International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 12 4172 - 4175

Detection And Localization of Wireless Jammer

Ms. Swati Shripati Kadam
M.E. (E&TC)
KIT's College of Engineering
Kolhapur, India.
swatikadam89@gmail.com

Prof. Y. M. Patil
H.O.D. Electronics Engineering
KIT's College of Engineering
Kolhapur, India.
ymp2002@rediffmail.com

***Abstract*—** In recent years, wireless technology has become more advanced, popular and affordable. Because of this broad class of new applications such as traffic monitoring, patient tracking, patient monitoring, video conferencing, video surveillance cameras monitoring of places like public buildings, banks, malls, railway stations etc has increased which utilizes wireless networks. These applications are totally depends on wireless communication for their successful deployment. Security is most important issue to avoid nuisance in both routine and critical communications services. One threat for the security of wireless network is jamming attack. Jamming attacks can severely affect the performance of Wireless Networks due to their broadcast nature. The most reliable solution to reduce the impact of such attacks is to detect and localize the source of the attack. This will help to take further security actions. This project aims to find the location of wireless jammer by simulation method using MATLAB software.

Keywords- *Jamming; Jammer detection; Jammer localization.*

*****

I. INTRODUCTION

The wireless network rapidly becomes more advanced and increases new applications utilizing wireless networks which are more popular and affordable for example health monitoring, fire detection, traffic monitoring system surveillance cameras monitoring of some places like public buildings, banks, malls, railway stations etc. To ensure the successful deployment of these pervasive applications, the dependability of the wireless communication becomes important. Security is a main concern of these applications. One threat which is especially harmful is jamming attacks. Jamming attacks can severely affect the performance of Wireless Networks due to their broadcast nature. The wireless jammer continually emits a radio signal along the same frequency that wireless nodes uses. Jammer does not wait for the channel to become idle before transmitting. Jammer can effectively prevent legitimate traffic sources from getting hold of channel and sending packet. Jamming technology generally does not discriminate between desirable and undesirable communication. A jammer can block all radio communication on any device that operates on radio frequencies within its range (i.e. within a certain radius of the jammer) by emitting radio frequency waves that prevent the targeted device from establishing or maintaining a connection. Jammers are more than just a nuisance; they pose an unacceptable risk to public safety by potentially preventing the transmission of emergency communications. Wi-Fi jammers maliciously disrupt both routine and critical communications services.

Sometime jamming is very important for security purpose. Somewhere it is legal to use for example at petrol/ Gas station, theatres, lecturer hall, government office and some secured places etc. That means it could be legal. It could be illegal. It has advantages and disadvantages both. The main motto of my project is to find the location of jammer which intentionally jams the area. For example a jammer can be used with bad intention in bank robberies, ATM, disturbance in traffic monitoring system, Military, Medical applications. Jammer maliciously disrupts communication and create nuisance. To avoid this first step is to detect and find the location of jammer. Finding the location has great importance for restoring the normal network operation and taking further security action. The purpose of a jammer is to influence the channel quality between a node and its neighbors. A node losing its sending ability is a clear sign that it is being jammed, a weak reception capability i.e. a low packet delivery ratio (PDR). PDR defines 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. PDR and signal strength are powerful measurements which is capable of detecting jamming scenario.

The remainder of this paper is organized as follows. In section II, describe jammer detections methods. In section III presents the assumptions that our system makes and section IV introduce jamming localization scenarios. Lastly, we conclude in section V.

II. DETECTING JAMMING ATTACKS IN SENSOR NETWORKS:

Detection of wireless jammer is important to find out the cause of disturbance in the legitimate communication. There are two methods of detecting jamming attacks

A. Signal Strength

In this method, measurement of signal strength is important because the distribution of signal strength is affected by presence of jammer. This is accomplished by measuring channel's received energy level at different times and collect N of these samples to form a window of samples. The average of signal strength window of N samples shows the effect of jammer on signal strength.

For example if constant jammer is present then average signalstrength value could be constant over the period of time, as shown in Fig 1. We can discriminate normal traffic scenario and constant jammer received signal scenario [5, 8].

 ISSN: 2321-8169
4172 - 4175

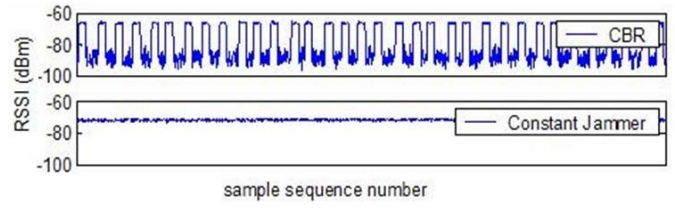

Figure 1. RSSI reading as a function of time.

B. Packet delivery Ratio (PDR)

Jamming attack will degrade the channel quality surrounding a node. A jammer may not only prevent a wireless node from sending out packets, but may also corrupt a packet in transmission. If the PDR is low then there is possibility of presence of jammer. To confirm presence of jammer more accurately both signal strength and PDR measurement methods apply simultaneously [5].

III. LOCALIZATION OF WIRELESS JAMMER

In this project MATLAB R2013a (8.1.0.604) software is used for simulation. Here, we focus on Localization of wireless jammer. We have some assumption to design the problem as features of simulation.

Features of simulation

- Location unaware nodes
- Nodes are stationary
- Each node has omni-directional antenna
- Jammer is a constant jammer
- Jammer is stationary and has omni-directional antenna
- Jammer is placed randomly in wireless network

In this work, we focus on locating a jammer after it is detected. Thus, we assume that jammer is already present. Jammer is placed randomly at fixed position in the simulation area and it is surrounded by multiple network nodes. We know that jammer deny receiving the packets within their range and it more effective on the nearest nodes which are very closely located to the jammer. They cannot send and receive even a single packet. The nodes which are away from the jammer have lesser effect of jammer on them. Thus the PDR ratio increases as the distance between node and jammer increases.

After plotting of jammer and wireless node, divide the network nodes under jamming attacks into the following three categories as shown below in Fig 2, [2],

- Unaffected node –These nodes are out of the range of jammer. They don't have any effect of jammer.
- Boundary node – These nodes are in the range of jammer but partially jammed. They can send/ receive some packets
- Jammed node – These nodes are in the range of jammer and very closely located to jammer. They can not send and receive packets. Hence, PDR ratio of these nodes is approximately equal to 0

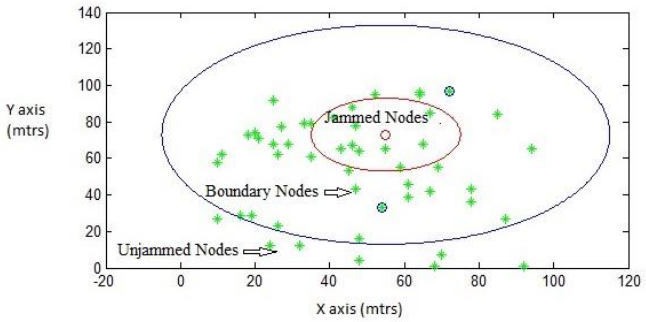

Figure 2. Divide the network nodes in three categories.

After dividing the nodes estimate the location of jammer in next section. Localization Scenario below.

IV. LOCALIZATION SCENARIO

Two scenarios are used to estimate the location of wireless jammer more correctly [1],

A. Jammed nodes

In this scenario, two jammed nodes are selected randomly as shown in Fig. 3. Both nodes cannot send and receive packets. These nodes find the location of jammer by using signal strength analysis. Low PDR does not mean low signal strength. This may be possible in neighbor failure case but in jammed case signal strength should be high towards jammer direction. First, jammed node rotates the node antenna and measures the signal strength in every direction at angle 0 to 360 degree. Then, node will find the maximum signal strength direction. This procedure is repeated for second node and second jammed node also finds the direction of maximum signal strength.

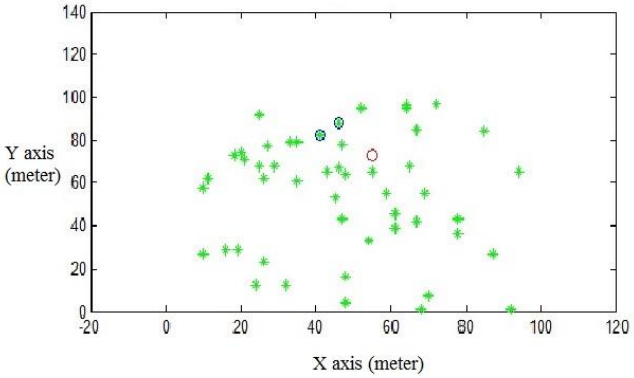

Figure 3. Random selection of jammed nodes.

The direction of maximum signal strength considered as direction of jammer from that node. There are two direction lines which get intersect at a point. This intersection point is location of wireless jammer; see in Fig. 4,

Co-ordinates of jammer position is calculated by linear equation of straight line.

Equations of straight lines for two nodes

Node 1: $y1= m1x1+b1$

Node 2: $y2=m2x2+b2$

We know,

$m1= \tan \theta 1$

$m2= \tan \theta 2$

Therefore,

b1 and b2 will calculate

At the point of intersection they will both have the same y-coordinate value, so we set the equations equal to each other:

m1x+b1 = m2x+b2

Therefore, the coordinates of jammer,

x = (b2- b1)/ (m1- m2)

y = mx + b.

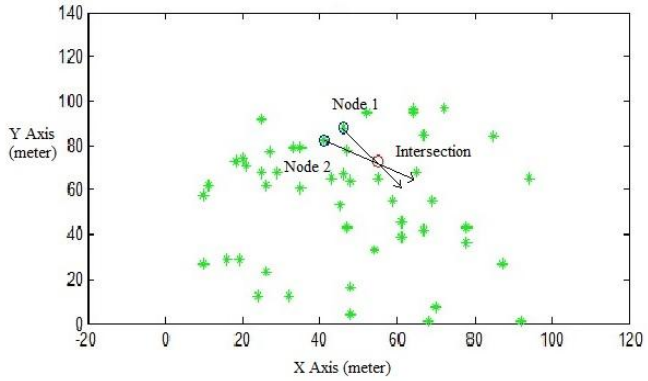

Figure 4. Intersectionof two jammed nodes.

B. Boundary nodes

In this scenario, two boundary nodes select randomly as shown in Fig. 5.

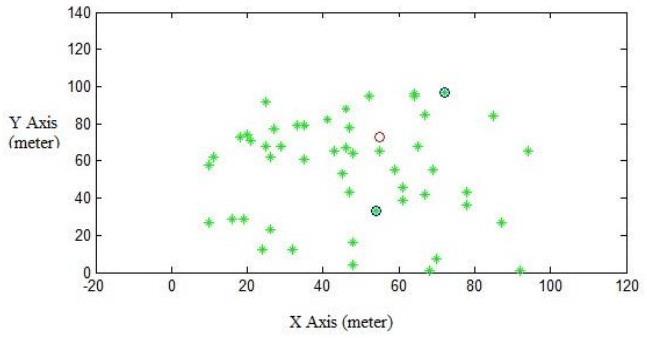

Figure 5. Random selection of boundary nodes.

Both nodes partially jammed. These nodes can send and receive some packets. So here localization of wireless jammer is done by PDR measurement. PDR of nodes is directly proportional to the distance between node and jammer when jammer is ON. In this simulation program PDR increases constantly with distance which practically may not happen because PDR depends on other environmental conditions also. PDR value gives the distance between node and wireless jammer. By selecting two nodes calculate the distance between node and jammer with the help of PDR of that respective node. From that we get two radius of two nodes having the two intersects and one of that intersect is jammer position as shown in Fig 6.

Then, how could finalize exact position of jammer from that two intersect. Here we use reference of position value calculated by signal strength measurement in jammed scenario. The intersect value which is close to position value of jammer calculated by signal strength and is our estimated location of jammer.

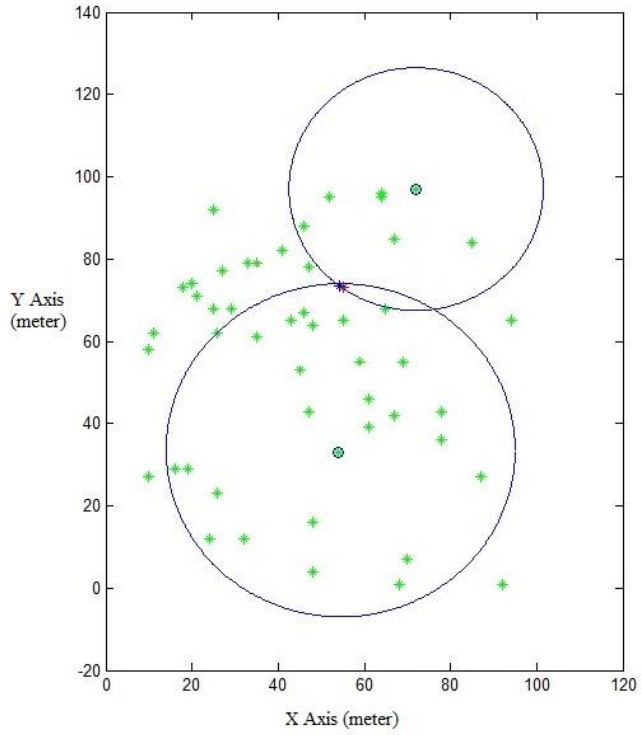

Figure 6. Localization of wireless jammer by boundary nodes

V. CONCLIUSION

Wireless sensor and ad hoc networks using distributed wireless technology are used in many applications, such as Tactical operations, Rescue missions, Commercial use and Education. Due to their nature, wireless network is vulnerable to jamming attack. To avoid nuisance and for further security option detection and localization is important. In this paper we studied, the detection of wireless jammer by signal strength and PDR analysis which shows signal strength should be high and PDR is low when jammer is present.

In this study, we have proposed localization of wireless jammer. Localization is done by jammed nodes and Boundary nodes scenario. Jammed nodes locate the wireless jammer with the help of signal strength analysis and boundary nodes locate the wireless jammer by PDR analysis.

VI. ACKNOWLEDGMENT

I would like to express the deepest gratitude to my guide professor Y M Patil, HOD of Electronics department that without their help, this project would not possible. He has always guided and helping me in successfully completing this project.

VII. REFERENCES

[1] "Catch the Jammer in Wireless Sensor Network" Personal Indoor and Mobile Radio Communication, 2011 IEEE 22nd international symposium by Yanqiang Sun, China.

[2] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Wireless jamming localization by exploiting nodes hearing ranges," in Distributed Computing in Sensor Systems, ser. Lecture Notes in Computer Science, R. Rajaraman, T. Moscibroda, A. Dunkels, and A. Scaglione, Eds. Springer Berlin / Heidelberg, 2010, vol. 6131, pp. 348–361.

[3] W. Xu, Wade Trappe, Yanyong Zhang. Jamming Sensor Networks: Attack and Defense Strategies. Published in IEEE network, volume 20, Spring 2006.

ISSN: 2321-8169
4172 - 4175

[4] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, ser. MobiHoc '05. New York, NY, USA: ACM, 2005, pp. 46–57

[5] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In Proceedings of the 2004 ACM workshop on wireless security, pages 80 – 89, 2004.

[6] H. V. Poor. An introduction to Signal Detection & Estimation. Springer Verlag 2 edition 1994.