ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 32 – 36 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp07.pdf

OPTIMIZED HYBRID APPROACH FOR SEARCHING LOCALIZED JAMMERS IN WIRELESS NETWORKS

M.Jayasree[1],K.Sekar[2]
[1]139E1D5812, M.Tech CSE Student, S.V.Engineering College for Women, Tirupati, AP, India
Jaya.mvp@gmail.com
[2]Associate Professor, Dept. of CSE, S.V.Engineering College for Women, Tirupati, AP, India,
Sekhar.k@svcolleges.edu.in

ABSTRACT

The communication in wireless networks can be severely disturbed by jammers as it continuously emits radio interference signals and the jamming attacks suspects the reliability of wireless communication in the network. The jammer location details makes the protector to eradicate the jamming attacks. This paper focus on an approach that can identify one or multiple jammers. Previous schemes used indirect measurements like nodes hearing ranges, packet delivery ratios, neighbor lists which don't identify the true position of jammers. Here a direct measurement called Jamming Signal Strength(JSS) is utilized. Evaluating JSS is still difficult as they are surrounded in regular network signals. To identify the estimated locations of jammer, an evaluation feedback metric is defined. For obtaining the better location we use heuristic search methods which uses JSS based direct measurement and centroid based localization approach for estimation of jammer,. By combining these two methods we can achieve the better result to localize the jammer in wireless network.

Key words: Jammers , radio interference, JSS,ANF

1.INTRODUCTION

Wireless Networks are widely used in many communication areas. Now it will be difficult in the issue of providing security as these networks gain popularity. However, wireless networks are suspectible to many security threats. One of the serious threat especially harmful is radio interference attack i.e. jamming attack Jamming is defined as an act of emitting interference signals thereby disturbing the communication in the wireless networks. Sometimes the jammer may be a device who purposefully aim to prevent the users from gaining the actual communication either for sending message or causes packet collision which leads to blocking of communication in the networks. Therefore, to make sure the successful deployment of wireless networks, localizing the jammers becomes utmost important. By defining the position of jamming device the network communication can be restored. Here, identification of one or multiple jammers can be focused in order to increase the accuracy of jammer position.

Some of the approaches that are available are packet delivery ratios, neighbor lists and hearing ranges of nodes which comes under indirect measurements that are not accurate to find jammer's position. These indirect measurement concentrate on finding one jammer at a time and cannot consider in the case of multiple jammers are close to each other. For this reason a direct measurement , jamming signal strength(JSS) is used .This JSS uses ambient noise floor(ANF),i.e. sum of all unwanted signals, which is freely available from many service devices. To localize jammers evaluation feedback metric is used which makes use of path loss and shadowing phenomena in radio propagation. Various heuristic search methods are used for finding best solution in localizing jammer's position.

2. RELATED WORK

Jammer is nothing but an entity who purposefully tries to interfere with the physical transmission and reception of wireless communications. The aim of jammer is to disturb the wireless communication by continuously emitting radio frequency signals so that the traffic in network can be completely blocked. The jammer achieves its goal either by preventing the source sending packets or by preventing the reception of packets. and tables. except at the beginning of a sentence:

2.1. Jamming Detection Techniques :

Some of the jammer detection methods are packet delivery ratios, neighbor lists ,hearing ranges of nodes. All these comes under indirect measurements.

2.1.1.Packet Delivery Ratio:

The packet delivery ratio(PDR) is a metric obtained at each node and this ratio is used to find the corruption of transmission. It makes use of interesting nature of wireless medium. As the distance of transmitter is larger, the strength of jamming signal is smaller. The transmitter that is far from jammer doesn't sense JSS strongly. The transceivers will have increased PDR if they moved away from jammer. Regarding this property, a localization method is designed which suffers with the sensitivity to local minima.

ISSN 2347 - 3983
International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 32 – 36 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp07.pdf

2.1.2..Neighbor Lists:

There are two basic models of jamming attacks in this approach, they are region based and signal-to-noise ratio(SNR) based. The region based model determines the impact of jamming depending only on received strength of signals, whereas SNR based model measures the receiver's noise .The virtual iteration force approach(VIFA) utilizes both region based and signal to noise based models to find the true position of the jammer. Using this VIFA as number of packets. and iterations increases, the computational cost also higher.

2.1.3.Nodes Hearing Ranges:

Based on the changes of the neighbor node, this method is developed for localizing the jammer. The changes of communication range is found which are caused due to the presence of jammer and transmitted power using free space model. The neighbor node changes can be found from affected jammed node. Here, the jammer position can be solved using Least-Squares(LSQ) analysis that determines the change in the communication medium. Not apt for finding multiple jammers in the network.

From all the above detecting techniques, it is difficult to find exact position of jammers. So that a direct measurement i.e., jamming signal strength is used for detecting jammers which makes use of ANF .

2.1.4.Signal Strength:

The most important method is to determine the strength of the signal by measuring and analyzing the signal strength distribution in the presence of jammer. This approach involves comparison of average signal level with that of threshold value calculated from overall noise level.

2.2.Types of Jamming Attacks:

There are four jamming attacks in wireless networks. They are:

.

2.2.1 Constant Jammers:

The constant jammer always emits a radio signal to the channel without following any MAC layer. Moreover, the constant jammer does not wait for the channel to become inactive before communication Thus, a constant jammer can efficiently stop legal traffic sources from getting hold of channel and distribution packets..

2.2.2.Deceptive Jammers:

The deceptive jammer frequently inject usual packets to the channel without any gap between following packet transmissions. It also broadcasts fictitious messages and reply old ones. Hence even if a node has packets to send, it cannot switch to the send node because a steady flow of incoming packets will be found.

2.2.3.Random Jammers:

The random jammer alternates in between resting and jamming once jamming occurred for tj units of time ,it stops release and enters a resting mode for a period of ts units of time. It will continue jamming after sleeping for ts time.tj and ts can be fixed or random values. A special feature of this model is that it tries to take energy into consideration, which is particularly essential

2.2.4.Reactive Jammers:

This type of jammer will wait moderately when the channel is at rest .As quickly as it senses action on channel, it starts signal transmission. Active jammers are relatively easy to detect whereas reactive jammers may be hard to detect.

3.PROBLEM IDENTIFICATION

Many jammer attack strategies are available that can performs disruption in wireless communications. It is not possible to cover all jamming attack models that might exist. Here, constant jammers are focused which continuously emits radio signals, by not considering of whether the channel is at rest or not.

Such jammers are unintentional radio signals which are always energetic that keep disturbing network communication. Locating of jammers' positions will be performed after the jamming attack is found. Based on the level of disturbance caused by the jammer, the network nodes can be divided into three categories

3.1.Unaffected node

A node is said to be unaffected only if it communicate with all its neighbor nodes. Such kind of node can be affected by jamming attacks and not able to get correct measurement of JSS.

3.2.Jammed node

A node is a jammed node which does not communicate with any of unaffected node. Here,this kind of nodes can measure JSS but does not always report JSS measurements.

3.3.Boundary node

A node is a boundary node which can communicate with part of neighbors but not with all its neighbors. Boundary nodes measures JSS and report their measurements also based on jammer's position.

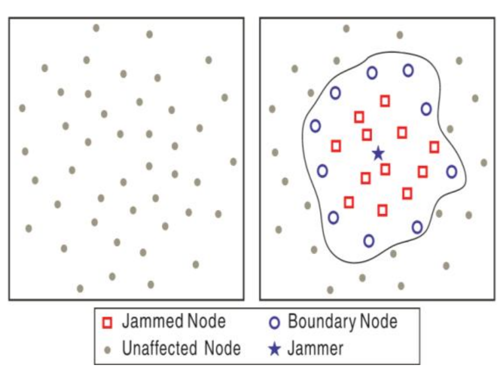

Figure 1: Classification of networks before jamming(left) and after jamming(right)

ISSN 2347 - 3983
International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 32 – 36 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp07.pdf

Before jamming, all nodes can communicate with their neighbors. If the jammer became energetic represented by star, affected nodes can loose their neighbors partially or fully.

4. LOCALIZATION FORMULATION:

Here, first a set of JSS is collected for all assumed positions and then evaluation feedback metric is calculated. This metric finds the distance between assumed locations and true positions of jammer. For example, a minimum value of evaluation feedback shows that assumed position are near to true positions with high accuracy. Here, localization is a two step process.

1.Collection of JSS:JSS can be obtained for every boundary node.

2.Estimation Searching: A particular node is roughly estimated from the JSS collection. After that it refines the searching for the position of jammer which decreases the evaluation feedback metric.

The Jammer localization has a few subtasks.

1.EvaluateMetric() defines a metric to find accuracy of assumed jammer's position..

2.JSSMeasure() obtain JSS even if they are surrounded in regular transmission.

3.SearchingFor Best() searches for best estimation using collected JSS measurements. So that, we model jammer identification as an optimized approach.

Algorithm 1Framework for jammer localization

p=measureJSS()
z=Initial positions
While terminating Condition true **do**
ez=EvaluateMetric(z,p)
ifNotSatify(ez)**then**
z=SearchForBetter()
end if
end while
Min(ez)=ez
(xi,yi)=GetEstJammer(z);
(xjammer,yjammer)=GetCentroid);
(xest,yest)=Average(xi,yi,xjammer,yjammer);

4.1. Radio Propagation Basics*:*

In the communication of wireless networks ,receiving signal strength(RSS) attenuates as the distance between sender and the receiver increases because of shadowing and path loss. Path loss is average attenuation and shadowing is random attenuation through reflection, scattering, diffraction and absorption.

Here, localization method under path loss and shadowing is given as follows:

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

Where Xσ is zero mean Gaussian zero mean variable with standard deviation σ,

K is a unit less constant that depends on channel attenuation, and η is exponent of path loss .In a free space, η is 2 and Xσ is always 0.

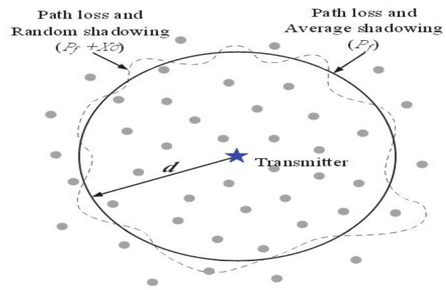

Figure 2: RSS attenuation for pathloss and shadowing.

4.2.Evaluation metric for localization :

The evaluation feedback metric can be calculated for both single jammer and multiple jammers. Assume single jammer J located at(xi,yi) starts to transmit at power level of pj, and m nodes located at{(xi,yi)}i Є [I,n] become boundary node.

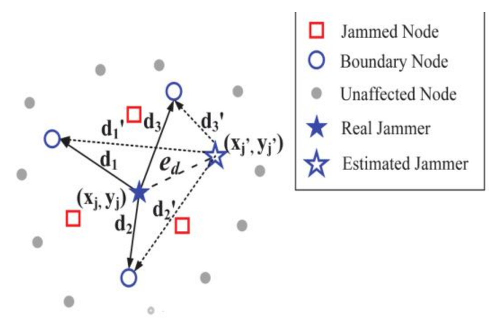

Figure 3: .jammer localization

Algorithm 2:Evaluation feedback metric calculation.

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

Similar to single jammer, multiple jammers can also be located by measuring JSS locally for m nodes.

5. JAMMING SIGNAL MEASUREMENT:

Getting the jamming signal strength is difficult because they are surrounded in regular network during transmission. Obtaining JSS is difficult because many wireless devices sends packets at a same time, as the jammer always interrupts the regular operations in wireless networks.

Here, most important method is to determine the strength of the signal by measuring and analyzing the signal strength distribution in the presence of jammer. This method makes the analysis of comparing average signal magnitude and threshold value calculated from all noise medium.

5.1. Obtaining Ambient Noise Floor:

Obtaining JSS is difficult because they are embedded in regular network signals. So that JSS makes use of ambient noise floor which is the sum of jamming signals and white noise and it is represented as follows: PN = PJ + PW
Where, PJ is Jamming signal strength and PW is white noise which includes thermal and atmospheric noise.

Estimating Strength of Jamming Signals:

For getting JSS, our method involves sampling of ambient noise values either the channel is at rest or not. For every node, there will be n measures of ambient noise at fixed rate, denoted as s={s1,s2,,,,sn}. These measuring set s can be categorized into two subsets(s=saUsc).
1)sa={si|si=PJ},when the jammers are active this set contains measurements of ambient noise
2)sc={si|si=PJ+PC}, if jamming signals(PJ) and sender signal(PC) are present, this set contains ambient noise floor.
Finding JSS is equal to obtain the average value of ambient noise floor nothing but mean(sa). In some cases like sc ≠Ø and sa C s. And in some cases sc ≠Ø and sa C s. where no sender has ever transmitted packet in whole process of getting n measurements, The algorithm for calculating the ANF should be able to cope with both cases.

Algorithm 3:Obtaining the Ambient Noise Floor (ANF)

Procedure MEASUREJSS
S = { *S1*, *S2*,……. *Sn*} = MeasureRSS( )
if var(s) < varianceThresh **then**
sa = s
else
JssThresh = min(s) + α[max(s) – min(s)]
α Є [0,1]
sa = {Si | Si < JssThresh, Si Є s}
end if
return mean(sa)
end procedure

The above algorithm obtains ambient noise floor. RSS is nothing but received signal strength which is the mostly used localization measurement. A regular node will have n measurements of ANF. If there are no sender at the time of measuring, we consider ANF as average of all measurements, else ANF is the average of sa which can get by filtering sc from s. The difference between two cases is that if jamming signals are present, then variance of n measurements is small, else ,if various senders transmit then ambient noise will vary. To get the value of sa, the upper bound i.e JssThresh of sc is the percentage of amplitude span of ambient noise measurement.

6.BEST ESTIMATION:

Here, jammer localization issue can be viewed as an optimization problem and getting a good estimation of jammer's position which is equal to get the solution which decreases the evaluation feedback metric. Here, a relationship between estimated location and true location of jammer shows that greedy algorithms is not able to get the global optimal value. So that, some of the heuristic search methods are used which gives global optimum by not diverting to a local minima. Some of the heuristic search methodologies are as follows: Heuristic method is a searching technique which gives global optimum solution.

6.1.Genetic Algorithm:

GA finds a global finest solution by minimizing the method of normal choice. Iteratively produces a number of solution called as "population". For every iteration a new solution is obtained. Here searching for best estimation of jammer location, a new solution obtained is ez. The smaller ez is better.

6.2.Generalised Pattern Search:

Generalized Pattern Search verifies a number of solutions around the current solution and look for the smaller one from the current solution. Now, the one which is smaller is now new solution.

6.3.Simulated Annealing:

Simulated Annealing finds for the better solution by the method of heating a method by the physical process and temperature can be controlled by lowering to decrease the defects. For every iteration, Simulated annealing compares current solution with newly generated one.
The GPS involves searching for a better solution using a fixed pattern, while GA and SA generates new solutions at each iteration. Here, we utilize centroid localization algorithm to improve the accuracy of localization. By using this method we increase the efficiency, packet delivery ratio and decrease packet loss, energy spent and delay.

6.4.Centroid Localization:

In case of jammer localization ,the target node is the jammer, and the neighboring nodes of the jammer are jammed nodes. This method collects all coordinates of jammed nodes, and finds average of their coordinates as the estimated location of jammer. Consider that there are N jammed nodes(X1,Y1),(X2,Y2),…(XN,YN),the location of jammer can be estimated by
(XJammer,YJammer)=(∑i=1 to N Xi)/N,(∑i=1 to N yi)/N

6.5.Localizing Jammers by Average:

Finally to localize the jammer with more accuracy we will take the average of (Xj,Yj) with less ez and (Xjammer, Yjammer) calculated by centroids localization. By taking the average of these two values the jammer's location can be identified with more accuracy.
(Xi,Yi)={(Xjammer+Xj)/2,(Yjammer+Yj)/2}

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 32 – 36 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp07.pdf

7.RESULT:

When compared with the previous existing schemes ,the current schemes gives high accuracy by knowing the true position of the jammer. At a time multiple jammers can be identified. The hybrid approach which uses heuristic methods and centroid localization gives us exact position of jammers so that by identifying jammer position packets can be transferred from source to destination with security.

8. CONCLUSION:

Here, we represented the problem of identifying jammers in wireless networks, aiming to widely decrease estimation errors so that communication between source and destination can be made securely. A best estimation method for locating the position of jammers in wireless networks is used which exploits the jamming signal strength (JSS).Our goal is aiming to extensively reduce estimation errors using an evaluation feedback metric which uses ambient noise floor ,which is the sum of all unwanted signals freely available from many devices. From this estimation approach, we can correctly obtain the JSS from the measurements of ambient noise floor. Here, heuristic search algorithms such as genetic algorithm, generalized pattern search, simulated annealing are used. In particular, we combined the centroid based localization with the existing estimation approach. By combining these two methods we can achieve the better result to locate the jammer in wireless 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] 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.

[4] T. Cheng, P. Li, and S. Zhu, “Multi-Jammer Localization in Wireless Sensor Networks,” Proc. Seventh Int’l Conf. Computational Intelligence and Security (CIS), 2011.

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

[6] Z. Liu, H. Liu, W. Xu, and Y. Chen, “An Error-Minimizing Framework for Localizing Jammers in Wireless Networks,” IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, pp. 508-517, Feb. 2014.