Detection and Localization of Wireless Jammer using XBee module

Miss 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*—** Now days, wireless technologies has becomes more popular and affordable. In every field e.g. government sector, education, business, military, medical etc. use of wireless network have been increased which enables broad class of new applications. These applications make work easier and faster but one threat which is harmful i.e. jamming attack. The wireless jammer continually emits a radio signal along the same frequency that the wireless nodes use. 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 which create nuisance in our critical communication services. Most reliable solution to avoid nuisance is detection and localization of wireless jammer which helps to take further security actions. This project aims to detect wireless jammer and find the location of wireless jammer by experimental setup.

Keywords- *wireless jammer; detection; localization.*

*****

I. INTRODUCTION

Wireless technologies becomes more advanced because of broad class of new applications increases which utilizes wireless networks, such as patient tracking and monitoring via sensors, traffic monitoring through vehicular ad hoc networks, and emergency rescue and recovery based on the availability of wireless signals. To ensure the successful deployment of these pervasive applications, the dependability of the wireless communication becomes utmost important. One threat that is especially harmful is jamming attacks. Jamming attacks can severely affect the performance of Wireless Sensor 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. The wireless jammer continually emits a radio signal along the same frequency that wireless nodes uses. 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 by emitting radio frequency waves that prevent the targeted device from establishing or maintaining a connection.

For example Jammer can:

- Avoid cell phone from making or receiving calls, text messages, and emails.
- Avoid Wi-Fi enabled device from connecting to the Internet.
- Avoid GPS unit from receiving correct positioning signals.

Jammers are more than just a nuisance; they create 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 e.g. at petrol/Gas station, theatres, lecturer hall, some secured places etc. This means it could be legal. It could be illegal also at some places. It has advantages and disadvantages both. The main motto of my project is to find the location of jammer which intentionally jams the area. e.g. the jammer used in bank robbery, ATM, traffic monitoring system, Military, Medical etc. Jammer maliciously disrupts communication and create nuisance. To avoid such malicious activities, detection and finding location of jammer is necessary. Finding the location has great importance for restoring the normal network operation and taking further security action. There are three scenarios used to detect wireless jammer. These are signal strength packet delivery ratio and carrier sensing time [5]. In this project, we detect and localize the jammer with the help of PDR. Existence of jammer is affects on PDR value. 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 [1,3]. We made hardware setup for that which contains transmitter, receiver and wireless jammer.

II. EXPERIMENTAL SETUP

In experimental setup, hardware contains:

- Two wireless nodes
- One Jammer.

Here, receiver node detects and localizes the wireless jammer with the help of PDR value measurement. It shows the effect of jammer on PDR value of wireless nodes.

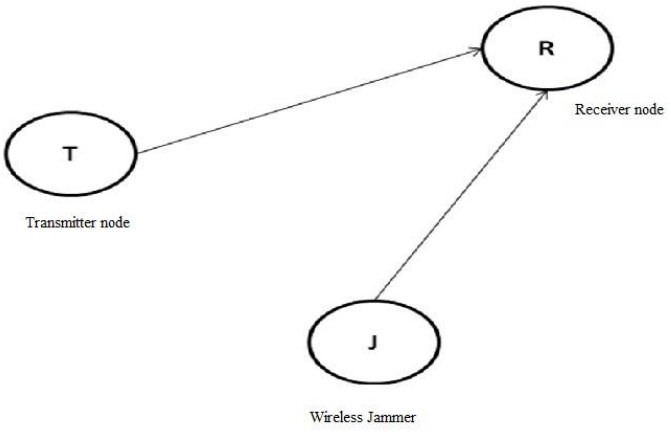

Figure 1. Scematic of hardware setup.

Scenario of Jamming:

- When Jammer is OFF. Then two wireless nodes have reliable communication between them.
- When Jammer is ON. Jammer interrupts into their communication and results in decreasing PDR.

Hardware experimental setup has three devices:

- Transmitter node – It is a device which transmits data in the form of packets towards receiver through the wireless media.
- Receiver node – It is a device which receives data in the form of packets from transmitter through the wireless media. It measures and displays PDR value.
- Wireless Jammer- It is a device which interrupts in communication between these two wireless nodes.

III. CIRCUIT DIAGRAMS AND DESCRIPTION

In this project a hardware setup has three wireless nodes, transmitter, receiver and wireless jammer. Their circuit diagrams and description are as follows.

*A. **Transmitter***

Transmitter is a device which transmit signal at frequency 2.4 GHz to the receiver. For transmission of signal we are using XBee protocol and Atmega 8 microcontroller.

Microcontroller: Atmega 8 is the microcontroller used in transmitter. It is an 8 bit microcontroller based on the AVR RISC architecture.

As shown in Fig.2 Pin no. 1 is reset pin so for proper working of controller reset pin is pulled up to Vcc that's why pin nos. 1and 20 are connected with 10k resister. This microcontroller will digitize the signal and send it to the XBee.

XBee pro S1: It is 2.4 GHz XBee 802.15.4 module. It can communicate up to 100m RF range. XBee shield consist of 3.3V regulator. The entire XBee communication especially pro version communicates at 3.3V power consumption level. It also have few current limiting resisters, LED is used to display whether communication is going on or off. There is a reset circuit in to the XBee. It has two modes XBee and USB which can be used to communicate with XBee and computer. In our case it should be at XBee mode.

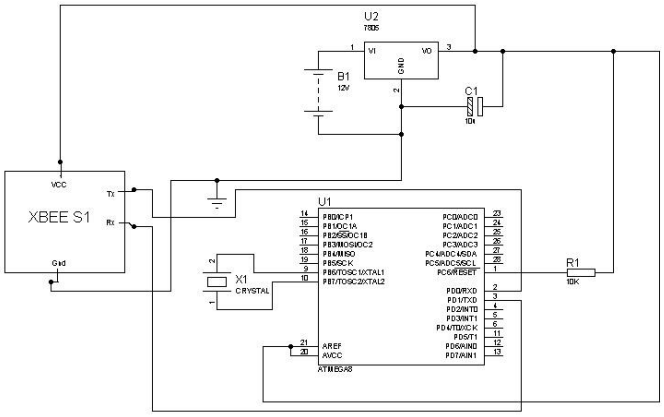

Figure 2. Transmitter Circuit Diagram

Voltage Regulator: Transmitter has battery of 6V but controller runs on 5V so there is another regulator 7805 this convert 6V battery to 5V Vcc and ground level. To filter the any output vibration we have 10µF capacitor. This is electrolytic capacitor which bypasses all AC signal to the ground.

B. Wireless Jammer

Second device is wireless jammer which transmits random data at same frequency of transmitter. This will disturbs the communication between two legitimate nodes. This jammer circuitry is just like transmitter. The circuit diagram of wireless jammer is shown in Fig.3.

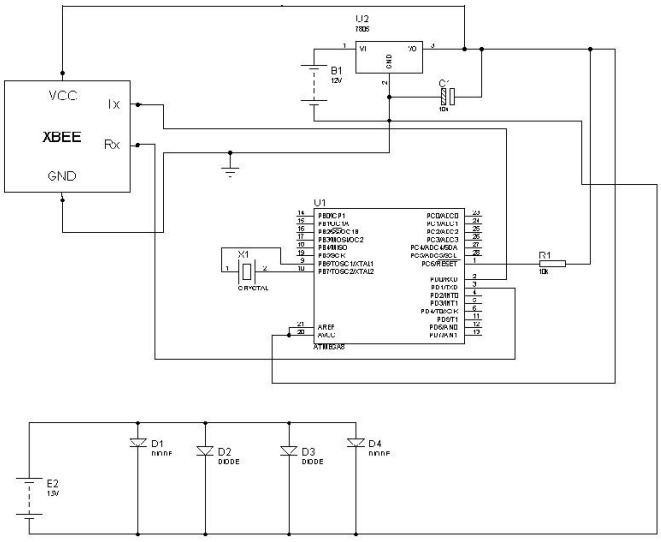

Figure 3. Wireless Jammer Circuit Diagram

It consists of microcontroller Atmega 8, XBee pro S1, voltage regulator. It is same as wireless node but, used to jam wireless node intentionally it continuously emits radio signal. The only difference is infrared LED. These are used for finding direction of wireless jammer which is detected by photo detector placed on receiver. For infrared LED have separate

 ISSN: 2321-8169
365 - 367

battery 1.5V and 5Ah which is directly connecting to 4 LED of 1.5A.

C. *Receiver*

This is wireless jammer detector. It receives the signal coming from transmitter effectively. If there is no any jammer device then it will give approximately 100% PDR value. If jammer is present then PDR value becomes low. If jammer is very close to the receiver then PDR value is approximately zero. Low PDR value implies jammer is present in the range of receiver node, then with the help of RSSI value receiver calculates approximate distance between jammer and receiver node. Receiver also has almost same circuitry like transmitter and jammer as shown in Fig. 4 below.

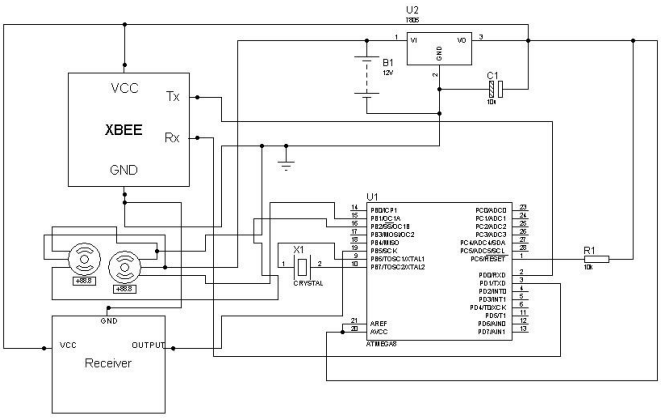

Figure 4. Receiver Circuit Diagram

Only difference is servo motors and photodetector. We have mounted a LCD to display PDR value, distance (between jammer and receiver node) and angle at which jammer may be present. Circuit vise all the connections are same. Pin 19 goes to detector circuit consisting of photodiode which detects transmission of infrared LED. Servo motors are connected to pin 15 & 16. Servos require 6V & 4.5A power supply. Each servo motor rotates 180 degree. One servo motor is mounted on the second servo motor so that it completes total 360 degree rotation. Servo motors rotates every 1 min to find the direction of jammer which is displayed on LCD.

IV. CONCLUSION

We studied detection of wireless jammer with the help of PDR and signal strength measurement, and then localize the jammer by using XBee protocol in hardware setup.
With the hardware setup, we detect the jammer and observe effect of jammer on PDR value of wireless node.

V. ACKNOWLEDGMENT

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

VI. REFERENCES

[1] “Detection and localization of wireless jammer” in International Journal on Recent and Innovation Trends in Computing and Communication Volume 2 Issue 12, 2014, Page No.: 4172 - 4175.

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

[3] 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.

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

[5] 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