength, carrier sensing time and packet delivery ratio. • Analysis of issues in diagnosing the presence of jamming attacks.	**Advantages** • Proposes two enhanced detection algorithms – one employing signal strength and other employing location information as consistency check with combination of PDR. **Disadvantages**: • Large carrier sensing time may be due to congestion.
Direct Measurement of Jammer Localization • Based on the measurement of strength of jamming signals at the boundary nodes. • Proposed estimation scheme can accurately derive the JSS from the measurements of ambient Noise Floor(ANF). • Estimation accuracy can be further improved by designing an error-minimizing framework to localize jammers. • Defined an evaluation feedback metric that quantifies the estimation errors of jammers' positions. • Studied the relationship between the evaluation feedback metric and estimation errors, and showed that the locations that minimize the feedback metric approaches jammers' true locations.	**Advantages** • Addresses the problem of localizing jammers in wireless networks. • Simulation results shows that good localization accuracy can be achieved. • Packet delivery ratio (PDR) evaluation shows better performance than existing schemes. • Increased Throughput. • Packet drops may be reduced to zero.

7. CONCLUSION

In this article, we had an overview on the characteristics of four different jammer attack models that may be employed against a wireless network. Then we analysed some of the existing jammer localization schemes that employs indirect measurements for detecting jamming attacks. We then summarized the advantages and shortcomings of the above discussed jammer localization approaches. To address the limitation caused by indirect measurements of jamming attacks, we proposed the jammer localization by utilizing direct measurements- the strength of jamming signals (JSS). The primary focus of this work is to provide a jamming-aware traffic allocation in the wireless networks. This analysis will serve as the basis for researcher pointers for open research issues in this field and to provide a better optimization in jamming detection. Our simulation results show that our error-minimizing-based framework based on direct measurement achieves better performance than the existing schemes utilizing indirect measurements. Our future work will be to localize all type of jammers even in the lower bound of the network.

REFERENCES

[1] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S.V. Krishnamurthy, “Lightweight Jammer Localization in Wireless Networks: System Design and Implementation,” Proc. 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, vol. 17, pp. 531-547, 2010.

[3] Z. Liu, H. Liu, W. Xu, and Y. Chen, “Exploiting Jamming-Caused Neighbor Changes for Jammer Localization,” IEEE Trans. Paralleland Distributed Systems, vol. 23, no. 3, pp. 547-555, Mar. 2012.

[4] H. Liu, Z. Liu, Y. Chen, and W. Xu, “Localizing Multiple Jamming Attackers in Wireless Networks,” Proc. 31st Int’l Conf. Distributed Computing Systems (ICDCS), 2011.

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” MobiHoc ’05: Proc. Sixth ACM Int’l Symp. Mobile Ad Hoc Networking and Computing, pp. 46-57, 2005.

[6] P. Enge and P. Misra.Global Positioning System: Signals, Measurements and Performance. Ganga-JamunaPr, 2001.

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