Detecting Jamming Attacks for IEEE 802.11b Wireless Networks

By

Nadeem Sufyan
2009-MS-PhD-IT-23

Supervisor

Dr. Nazar Abbas Saqib

Department of Electrical Engineering

Submitted to the Department of Computing, School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad in partial fulfillment for the requirements of a M.S. Degree in Information Technology

November 2012

ABSTRACT

Wireless local area networks are used in domestic, commercial and military application. Among different wireless protocols, IEEE 802.11b is the most prominent one. Due to broadcast nature, wireless networks are vulnerable to malicious attacks. Up to certain extent, robust transmission is achieved using channel coding and forward error correction schemes employed by protocol in presence of noise and interference. However, detection of attacks on IEEE 802.11b wireless networks is necessary due to their severe impact on the network performance. Among various malicious attacks, jamming attacks are the most prominent one. The attacks on the radio signal could be protocol aware or protocol independent. Since jamming attacks drastically affect the performance of wireless networks, an effective mechanism is required to cope up with them. We investigate a multi-modal scheme to detect several jamming attacks. This proposed scheme is based on generating profile under different jamming attacks during training session. Our proposed model generates jamming profiles. The profiles generated in detection model are based on packet delivery ratio, signal strength variation and pulse width of the received signal. The model works for both protocol-aware and protocol unaware jammers. We have attempted the proposed model in several jamming scenarios. The achieved results demonstrate a significant improvement in the detection ratio.

Approval

It is certified that the contents and form of the thesis titled **"Detecting Jamming Attacks for IEEE 802.11b Wireless Networks"** submitted by Nadeem Sufyan have been found satisfactory for the requirement of degree.

Advisor: Dr. Nazar Abbass Saqib

Signature: ____________________

Date: ________________________

Committee Member: Dr. Syed Ali Khayam_

Signature: ____________________________

Date: ________________________________

Committee Member: _Dr. Fauzan Mirza___

Signature: ____________________________

Date: ________________________________

Committee Member: Madam Ayesha Saleem

Signature: ____________________________

Date: ________________________________

Certificate of Originality

I hereby declare that this submission titled “**Detecting Jamming Attacks for IEEE 802.11b Wireless Networks**” is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or any other education institute, except where due acknowledgment has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project’s design and conception or in style, presentation and linguistic is acknowledged.

Author Name: Nadeem Sufyan

Signature: ________________

ACKNOWLEDGMENTS

First of all thanks to **Allah** almighty; for making my task easier for me. WHO gave me courage whenever I was in need.

Thanks to my **Family** for their love, support and prayers all the time in thick and thin.

I owe my deepest gratitude to my research advisor **Dr. Nazar Abbas Saqib** for his support, guidance and help not only in academic area but also related to other issues, I faced during the time I worked with him on my thesis. One simply could not wish for a better or friendlier supervisor than him.

I am also thankful to my Committee members **Dr. Syed Ali Khayam, Dr. Fauzan Mirza** and **Ms. Ayesha Bint Saleem** in helping me and sparing time for me

I am also very thankful to my friends in SEECS for providing me help in understanding and resolving many of my research issues.

Last but not least, I am highly obliged and grateful to **WISENET & CEFAR LAB** that provided me scarce Lab resources and helped me time to time in number of ways.

LIST OF FIGURES

Contents

1 INTRODUCTION

2 BACKGROUND

3 LITERATURE REVIEW

4 EXPERIMENTAL SETUP TOOLS AND TECHNOLOGIES

5 EXPERIMENTS AND ANALYSIS OF RESULTS

6 MATHEMATICAL MODEL FOR DETECTION

7 CONCLUSION AND FUTURE WORK

CHAPTER 1

INTRODUCTION

1.1.Introduction

IEEE wireless LAN has gone through many changes since its inception. Various versions (list of alphabets) have been appended to 802.11 to depict various changes that it has come across. Different versions deal with different issues. Security and authentication of sensitive data on air medium are prominent ones. However, these are not the only issues. Jamming is one of the challenges in wireless medium. The easiest way of disturbing a wireless communication is by generating a high power noise across the entire bandwidth near the transmitting and/or receiving nodes. The device that generates such a noise is called a *jammer* and the process is called *jamming.* There are various jamming techniques for a wireless medium like constant jammer, deceptive jammer, reactive jammer, intelligent jammer and random jammer. All of these have compromises between detection probability and power usage. Intelligent jamming is one that exploits the loop holes of the wireless protocol being used, here it is 802.11b. Many detection techniques have been proposed in literature but all these suffer from problems of incomplete detection, false alarm rate, partial detection of jamming attack etc. The main reason for this is that they do not consider the impact of different detection parameters on each other and that is why fail to completely detect the jamming attacks.

1.2. Motivation

The wireless networks are of broadcast nature. Due to shared and open nature of wireless channels, they provide limited mobility and convenience. On the other side, they are susceptible to radio jamming attacks and other security issues. There are various solid reasons for detection of such jamming attacks which include the following:

- To identify the regions of poor radio connectivity conditions and therefore, routing around the jammed area or applying recovery techniques or spatial retreats
- To build secure and dependable wireless network
- To detect jamming attack by hostile forces that brings down friendly force network and command and control system

1.3. Problem Statement

The problem statement of the thesis is as follows:

“To detect RF jamming attacks in 802.11b wireless networks and model a proactive multi-modal detection scheme for classification of RF jamming attacks especially protocol aware jamming (intelligent jamming)”

1.4. Thesis Aims and Objectives

The main aims and objectives of this thesis are as follows:

I. Modeling multi-modal detection mechanism for all type of jammers especially protocol aware intelligent jamming attacks in IEEE 802.11b network.

II. Achieving results based on test bed setup. No simulation is performed to get the results

1.5. Thesis Contribution

The main contribution of this work is the classification of different jamming attacks launched by malicious nodes. In this work, a multi-modal detection scheme has been developed. Multi-modal detection scheme is a detection mechanism that is based on more than one detection parameter. It not only caters constant and random jammers but also the protocol aware jammers. Protocol aware jammers can drop packet delivery ratio with relatively smaller pulse width and lesser detection probability. It accounts for different data transmission rates and observes behavior of concerned parameters.

1.6. Methodology

Below is the methodology adopted to solve problem.

I. **Background Study**

Study the protocol under discussion that is IEEE 802.11b. Channel access mechanism by nodes connected using this protocol. Different types of jamming models and metrics used for jamming. Different jamming detection parameters and metrics used for detection.

II. **Literature review and understanding of problem**

Number of existing detection techniques have been studied and tried to find a detector that not only detect all types of jammers but also classify type of jamming attack. All the existing techniques consider only one or at most two parameters to detect a radio jamming attack. Drop in packet delivery ratio (PDR) could be due to congestion or channel fading, jamming is not the only reason. Similarly, signal strength based jammers cannot distinguish between random jamming and constant bit rate (CBR) traffic. Carrier sensing time is found to be another measure for detection of jamming attack but in case of shot noise based jammers, carrier sensing time is not an issue at all but still the receiver gets zero packet delivery ratio (PDR). Observing all the above existing techniques, it is easy to realize that each one is missing necessary information to completely detect jamming attack. No one is successful in detection of radio jamming attack with lowest false alarm rate and high accuracy. Moreover, classification of jammers on the detector side remains a question mark.

III. Proposing a Solution

Keeping all the problems discussed in previous section, there is need of a multi-modal detection scheme. This scheme not only detects different radio jamming attacks for IEEE 802.11b network but also provide classification of these attacks in a multi-dimensional model. The accuracy of these techniques strengthens with the use of multiple relevant detection parameters simultaneously.

IV. Determining appropriate tools and apparatus

This portion of thesis describes the tools and technologies have been used. How the devices are setup and software scripts and software tools used. Since previously, most of the work is performed in simulation environments; our attempt is to perform it in real test bed with actual apparatus.

V. Developing algorithm for jamming detection and mathematical model

In this section, the relation among different parameters is organized in the form of a detection algorithm. The pseudo code of the algorithm is provided. Moreover, a mathematical model is also proposed for classification and detection of various jamming attacks.

VI. Determining impact of signal strength variation on PDR

In case of jamming attack, the drop in PDR is directly related with the disturbance in signal strength and hence pulse width. In this section, we discussed how the three parameters are correlated. Consider signal strength variations when there is no transmission on channel at all, when there is normal transmission and when jammer activated. How the behavior of PDR changes with signal strength and pulse width.

VII. Detecting different jamming attacks and plotting results

In order to classify different jamming attacks, we setup the considered jamming attack models in real test bed environment and launch the jamming attacks. The detector collects the samples in real time and plots it in multi-dimensional model. That not only helps to visually classify the data but also provides insight on the behavior of jamming attack.

1.7. Thesis Organization

Rest of thesis is organized as follow. Chapter 2 describes the background of the thesis. Chapter 3 discusses the literature review and related work in existing techniques. Chapter 4 discusses the detection algorithm, tools and software used in thesis. Chapter 5 provides comparative analysis of the detection results of different jamming attacks. Chapter 6 describes the proposed mathematical model. Chapter 7 is the final chapter of thesis. It concludes the work and setup future directions.

CHAPTER 2

BACKGROUND

The topic of jamming and its detection are discussed in parallel so that reader could have better insight into it. This chapter briefly describes wireless channel, channel access mechanism of media access control (MAC) layer protocol used by IEEE 802.11b standard, different jamming techniques and metrics used for detection of various jamming methods.

2.1. Wireless Channel

There are three ways of communication to transfer information between senders and receiver. 1) Wired medium that is copper wires in which flow of electrons causes' information flow. 2) Optical fiber in which light energy acts as medium of communication and provides highest throughput so far. 3) Wireless medium in which the nodes connected with each other wirelessly and use air as medium of transporting information over electromagnetic radiation.

Each medium has its own pros and cons. Our discussion is limited to the wireless medium. In wireless medium, data travels on electromagnetic waves. These waves are affected by various factors like attenuation, scattering and diffraction caused by environment. First factor attenuation is defined as the loss in signal strength which is measured in decibels (dB). Attenuation or loss in signal strength is higher if distance between transmitter and receiver is higher and vice versa. When there are many physical obstacles on the way of wireless signal, it rebounds many times. This is called reflection. Reflection combined with scattering causes noticeable attenuation in wireless signal. Scattering of signal is caused when a signal strikes a sharp edge and divides into more than two phases, each with different level of attenuation. These signals reach the receiver at different times. It makes difficult for receiver to correctly receive the intended message and interpret it.

2.2. Coding and Modulation

Two communication nodes (transmitter and receiver) represent data as binary sequence of bits on physical layer. Before sending data on communication channel, it is passed through an encoder of data. Purpose of encoder is to add redundancy and parity bits. Redundancy bit is added to recover the original data in case of packet corruption on air due to interference or noise on channel. After encoding, the transmitter performs modulation of the binary sequence. It is last step performed with data at sender side. Modulation is the process of conveying a message signal, for example a digital bit stream or an analog audio signal, inside another signal that can be physically transmitted [14]. Modulation is of different types. For example, binary phase shift keying (BPSK) modulates 1's to one wave form and 0's to other and that is why called Binary Phase Shift Keying. Sometimes, each wave form carries multiple *n* symbols from binary sequence.

When these signals reach at receiver via channel; these are demodulated. Demodulation is reverse process of modulation in which the received signal is converted to binary sequence. This binary sequence is approximation of the originally sent data. This binary sequence is then passed through decoder which is having knowledge of encoding and redundancy, extracts exactly sent data. Table 1 summarizes coding and modulation schemes used at different data rates of IEEE 802.11b.

Data Rate (Mbps)	Modulation	Channel Coding
1	DBPSK	DSSS-11 Barker
2	DQPSK	DSSS-11 Barker
5.5	DQPSK	HR-DSSS/CCK
11	DQPSK	HR-DSSS/CCK

Table1. Channel coding and modulation for IEEE 802.11b physical layer

2.3. IEEE 802.11b

IEEE 802.11b is the first wireless local area networks standard that is heavily deployed on variety of computers specially laptops. Idea of 802.11b was proposed by IEEE in 1999. Soon after that, idea of multiple wireless access points was caught up so that the business people could use it for checking email and surfing internet. After success of wireless networks in business communities, the commercial products became available that established Wi-Fi for a long way to go.

2.4. MAC Layer and Channel Access Mechanism of IEEE802.11b

Since protocol-aware jamming models exploit MAC protocol of 802.11b, it is necessary to understand how it works. MAC layer is based on carrier sensing and media access (CSMA) for collision avoidance (CA). CSMA/ CA works in two modes, 1) Basic mode and 2) RTS/CTS mode.

2.4.1. CSMA/CA Basic Mode

CSMA/CA basic mode of operation is shown in figure 2.1. A node can access the channel at once if a medium is sensed idle for at least the DIFS interval. In case of busy channel, before entering contention phase, node has to wait for DIFS interval. Every contending node chooses a random back off interval within a contention window and delays the access to channel in addition with DIFS. If the node senses the channel busy during its back off timer, it freezes its back off timer, waits for channel to be idle again for DIFS interval. Then it resumes its back off timer until it reaches zero. Here, two conditions apply; node transmits successfully or collides its transmission with other node's transmission. In case of collision, the node backs off again exponentially.

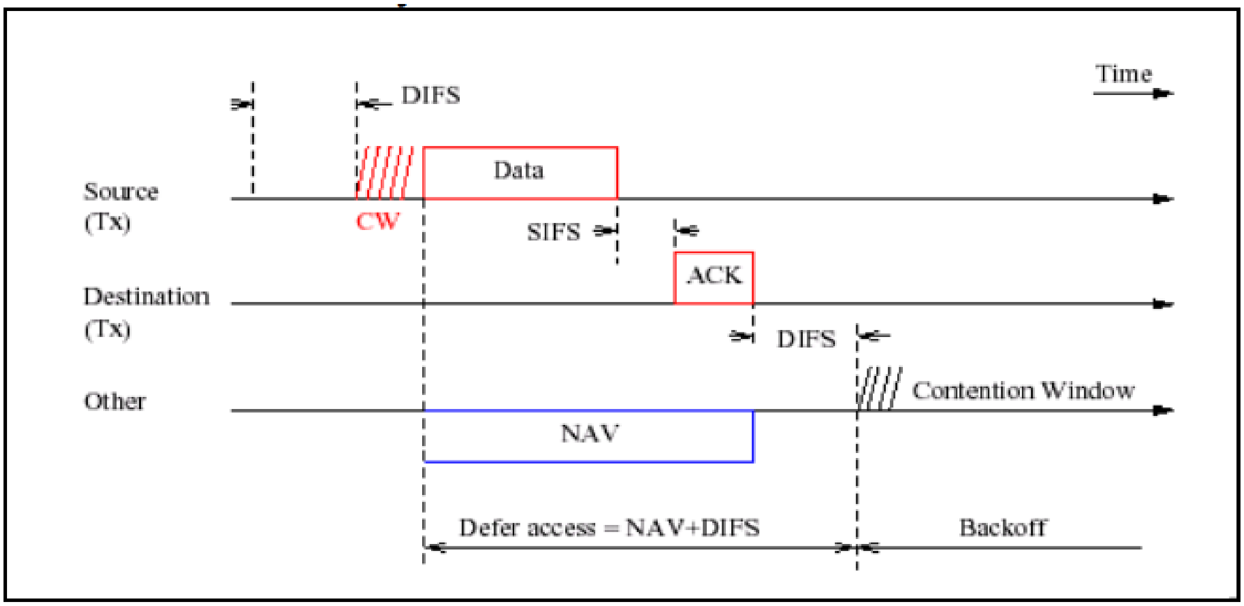


Figure 2.1. CSMA/CA with Basic mode in 802.11b networks [13]

2.4.2. CSMA/CA Virtual Carrier Sensing (RTS/CTS Mode)

Since basic CSMA/ CA could not solve the problem of hidden terminals that occurs when one receiving station can hear two transmitting stations but transmitters cannot hear each other. If both transmitters sense the channel idle and send data simultaneously, collision occurs at receiver. RTS (Request to send) and CTS (Clear to send) is explained in figure 2.2. Exactly like basic mode, after waiting for DIFS and some remaining back off time, the intended transmitter can issue RTS packet. RTS packet structure includes address of intended receiver and duration for which transmission of data plus acknowledgments required. Every receiving node has to set their Network Allocation Vector (NAV) in accordance with RTS duration values specified. This

NAV value specifies after how much time sleeping stations can contend for the medium. Successful RTS is followed by CTS within SIFS where SIFS < DIFS. As soon as the CTS packet received, the transmitter transmits DATA and ACK packets with SIFS interval between each frame. In case RTS is victim of collision, the node backs off exponentially.

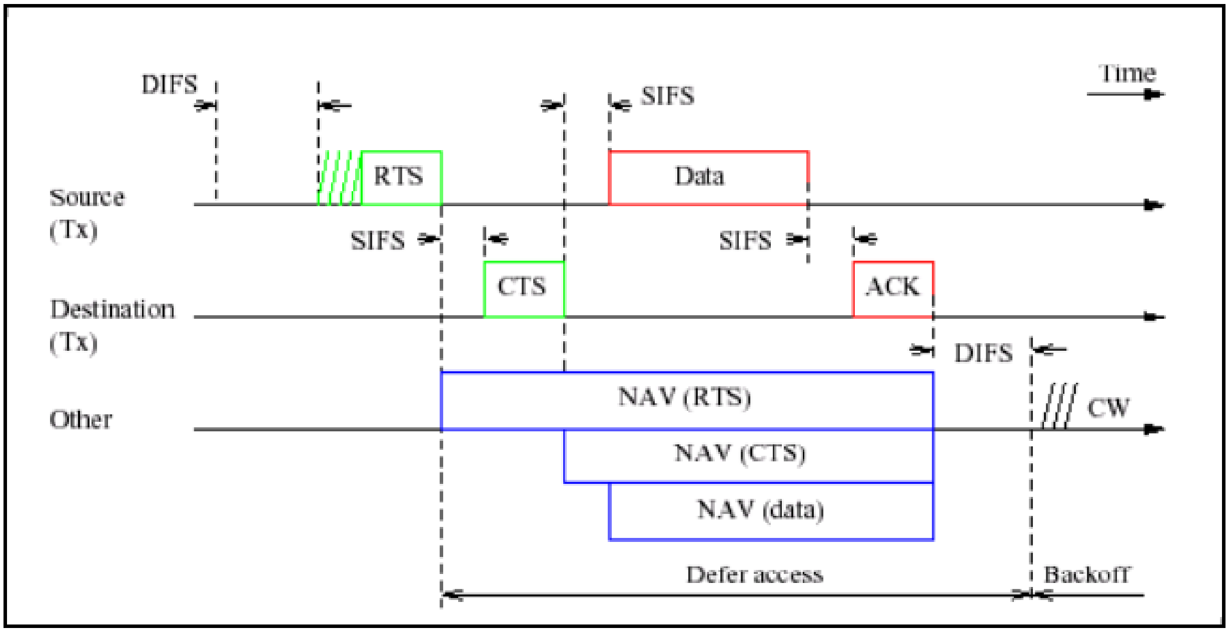


Figure 2.2. RTS/ CTS mode in 802.11b networks [13]

2.5. Jamming Attack Metrics

A jamming attack can be classified based on metrics it is using. Below are few commonly used metrics for jamming attacks:

- Energy conservation to get highest jamming efficiency with least energy used.
- Least detection probability
- Stealthy against detectors.
- Completely denial of service like constant jammers
- Protocol aware so that less likely to detect

- Authentication of users
- Strength against forward error correction (FEC) codes
- Strength at physical layer to beat channel coding techniques

Different type of application addressed depends on different type of metrics. Energy efficiency is the most important metric for all type of jammers and specifically jamming sensor networks for long time. Strong denial of service (DOS) would be critical in battle field where few successful message packets could compromise security. Least probability of detection is desired for jammers if they have to keep for long time in enemy area safely. Strong forward error correction (FEC) codes could be compromised with constant or intelligent jamming. FEC increases resilience of packet against errors.

2.6. Radio Frequency Jamming

Radio jamming is process of transmission of high energy radio signal that disrupts the legitimate communication by decreasing signal to noise ratio (SNR). The transmission could be intentional or unintentional. Intentional is when the operator knows the channel it is interrupting is busy or about to be busy. Hence, deliberately affects the legitimate communication taking place on the radio frequency. We will discuss this type of jamming throughout our work. Unintentional jamming can take place when some equipment like cable TV accidentally radiates on aircraft emergency frequency or microwave oven disrupts wireless network communication. There are various jamming methodologies for a wireless medium like constant jammer, deceptive jammers, reactive jammer, intelligent jammers and random jammers. All of these have compromises between detection probability and power usage.

2.6.1. Constant Jammers [1]

Constant jammer continuously produces high power noise that represents random bits; the bit generator does not follow any MAC protocol and independent of channel sensing or traffic on channel.

2.6.2. Random Jammers [1]

Random jammer operates randomly between sleep interval and jam interval. During sleep interval it sleeps irrespective of any traffic on the network while during jam interval, it acts like constant or reactive jammer. This jammer also does not follow any MAC protocol and there are chances of PDR improvement in case sleep interval increases and packet size decreases.

2.6.3. Deceptive Jammers [1]

These jammers continuously send illegitimate packets on channel so that channel appears busy to legitimate nodes. These jammers are protocol aware and increase carrier sensing time for other legitimate nodes indefinitely. The difference between deceptive and constant jammer is that constant jammers send continuously random bit and deceptive jammers send packets that appear legitimate to the receiver.

2.6.4. Reactive Jammers [1]

Targeting at receiver, reactive jammer activates when it senses any transmission on the channel. In case channel is idle, it remains dormant and keeps sensing the channel. It introduces enough noise in packet on air that packet checksum could not be recovered at receiver side and discarded. Hence causes drop in PDR.

2.7. Metrics for Detection of Jamming Attack

Metrics required for efficient and accurate detection of jamming attack are:

- Low false alarm rate
- Proactive detection
- Least computational cost
- Quick detection

2.8. Parameters for Detection of Jamming Attack

Jammer detection parameters are explained in section below:

Packet Delivery Ratio: It is defined as the ratio of total number of packets correctly received to the total number of packets received. For an environment with noise and interference, PDR could be measured at receiver as the ratio of number of packets received that pass CRC check to total number of packets received. Another way of PDR calculation at transmitter is total number of ACKs received to the total number of packets transmitted.

Packet Delivery Ratio (PDR) = (Correctly received packets) / (Total received packets)

Carrier Sensing Time: The time a station has to wait for channel to get free so that it may start its transmission. Drawback of using this approach is that the carrier sensing time (CST) of different Jammers is less than that in congested scenarios [1].

Signal Strength: The variation in received signal power that detector observes. Signal strength can be used as detection parameter [1]. There are two approaches that are used to characterize, (1) Average value of signal strength within the specific window and (2) spectral discrimination technique.

Detection of jamming attack could not be guessed based on single parameter.

CHAPTER 3

Literature Review

Wireless LANs are vulnerable to jamming attacks due to their broadcast nature. To detect these attacks, it is therefore necessary to understand jamming and its types. In the next sections, we will discuss protocol aware jamming attack models, protocol unaware jamming attack model and then the related work that has been done to detect these jamming attacks.

3.1. Protocol Aware Jamming Attack Models

Intelligent jammers are special type of jammers. These jammers utilize weaknesses of protocol under use. Thus achieve high jamming efficiency with least energy consumption and detection probability. For IEEE 802.11b network in CSMA/CA mode, four types of protocol aware intelligent jammers classified [19] as below:

i. CTS corrupt Jamming
ii. Data corrupt jamming
iii. ACK corrupt jamming
iv. RTS corrupt jamming

Intelligent jammer distinguishes between data and control packets by analyzing the headers of packets. In CTS corrupt jamming, jammer catches RTS packet and after receiving an RTS, it waits for a SIFS interval. After that, assuming corresponding CTS is on the way, sends a short pulse so that CTS is destroyed and have to resend the RTS. Since the CTS packet does not get through, no data is ever transferred. This attack is among the most efficient (energy use) of the methods presented here. This is due to the fact that the jammer actives for only short interval of time necessary to disrupt the CTS packet.

In data corrupt jamming, after receiving a CTS frame, a short pulse is send after a DIFS interval. This destroys data frame and it needs to be retransmitted. In ACK corrupt jamming, after data transmission, jammer waits for SIFS interval and sends a short pulse to corrupt ACK packet. Since the sender never finds an ACK, assuming the DATA has been lost, retransmit it again and again and finally DIFS wait jamming, wherein a short pulse is sent by the jammer after sensing the medium idle for DIFS time to disrupt either an RTS packet or a DATA packet.

Other types of protocol aware jammers include reactive and deceptive jammers (see section 2.6.3, 2.6.4).

3.2. Protocol Unaware Jamming Attack Model

Protocol unaware jammers do not follow any MAC layer etiquettes and transmit jamming pulses irrespective of legitimate transmission on wireless channel. Constant, random and periodic jammers are examples protocol unaware jammers (see section 2.6.1, 2.6.2).

3.3. Literature Review

Packet delivery ratio (PDR) and packet send ratio (PSR) are important measures to detect jamming but PDR may also effect from channel fading, network congestion or any similar issue. Among all the above defined jamming techniques, [7] present idea of shot-noise based intelligent jamming that is most energy efficient and with lesser probability of detection in which the jammer captures the NAV value and hence transmission length. During the packet transmission, the jammer sends a high power pulse with enough width that corrupts enough bits so that FEC would be exhausted. So checksum would not be passed and packet drops. Since the sender would not get the ACK so it will retransmit the packet. The proposed technique has least detection probability and lowest possible energy requirement.

In [8] again PDR is considered as detection parameter. It shows that PDR is 78% under normal network operation. However effects of channel fading, poor link and other could be other causes of drop in PDR. [1] suggests adaptive threshold like in BMAC but it has the drawback of continuously increasing threshold eventually jammer blasting at channel and detector just show the channel idle. Two signal strength measurements are taken into consideration. Basic average for energy detection is not good in case of constant jammer so the technique of spectral discrimination is used which shows that if we use higher order crossing (HOC) then it works for constant and deceptive jammers but cannot distinguish random and reactive jammers. Carrier sensing time is taken another measure as the time a node has to wait for the channel to start its transmission. It is observed that under normally congested network, the CST is greater than random and reactive jammers. Another detection strategy using PDR with two consistency checks that are signal strength consistency check (SSCC) and location consistency check (LCC) proposed in [1]. If signal strength is high then packet delivery ratio must be high while converse is not true. In case of location consistency check, an assumption is made that all nodes in network have their neighbor information from their upper routing layer. If a node observes low PDR, it compares it with that of its neighbor and based on these decides whether the channel is jammed or not. Moreover, the neighboring nodes have to pass location update messages periodically about their new location. This is communication overhead. The effectiveness of methods in [1] is based on the analysis of large amount of data collected in all possible scenarios. Thus they are not designed as real-time method. Another disadvantage is that the jamming detection method and counter-measure are separately considered so that the problems are simplified but the network performances are not optimized. In [2], there is discussion about detection probability and power usage by different jammers. It shows that constant jammer have highest detection probability and highest power usage while intelligent jammers are best for their least detection probability and power usage. In [2], an optimal omniscient jammer is considered that jams ACK with probabilistic model. Moreover, it takes pulse width of 22 micro seconds to jam ACK at data transmission rate of 1 Mbps. However, it is difficult to detect the transmission of ACK due to its short length. Moreover, 22 micro seconds pulse is too long as compared to the length of ACK packet. In [3], intelligent jamming detection is based on a measure of dependence for the case when there is no jamming and when there is jamming. To measure this, statistical correlation is used that is measurement between two random variables. In this case it strongly exists between error and correct reception time. It further computes threshold by mathematical model as well as using multiple simulation for the network. The threshold is defined as the maximum value of slope that any couple of correlation coefficient (CC) and error probability (EP) could have. This correlation is checked with certain predefined error probability (EP) and estimated threshold. If the relation is within the threshold then it is considered non-jammed else it is jammed. However it works in case of reactive jammer that activates when they sense activity on wireless medium.

Fabricated CTS specifying certain amount of NAV duration time to jam the wireless channel has been discussed in [4]. In this way the malicious node forces its neighbors to keep quiet as long as specified in CTS NAV duration field. It investigates the adverse effects of such attacks on channel throughput and delivery ratio and proposes a simple method called address inspection schema (AIS) that uses two-hop neighborhood information. The main idea is to compare the destination field on the CTS frame with the neighborhood information. The targeted node sends a Clear Reservation (CR) message back to all neighbors and all nodes reset their values to previous NAV values. However it uses two-hop neighborhood information that all nodes must maintain using periodic HELLO messages so that freshness of information could be maintained. Also the node getting the fabricated CTS message with its ID as targeting address sends back a Clear Reservation (CR) message. Hence there is communication overhead in this technique. Also this technique suffers from problem of partial detection of jamming, a portion of the network remains jammed and other recovers and works perfectly.

Cell breathing is a new technique discussed in [5] not only for the case of jammers but also for normal network operations to increase the network throughput. The approach works for constant jammers detection and not for intelligent jammers. It is based on number of frames transmitted per total attempts of transmission. If the transmission attempts are above a certain predefined threshold, the node is considered jam. After that jammer detection, cell breathing is used to reduce or increase the transmission power of the access point (AP) so that the jammer may be away from the range of the node. This not only helps in mitigating the jamming attack but also load balance the network throughput.

Since the technique used in [1] suggests collection of large amount of data before analysis, [6] proposes a model based jamming detection technique for wireless networks. Without the need of prior knowledge of the network status, a head station can detect a jamming attack based on PDR observed for certain value of signal to noise (SNR). However under some condition, it is hard to tell whether the drop in PDR is due to network congestion or high SNR value. It then suggests network throughput as a measure of jamming detection. It shows that for given values of SNR and probability of successful transmission, rate of change of network throughput first increases with number of nodes in the network and reaches a peak value and then drops almost like a straight line. It uses expected and observed throughput with margin threshold to detect jamming. However this margin threshold varies with network and environmental parameters and [6] does not suggest any technique to measure it. Once the attack is detected, it uses a self-healing approach based on runtime channel allocation (RCA) algorithm to dynamically assign the most optimal second channel with best switching probability that minimizes transient time to stable state. However this will work for wideband jammers where number of channels with reasonable frequency separation is available.

3.3. Conclusion

Different jamming detection techniques studied in literature survey but they do not solve the problem of complete detection of jamming attacks. Moreover, No one provide classification of different radio jamming models. So there is need of developing multi-modal detection technique that detects all jamming attacks with lower false alarm rate and high precision.

CHAPTER 4

EXPERIMENTAL SETUP TOOLS AND TECHNOLOGIES

Introduction

This chapter includes main detection algorithm, hardware configuration, software installation and software scripts written for test bed. In short it covers setting up complete test bed environment. The section below explains our experimental setup.

4.1. The Detection Algorithm

The proposed detection algorithm is based on three parameters that are packet delivery ratio (PDR), signal strength variation (ΔS) and pulse width (pw). Pseudo code of proposed algorithm is as follows:

Algorithm: Jammer_Detection_And_Classification

```
{ PDR(N) : N ε Neighbors } = Mesure_PDR()
 totalPDR = total { PDR(N): N ε Neighbors}
if  totalPDR < PDRThresh then
    SS = Sample_Signal_Strength()
    ΔS = SS – Normal_Signal_Strength()
    PDR_SSV = Check_PDR_SS_Variation(totalPDR, ΔS  )
    If  PDR_SSV == false then
            Post   Network_Error()
    Elseif
            TT_Symbol = get_Symbol_Transmission_Time()
```

```
      TT_Packet  = get_Packet_Transmission_Time(Packet_Length)
      PW = get_Observed_Pulse_Width()
      If (PW $\leq$  (2*TT_Symbol))
          Post   PA_Intelligent_jammed()
      Else if (PW == TT_Packet)
          Post   Reactive_Jammed()
      Elseif (PW  == Constant_Jammed())
          Post  Constant_Jamming()
      Elseif (PW == Random_Pulse())
          Sleep_interval = get_Sleep_Interval()
              If (Sleep_Interval  < TT_Packet)
                  totalPDR  == 0
              else      totalPDR > 0
end
end
```

4.2. Experimental Setup

4.2.1. The Detector

Detector is a node equipped with Fedora kernel 2.6 and gnuradio-3.4.2 software library. The software defined radio (SDR) supports 802.11b traffic. The detector is attached via USB cable to USRP daughter board RFX 2400. Both hardware, the laptop and USRP kit, accumulatively called detector. Wire shark, a packet capture tool, is also installed on detector machine.

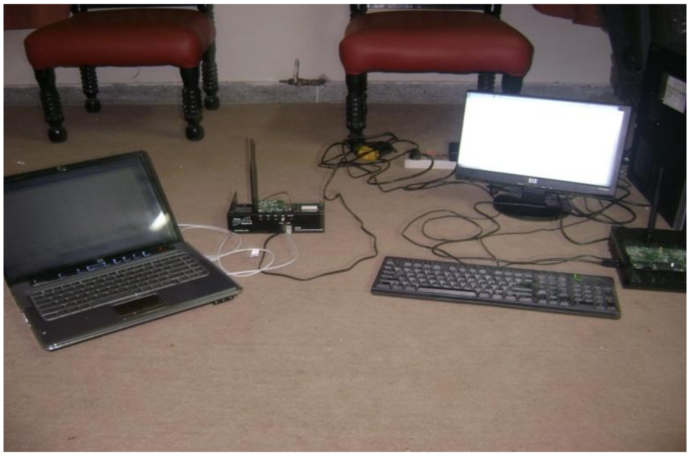


Figure 4.1. (Detector (on left), Jammer (on right))

4.2.2. Wireless Router

We used D-Link 2.4 GHz wireless router dl-514 as a base station. Transmitter and receiver both are connected with the base station to communicate with each other.

Figure 4.2. D-link DL-514 base station

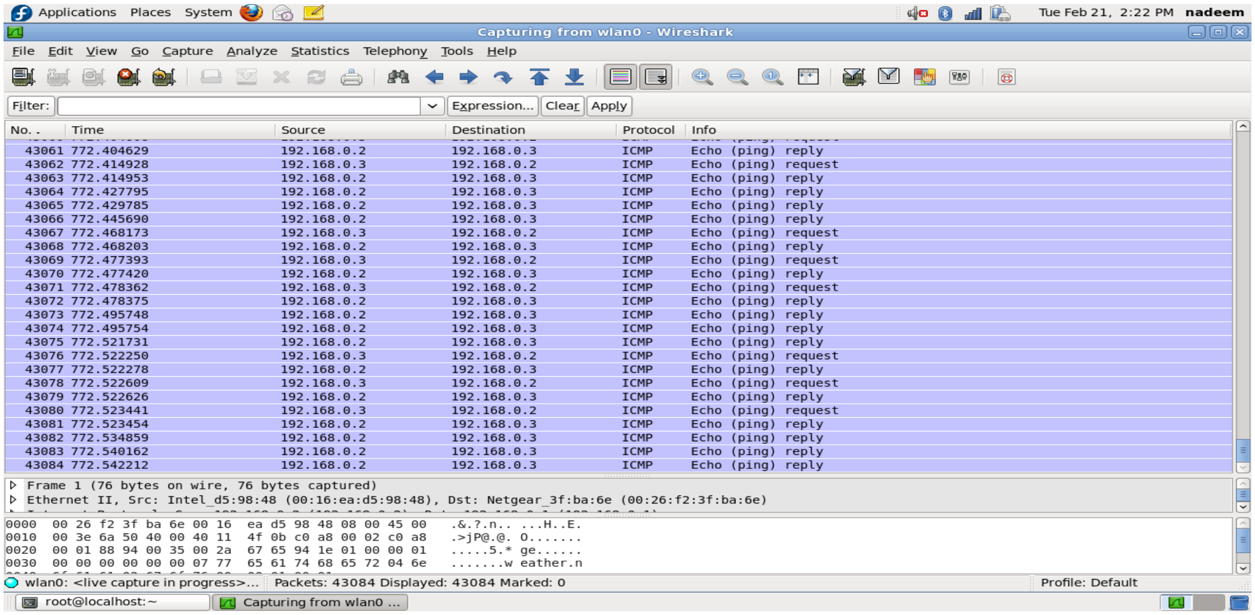
4.2.3. Transmitter

Transmitter of 802.11b traffic is a laptop computer with PCMCIA slot. For perfect 802.11b traffic, DWL-650 PCMCIA wireless card has been used. The transmitter is installed with Fedora 12.86 operating system with kernel 2.6 automatically detects the wireless card drivers. However, for Linux operating system with kernel version lower than 2.6, installation and configuration could be found at [15]. The card parameters are set for data rates of 11Mbps, 5.5Mbps and 2 Mbps using native Linux commands.

Figure 4.3. D-link DWL-650 PCMCIA network interface card

4.2.4. Wire Shark

Wire shark is network traffic capturing tool designed for network layer. It captures all the traffic that is on air and analyzes it. Basically it measures packet delivery ratio (PDR) in a pre-defined capture window. We computed the PDR by taking the difference of number of packets sent by a transmitter with number of packets correctly received at the receiver.



No.	Time	Source	Destination	Protocol	Info
43061	772.404629	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43062	772.414928	192.168.0.3	192.168.0.2	ICMP	Echo (ping) request
43063	772.414953	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43064	772.427795	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43065	772.429785	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43066	772.445690	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43067	772.468173	192.168.0.3	192.168.0.2	ICMP	Echo (ping) request
43068	772.468203	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43069	772.477393	192.168.0.3	192.168.0.2	ICMP	Echo (ping) request
43070	772.477420	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43071	772.478362	192.168.0.3	192.168.0.2	ICMP	Echo (ping) request
43072	772.478375	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43073	772.495748	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43074	772.495754	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43075	772.521731	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43076	772.522250	192.168.0.3	192.168.0.2	ICMP	Echo (ping) request
43077	772.522278	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43078	772.522609	192.168.0.3	192.168.0.2	ICMP	Echo (ping) request
43079	772.522626	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43080	772.523441	192.168.0.3	192.168.0.2	ICMP	Echo (ping) request
43081	772.523454	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43082	772.534859	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43083	772.540162	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply
43084	772.542212	192.168.0.2	192.168.0.3	ICMP	Echo (ping) reply

```
▷ Frame 1 (76 bytes on wire, 76 bytes captured)
▷ Ethernet II, Src: Intel_d5:98:48 (00:16:ea:d5:98:48), Dst: Netgear_3f:ba:6e (00:26:f2:3f:ba:6e)
```

```
0000  00 26 f2 3f ba 6e 00 16  ea d5 98 48 08 00 45 00   .&.?.n.. ...H..E.
0010  00 3e 6a 50 40 00 40 11  4f 0b c0 a8 00 02 c0 a8   .>jP@.@. O.......
0020  00 01 88 94 00 35 00 2a  67 65 94 1e 01 00 00 01   .....5.* ge......
0030  00 00 00 00 00 00 07 77  65 61 74 68 65 72 04 6e   .......w eather.n
```

```
wlan0: <live capture in progress>...  Packets: 43084 Displayed: 43084 Marked: 0          Profile: Default
```

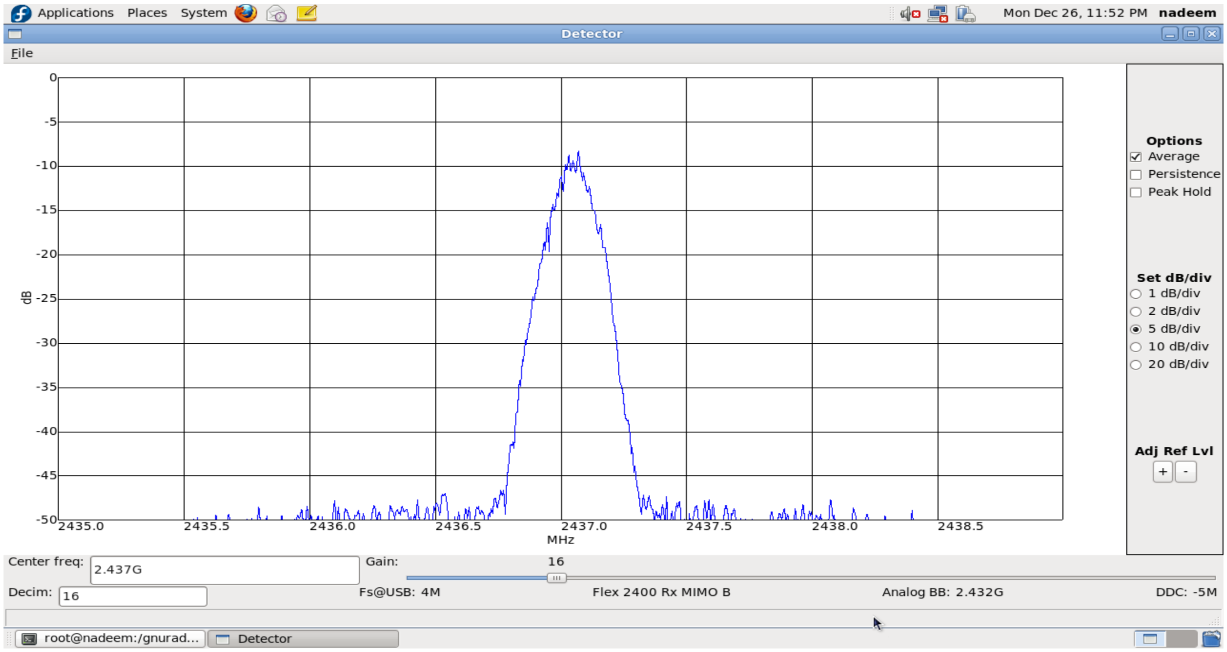
Figure 4.4. Packet capture through Wire shark

4.2.5. GNU Radio

GNU radio is software library that is combined with minimal hardware of USRP to generate, transmit and receive customized waveforms and signals. It provides fine-grained control over hardware via software. Python language scripts are written to achieve the desired results. The library could be configured on Fedora and Windows operating systems. We have configured it on Fedora 12.86.

4.2.6. Python Scripting

In order to measure the impact of jammers on channel, we wrote different scripts in Python. These scripts developed on GNU Radio library that installed on both jammer and the detector. Jammer script is used to create different jamming models. Detector script monitors the signal strength variation at every micro second and saves it to local disk file. Further processing is done on this file to generate the results. The output of these scripts is shown in figures (4.5, 4.6).



☑ Average
□ Persistence
□ Peak Hold

○ 1 dB/div
○ 2 dB/div
● 5 dB/div
○ 10 dB/div
○ 20 dB/div

Center freq: 2.437G

Gain: 16

Decim: 16

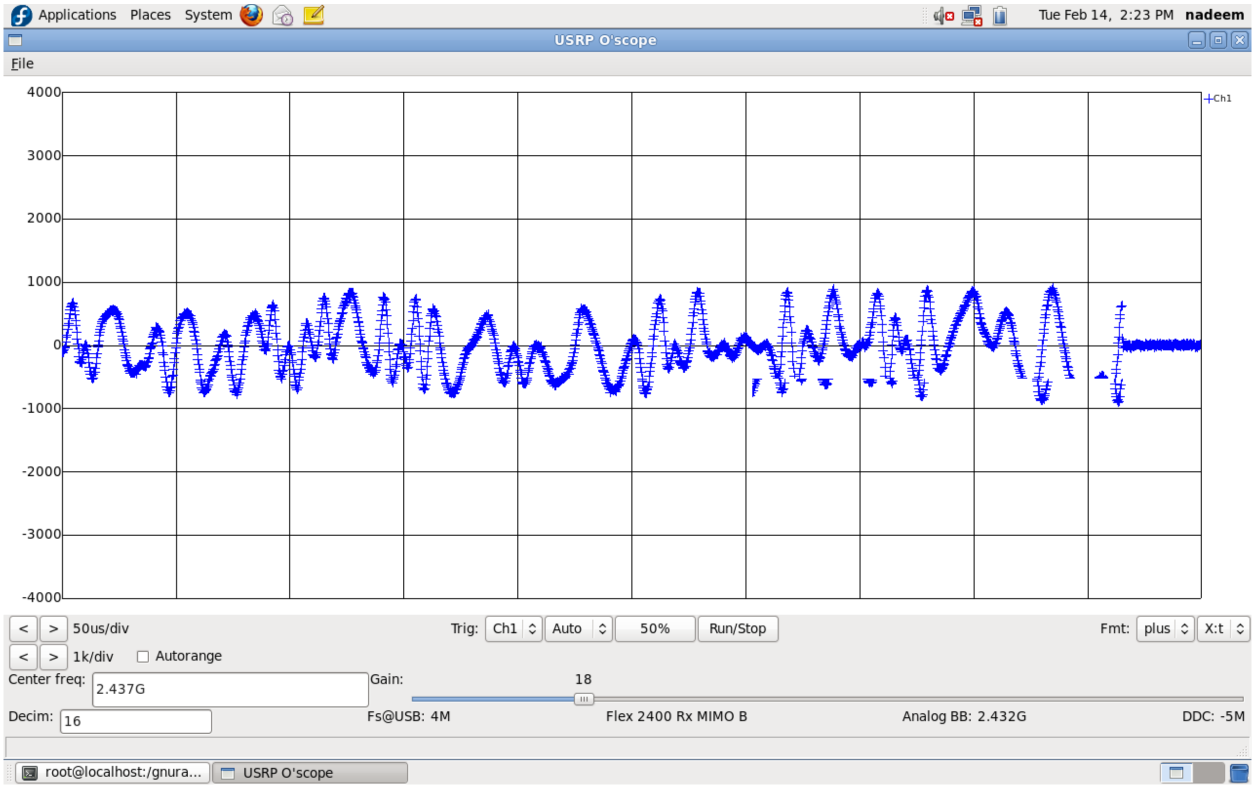
Fs@USB: 4M

Flex 2400 Rx MIMO B

Analog BB: 2.432G

DDC: -5M

Figure 4.5. Signal strength variation with jamming pulse



50us/div

1k/div

□ Autorange

Trig: Ch1 Auto 50%

Fmt: plus X:t

Center freq: 2.437G

Gain: 18

Decim: 16

Fs@USB: 4M

Flex 2400 Rx MIMO B

Analog BB: 2.432G

DDC: -5M

Figure 4.6. Pulse width in micro seconds

Data transmission is done by wireless LAN PCMCIA card DWL-650 supporting 802.11b on multiple nodes. Detector is a node that is placed inside the transmission range of all nodes. All these experiments are performed at different times of day and night to minimize the impact of external interferences caused by neighboring access points.

4.3. Complete Setup

Figure (4.7) shows a completely deployed setup. The base station is placed at the center of the network and all the other nodes are kept at boundary of network circle. All these nodes are equidistance apart. The distance between nodes to base station is 1.5 meters.

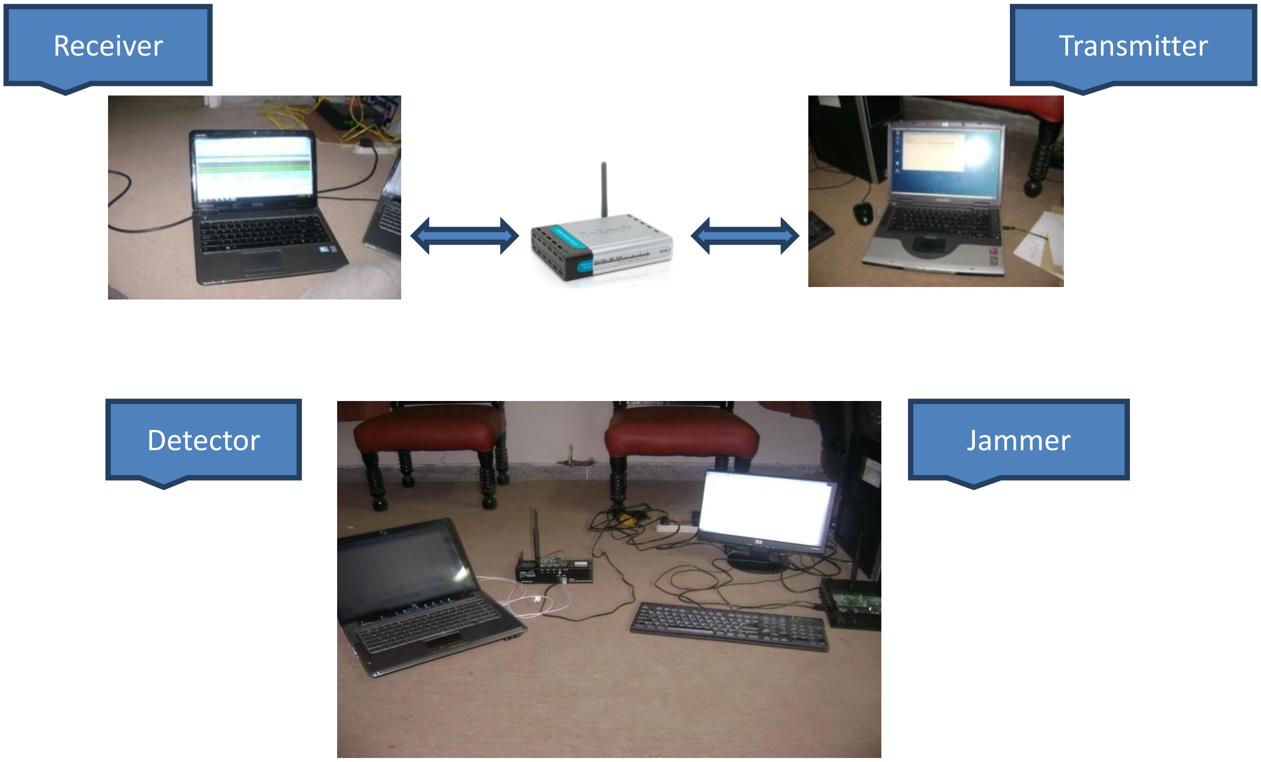


Figure 4.7. Deployed setup

4.4. Traffic Generation

The traffic from transmitter to receiver is generated as follows:

1. Normal traffic generated with saturated mode between transmitter and receiver connected via base station.
2. ICMP is used as IP layer protocol.
3. Ping utility is used with zero inter-packet intervals.
4. Packet size is chosen to be 1024 bytes.
5. Each session lasted for 180 seconds.
6. Retry limit of wireless LAN adapters is set to ZERO. This is to avoid retransmission attempts and to measure exact PDR.
7. All traffic captured is assumed to be in noise free environment

4.5. Proposed Solution

4.5.1. Training the detector

In this phase we train the detector for different patterns that can occur in case of jamming. The experimental setup for training comprise of a sender, receiver, jammer and detector. The sender sends the legitimate packet to receiver. Jammer jams it depending on what jamming technique it is employing that is constant, reactive, random or intelligent. Receiver on the other end gets the packet and saves it. The process is repeated for pre-defined period of time for each type of jammer. During this time, set of all packet effected by certain jamming is created. Meanwhile the detector keeps listening to certain parameters like PDR and signal strength. Based on the proposed multidimensional model, the region of occurrence of these parameters determined in the presence of each type of jammer. This exercise also repeated for normal network operation.

4.5.2. The Detection Model

Parameters discussed in section (2.8) are not sufficient enough individually to detect the presence of jamming attack; therefore we devised a multi-modal jamming detection scheme. This scheme is based on three parameters: PDR, signal strength variation time and signal strength disturbance. Based on these parameters, different profiles generated for different data rates for different types of jammers.

At the end of this chapter, test bed of devices has been setup. The readings collected from hardware and software plotted in chapter 5.

CHAPTER 5

EXPERIMENTS AND ANALYSIS OF RESULTS

In the experimental setup (Chapter 4), all these values are taken on the detector machine. Although, the values used in the model below have been defined in above section, more elaborate definitions are provided.

Packet Delivery Ratio (PDR): It is computed as the ratio of number of packets that pass the CRC check to the total number of packets received. All this is done on wire shark. Since wire shark captures all traffic that its network interface senses, different filters have to be applied on the collected data so that correct values may be obtained.

Signal Strength Variation: This is the variation in signal amplitude that appears when there is noise or radio interference activity on channel. In order to overcome the unintended noise, power of transmission is increased so that when both the noise and original data passed through filter, the one with better power is selected. This is the reason for sending relatively high amplitude pulses. That is how jammer can effectively jam the channel.

Pulse Width or Disturbance Interval (DI): This is the interval during which signal strength observed varying. It is taken between specific time window and disturbance interval is recorded.

5.1. Experiments and Analysis

In the section below, we considered different traffic patterns with and without jamming. These patterns are modeled with signal strength, PDR and pulse width. A detailed analysis is provided with each traffic pattern.

5.1.1. Detection of Shot-Noise based Jammer

Pulse jamming or shot-noise based jamming is protocol aware based jamming that activates when channel is sensed busy. 802.11b network operates in two modes: basic and extended. We considered CSMA/CA with basic mode of operation for experiments.

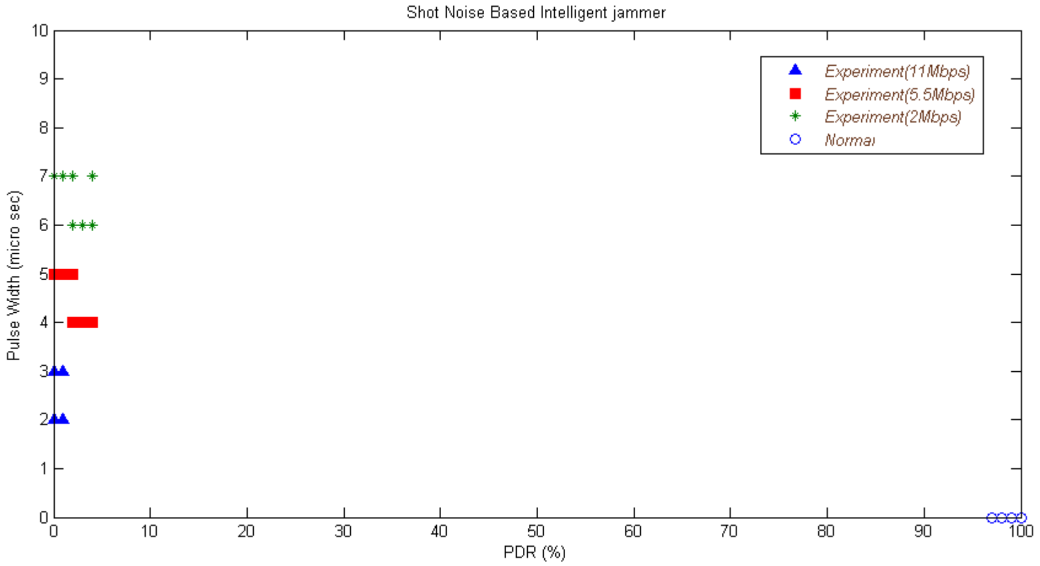


Figure 5.1. Pulse jamming or Shot-Noise based intelligent jamming

In the above model, we focused on data corrupt jamming since probability to hit the data part of transmission is high due to long transmission time of payload part of packet. Intelligent jammer does this because the probability to hit the RTS, CTS (extended mode of CSMA/CA) or ACK is low due to smaller packet length. Longest transmission is of data packet size. Shot noise based jammers are special case of protocol aware intelligent jammers that corrupt enough bits of ongoing transmission that cannot be recovered and hence packet drops.

Parameter Values

- PDR drops to zero when jamming pulse reaches a certain threshold.
- Choose sufficient length of jamming pulse to drop packet. The pulse width depends on data rate.
- Variation in signal strength (ΔS) is measured to be 15-18 dB.

Conclusion

- It is observed that PDR drops to zero after a certain pulse width threshold.
- Higher pulse width required at lower data rates and vice versa.

5.1.2. Detection of Constant Jammer

Constant jammer continuously transmits random bits without following MAC layer etiquettes. For the sake of experimental results, a continuous transmission generated for 1000 micro second. That is repeated for the whole transmission time. The reason for this is to create the effect of constant jamming.

Parameter Values

- Constant jammer drops PDR to ZERO.

- The variation in signal strength is measured to be 16-19 dB.
- Pulse width is also observed to be precisely 1000 micro seconds.
- Probability of constant jamming is always one.

Conclusion

- PDR drops to zero suddenly but still transmission energy is observed via energy spectrum.
- Signal strength variation is found to be 16-19(dB) indicates presence of some transmission.
- Cross-check with train of 1000 micro second pulses led to the conclusion of presence of constant jammer.

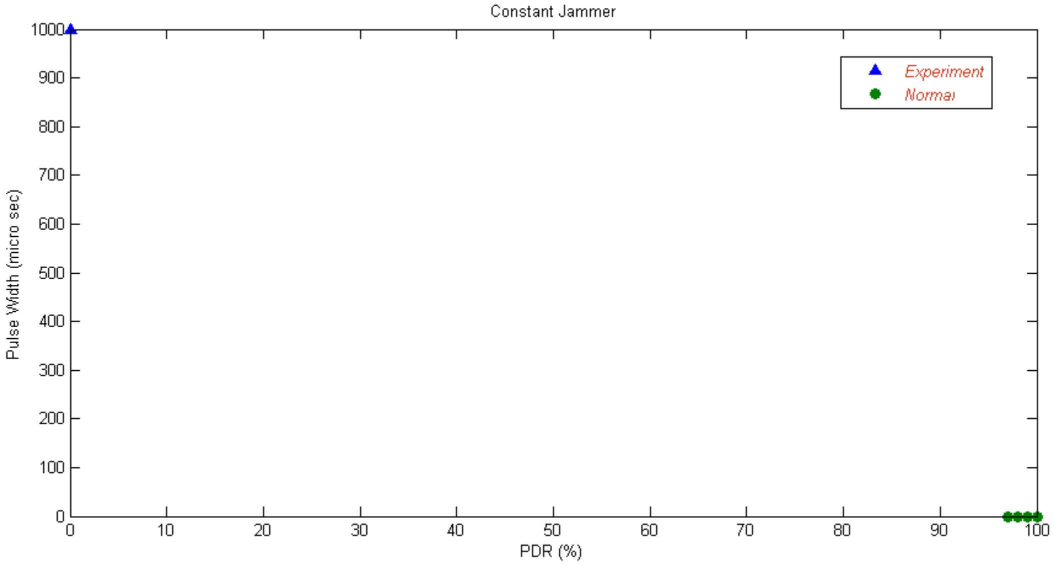


Figure 5.2. Detection of constant jammer

5.1.3. Detection of Reactive Jammer

Reactive jammer continuously senses channel and starts interfering when some legitimate node starts its transmission. The interference stops as soon as the legitimate node stops transmission.

Three groups of points show average network allocation vector (NAV) value (900, 1600 and 4200) micro seconds for data rates of 11, 5.5 and 2 Mbps respectively in figure 5.3. Based on the NAV values, the jammer sends jamming pulse for the duration of transmission required for 1024 bytes packet.

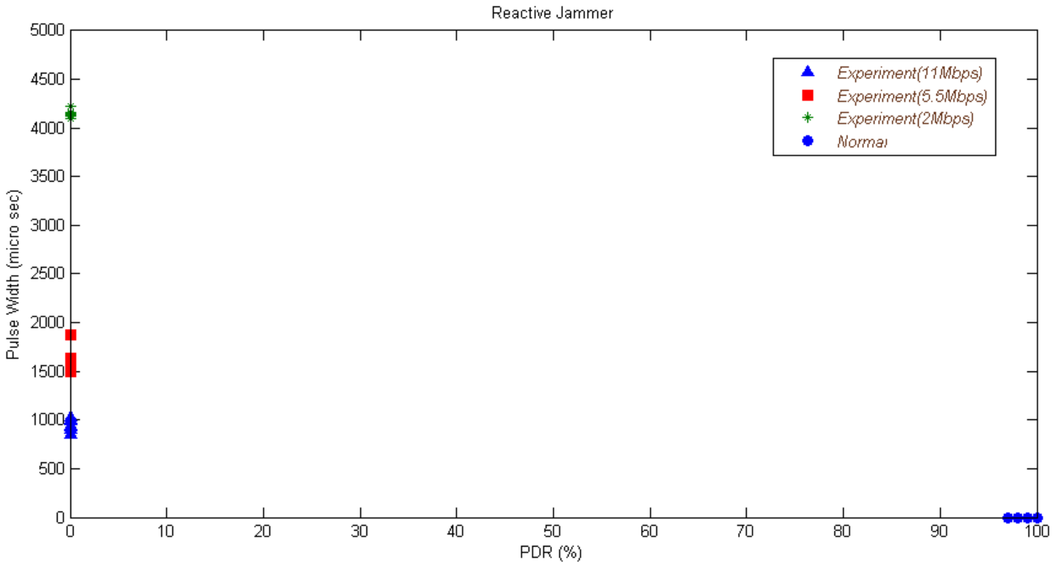


Figure 5.3. Detection of reactive jammer

Parameter Values

- PDR drops to zero immediately.
- Variation in signal strength (ΔS) measured to be 15-18 dB.
- Pulse width is also observed to be same as packet transmission time at specific data rate.

- The difference of reactive jammer and shot-noise based intelligent jammer is the pulse width that both jammers use.

Conclusion

- PDR drops to zero suddenly and increase in transmission energy is observed via energy spectrum.
- Signal strength variation (ΔS) is found to be 15-18(dB) that alarms the presence of interfering node.
- For a packet of 1024 byte payload, transmission time depends on data rate at which transmitter operating. From bottom to top (11, 5.5 and 2) Mbps shown in figure 5.3.

5.1.4. Detection of Random Jammers

Random jammer randomly jams the channel irrespective of legitimate transmission on channel. Jammer jams and sleeps iteratively according to continuous time Poisson arrival model. We altered jamming rates for 2Mbps, 5.5Mbps and 11Mbps as shown in figures 5.4.a, 5.4.b and 5.4.c respectively. These results are taken from test bed setup discussed in chapter 4.

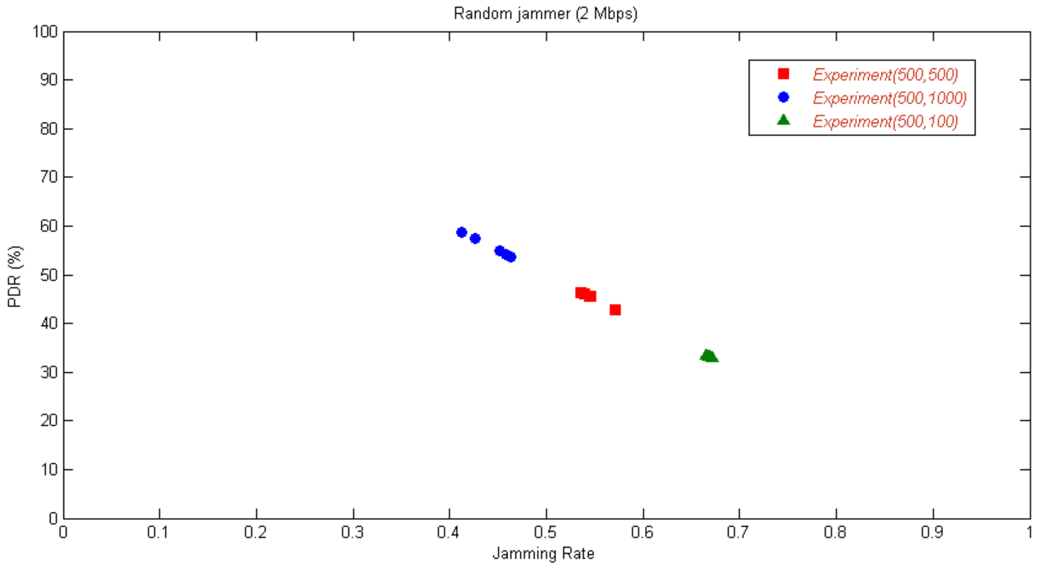


Figure 5.4.a. Detection of random jamming at 2 Mbps

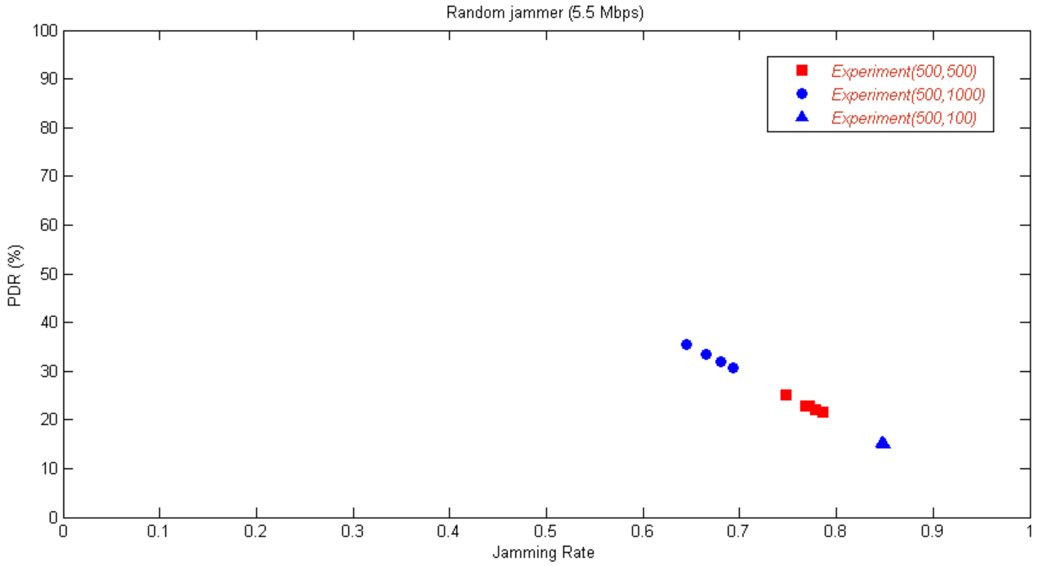


Figure 5.4.b. Detection of random jamming at 5.5 Mbps

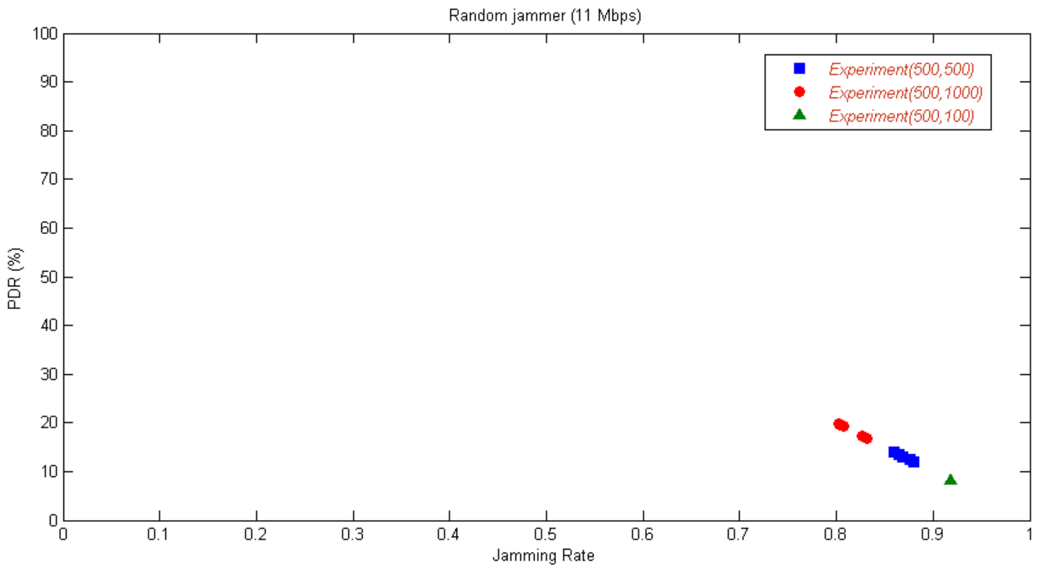


Figure 5.4.c. Detection of random jamming at 11 Mbps

Parameter Values

- PDR drops to zero when jammer is active and increases in sleep interval.
- The jam and sleep rates changed iteratively and the impact observed in figures 5.4.(a,b,c).
- The variation in signal strength is measured to be 15-18 dB when the jammer hits transmission.

Conclusion

- It is observed that PDR increases with increase in sleep rate. Figure 5.4 (a,b,c).
- It is also concluded that relatively higher PDR achieved for higher data rate for small packet size for same jamming rate. Lower data rates show high PDR than higher data rates for same sleep interval and pulse width. Figure 5.4 (a,b,c).

5.2. Jammer Classification

In figure 5.5, detection of different jamming attacks is show at 11 Mbps with packet size of 1024 bytes to transmit.

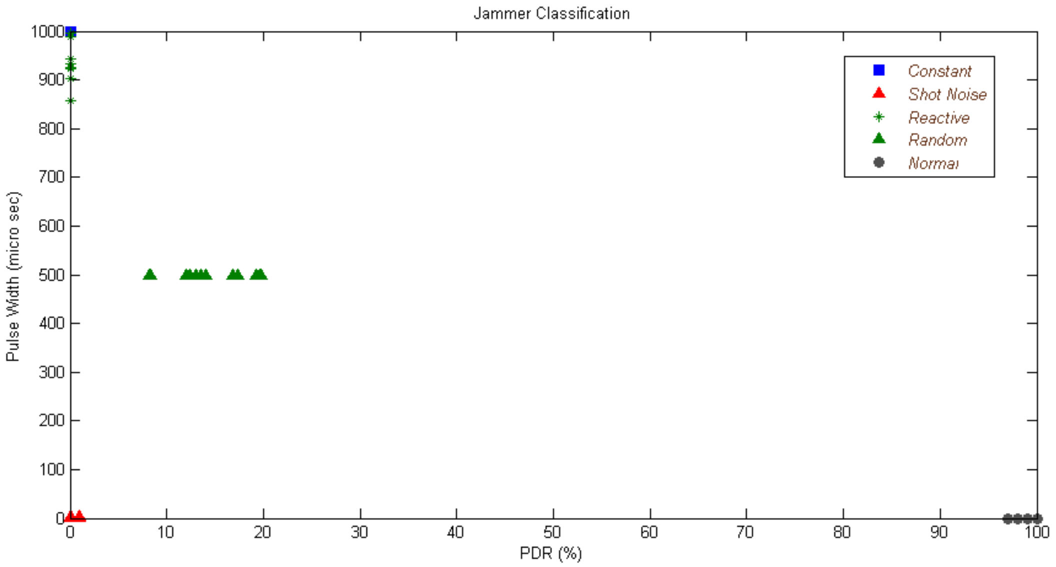


Figure 5.5. Detection of different jamming attacks at 11 Mbps

Conclusion

- It is observed that the shot noise based intelligent jammer consumes least pulse width to drop a packet as compared with constant and reactive jammers.
- Random jammer with mean jamming rate of 500 micro seconds. Sleep rate of 500 micro seconds and 100 micro seconds and 1000 micro seconds considered respectively. PDR increases with increase in sleep interval and vice versa.

5.3. Comparative Analysis of Standard Deviation

Standard deviation of 10 experimental values of (pulse width, PDR) is given in first row of table 2. Subsequent rows provide variation in standard deviation for mean value of (pulse width, PDR) for given jammer operating at data rate of 2Mbps.

Jammer	**Constant**	**Random**	**Reactive**	**Shot-Noise**
	512.989	239.66	2118.712	2.5214
Constant	512.989	316.67	2072.983	212.322
Random	497.48	239.66	2084	105.63
Reactive	925.167	1134	2113.609	879.416
Shot-Noise	509.275	240.619	2104.522	2.492

Table 2: Standard deviation between different jammers

Table 2 indicates the variation in standard deviation. It is computed if mean value of pulse width and PDR for any other jammer under consideration is provided.

CHAPTER 6

Mathematical Model for Detection

This chapter describes proposed mathematical model developed to solve the problem of jamming detection and classification identified in Chapter 3. In this chapter, initial steps toward development of fully functional mathematical model are provided.

6.1. Mathematical Model

Our mathematical model is based on three parameters: packet delivery ratio (PDR), signal strength variation (ΔS) and pulse width (pw). The derivation of mathematical model from these parameters is provided as follows:

- **Packet Delivery Ratio (PDR)**

$$\text{PDR} = \frac{\text{Number of Packets Passing CRC}}{\text{Total Number of Recieved Packets}}$$

- **Signal Strength Variation (ΔS)**

It is the change in signal strength due to normal network operation and observed during jamming conditions. It is taken in dB.

$$\Delta S = SS_{\text{observed}} - SS_{\text{network}}$$

Where, SS_{observed} is the signal strength under observation conditions when network is suspected to be under attack while SS_{network} is signal strength achieved during training session without jamming.

- **Pulse Width (PW)**

  It is the measure of time for which ΔS is greater than threshold value during observation window at detector. It is taken in micro seconds.

6.1.1. Signal Strength measurement

In case of pulse noise, signal strength is measured as [1].

$$T(k) = (\textstyle\sum_{j=k-N+1}^{k} \bar{s}(j)^2)/N \quad \_\_\_\_\_\_\_\_\_\_ \text{(1)}$$

Received energy levels s(t) of channel are measured at different time and N sub-samples are collected from a bigger window of samples as {s(k), s(k - 1), …… ,s(k - N + 1)}.

6.1.2. Jamming Rate Computation

The rate with which jammer jams the channel. It could be written as:

$$R_j = \frac{\text{The Time for Which } \Delta\text{S} > Threshold}{\text{Total Sample Window Time}}$$

Where R_j is the jamming rate, ΔS is change in signal strength due to jammer pulse and threshold is signal strength value observed during normal network operation.

For example, if jamming pulse lasts for 1 microsecond in total window of 1000 micro seconds, R_j could be said as 1/1000. For constant jammer, since there is continuous transmission of jamming pulse therefore the rate is 1.

Jamming Rate, R_j, for time T can be derived from following equation:

$$R_j = \frac{\sum_{i=1}^{N-1}(PW_{Ti+1} - PW_{Ti})}{T} \_\_\_\_\_\_\_\_ (2)$$

Where PW_T is jammer pulse time and $(PW_{Ti+1} - PW_{Ti})$ is the sub-window time during which $\Delta S > 0$. T is the total sample window time.

6.1.3. Parameters for Detection

Following few parameters are collected by detector to detect the jamming attack and its type,

1. Network Allocation Vector (NAV) values of each transmission.
2. Pulse width time subject to $\Delta S > 0$
3. Packet Delivery Ratio (PDR)

6.1.4. Data Rate Computation

The rate of transmission can be computed by the network allocation vector (NAV) value of each packet. The NAV value of each packet determines the time the packet would take during transmission. So the data rate can be computed as:

$$Data\ Rate\ (DR) = \begin{cases} 11Mbps & \forall\ NAV\ \leq 1700\ \mu sec \\ 5.5Mbps & \forall\ 1899\mu sec\ \leq NAV\ \leq 3400\ \mu sec \\ 2\ Mbps & \forall\ NAV\ \geq 9000\ \mu sec \end{cases} \_\_\_\_(3)$$

All the above derivations are for a MAC frame with size of 2312bytes. See [7] for reference.

6.1.5. PDR Computation

The PDR of a sampling window can be computed as follows:

$$\mathrm{PDR} = (1 - \mathrm{P_j})(1 - \mathrm{P_c}) \times 100 \_\_\_\_\_\_\_\_ (4)$$

Where, P_j is jamming probability computed for different jammers in subsequent sections and P_c is the collision probability of packets. Since single transmitter and receiver is used in experiments so P_c is always zero. However, it comes into account when number of contending stations for channel is more than one.

6.1.6. Jammers Classification

We first classify the jammers into two major classes i.e. protocol aware and protocol unaware. Protocol aware jammers are defined as the jammers that continuously senses the channel and only send jamming pulse when senses some transmission energy on the channel. Whereas, protocol un-aware jammers do not sense the channel before sending jamming pulse and independently jam the channel irrespective there is transmission or not on channel.

To model both types of jammers, we will take the following assumptions and conditions:

I. The network is operating in saturated mode. It means there is always a packet on channel.

II. For any pulse width (PW) of jammer, $\Delta S > 0$ for the pulse duration.

6.1.6.1 Protocol Aware Jammer

Protocol aware jammers continuously sense the channel and the transmission of jamming pulse is conditioned on the presence of valid packet transmission on channel. So the probability P of a packet to get jammed is that there is a packet transmission PKT_T and then the jamming pulse for the duration of PW_T strikes the channel.

$$P(PW_T | PKT_T) = \frac{PR\ (PW_T \cap PKT_T)}{PR(PKT_T)} \qquad \underline{\qquad} \text{(5)}$$

Each packet is composed of transmission symbols at physical layer. The number of data bits in each symbol is dependent on data rate at which the symbol will be transmitted. So the transmission time of each symbol can be computed by the following equation:

$$T_{symbol} = \frac{N_b}{DR} \qquad \underline{\qquad}\text{(6)}$$

Where N_b is number of bits in each symbol and DR is data rate at which symbol is transmitted.

Since IEEE 802.11b does not use any forward error correction except channel codes at physical layer (Barker and CCK). It means destroying one complete symbol will destroy the whole packet. So the jamming pulse threshold time, TH, required to destroy a packet ideally is:

$$TH = (2 \text{ x } T_{symbol}) + GI\underline{\qquad\quad}\text{(7)}$$

Where GI is the guard interval between two consecutive symbols and it is necessary to avoid inter symbol interference between two symbols that arrived at receiver from two different paths.

Table 2 shows the value of threshold (assume GI = 0), data rate and transmission time of symbol.

Serial Number	Data Rate (Mbps)	Transmission Time (μs)	Threshold Time (μs)
1	2	1	2
2	5.5	0.727	1.454
3	11	0.727	1.454

Table 3: IEEE 802.11b data rates and threshold time

Duration of jamming pulse is different for different types of protocol aware jammers. For typical reactive jammer, PW_T is same as PKT_T. It means jamming pulse lasts for the whole length of packet transmission. Where as in case of Shot-Noise based jammers, PW_T is greater than or equal to threshold time TH. It could be written as below:

$$PKT_T \geq PW_T \geq TH$$

The difference between reactive and shot-noise based jammers is pulse width. The shot noise based jammer intelligently hits the on air transmission such that forward error correction (FEC) introduced in packet fails to recover it at receiver side. Hence, with relatively less detection probability and higher energy efficiency, same jamming efficiency is achieved as compared with reactive jammer.

6.1.6.2. Jamming probability computation

The jamming probability for protocol aware jammers subject to condition of equation (5) can be computed as follows:

$$P_j = \frac{\sum_{i=1}^{K} f(\frac{PW_{Ti}}{THi})}{N} \quad , \ K \leq N \qquad \_\_\_\_(8)$$

Where K is number of effected packets and N is total number of packets in sampling window. $f(\frac{\mathrm{PW_{Ti}}}{\mathrm{THi}})$ is a function that is defined as follows:

$$f\left(\frac{\mathrm{PW_{Ti}}}{\mathrm{THi}}\right)\begin{cases}= 0, & \mathrm{PW_T} < TH \\ = 1, & \mathrm{PW_T} \geq \mathrm{TH}\end{cases} \text{———} \quad (9)$$

6.1.6.3. Relationship among Data Rate, Pulse Width and Jamming Probability

Relationship among data rate (DR), pulse width time ($\mathrm{PW_{T)}}$ and jamming probability ($\mathrm{P_j}$) for protocol aware jammers is shown in table 4. These results are obtained using test bed described in previous chapter.

Data Rate (Mbps)	Pulse Width Time (µ sec)	Jamming Probability ($\mathrm{P_j}$)
11	3	1
11	4	1
11	5	1
11	6	1
11	7	1
5.5	3	0
5.5	4	0
5.5	5	1
5.5	6	1
5.5	7	1
2	3	0
2	4	0
2	5	0
2	6	0
2	7	1

Table 4. Data Rate, Pulse Width and Jamming Probability for IEEE 802.11b

6.1.6.3. Protocol Unaware Jammer

We considered constant and random jamming models from protocol unaware jammers class. Jamming probability of constant jammer is one. This is due to the fact that it continuously transmits jamming pulses during the whole observation window and channel appears always busy to legitimate nodes for transmission.

Consider random jammers that jam the channel with transmission-independent sleep and jam intervals during a time window. Random jammer behaves exactly like a constant jammer if it does not sleep during the time window.

Consider a random jammer that acts as two state continuous time Markov chain process. It sleeps with exponential amount of time with mean 1/ λ (where λ is sleeping rate) and jams exponential amount of time with mean 1/μ (where μ is jamming rate). The jammer jams and sleeps iteratively. Consider a random jammer is jamming initially at t = 0, what would be steady state probability that the jammer would be jamming or sleeping at time t? See Appendix A for details.

Consider the following 2 state Markov machine,

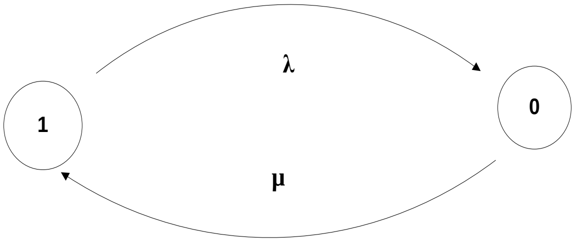


Figure 6.1: State transitions of random jammer

Where,

State 1: Jam state, MTTJ (mean time to jam) = 1/µ

State 0: Sleep state, MTTS (mean time to sleep) = 1/λ

Since the system is operating in steady state, global balance equations for both states are:

State 1: $\lambda\pi 1 = \mu\pi 0$ ______________ (10)

State 0: $\mu\pi 0 = \lambda\pi 1$ _______________ (11)

Where $\pi 0$ and $\pi 1$ are the proportions of time the jammer spends in state $x_{i = \{0, 1\}}$. Since both value in equation (1) and (2) are unknown.

From the normalization condition, we know that,

$$\pi 0 + \pi 1 = 1 \text{______________ (12)}$$

Putting the value of $\pi 0 = \left(\frac{\lambda}{\mu}\right)\pi 1$, from equation (11) to equation (12),

$$\left(\frac{\lambda}{\mu}\right)\pi 1 + \pi 1 = 1$$

$$\pi 1 = \mu/(\mu + \lambda) \text{________(13)}$$

Similarly, $\pi 0 = \lambda/(\mu + \lambda)$________(14)

Transient availability of each state is the rate of build up for each state and can be computed as follows:

Consider stat1,

Rate of build up = rate of flow IN – rate of flow OUT

$$\pi 1'(t) = \mu\pi 0(\mathrm{t}) - \lambda\pi 1(t)$$

$$\pi 1'(t) = \mu - [\lambda + \mu]\, \pi 1(t)$$

From problem statement, $\pi 1(0) = 1$ and further solving above equation yields. (See [18], Chapter 6, example 6.10 for complete derivation)

$$\pi 1(\mathrm{t}) = \frac{\mu}{\mu + \lambda} + \frac{\lambda}{\mu + \lambda}\mathrm{e}^{-(\mu+\lambda)\mathrm{t}}\_\_\_\_\_\_(15)$$

Similarly, $\pi 0(\mathrm{t}) = \frac{\lambda}{\mu+\lambda} + \frac{\mu}{\mu+\lambda}\ \mathrm{e}^{-(\mu+\lambda)\mathrm{t}}$ ______(16)

Above equations give transient probability for jam and sleep state. However, since we are considering the system in steady state therefore for large value of t, above equation (17) reduced to:

$$\lim_{\mathrm{t}\to\infty} \pi 1(\mathrm{t}) = \frac{\mu}{\mu+\lambda} \quad \_\_\_\_\_(17)$$

This is equivalent to equation (14).

The above set of equations (13) and (14) define the probability of random jammer to remain in any of the two states.

6.1.7. Jammers Classification

Based on equation (4), different jammers can be classified as shown in equation (18):

$$PDR \begin{cases} = 0,\ \ \mathrm{PW_T} = \mathrm{TH}, \Rightarrow \mathit{Shot\ Noise\ jammers} \\ = 0,\ \mathrm{PW_T} = \ \mathrm{PKT_T}, \qquad\qquad \Rightarrow \mathit{Reactive} \\ = 0, \mathrm{PW_T} = \mathrm{T_{win}}, \qquad\qquad \Rightarrow \mathit{Constant} \\ \geq 0, \mathrm{PW_T} = \mathrm{X}\ \pm \sigma \qquad\qquad \Rightarrow \mathit{Random} \end{cases} \text{\_\_\_\_\_}(18)$$

Where PW_T is pulse width time and T_{win} is time of whole sampling window. 'X' is mean jamming pulse that is observed in case of random jammer with threshold σ around it.

6.1.8. The Case of Shot-Noise Based Jammer

Shot noise based jammers are special case of protocol-aware jammers that just beat forward error correction (FEC) scheme used at physical and MAC layer. IEEE 802.11b networks use convolutional coding at physical layer, a single continuous pulse hitting legitimate packet can completely drop it. If a symbol is corrupted by a pulse of time T_s, it could drop whole packet.

T_{symbol} is the transmission time of symbol. For example, if a symbol contains 4 bits, these bits are spread over maximum four consecutive symbols (assuming linear spreading is used). To completely destroy the symbol and the packet ultimately, these four symbols have to be destroyed. Thus the time required for the pulse by jammer is illustrated in equation (19):

$$\mathrm{Ts} = \mathrm{N}\ \times (\mathrm{Tsymbol} + \mathrm{GI})\text{\_\_\_\_\_\_\_\_\_}(19)$$

T_{symbol} is the transmission time of maximum number of bits per symbol; N is number of bits per symbol and GI is guard interval between two symbols. It is to be noted that Ts would be different if bit interleaving or scrambling is used at physical layer.

6.2. Discussion

It is to be noted that physical layer of IEEE 802.11b does not have any forward error correction (FEC) scheme [17]. However, it uses different codes for different data rates as shown in table 5.

Data Rate (Mbps)	Code Length	Modulation	Modulation Rate	Symbol Rate	Bits / Symbol
1	11- Barker	DBPSK	11,000,000	1Msps	1
2	11- Barker	DQPSK	11,000,000	1Msps	2
5.5	8-CCK	DQPSK	11,000,000	1.375Msps	4
11	8-CCK	DQPSK	11,000,000	1.375Msps	8

Table5. 802.11b encoding at physical layer

Although the physical layer of 802.11b is quite robust against interference due to direct sequence spread spectrum (DSSS) and encoding techniques like Barker sequence for 1Mbps and 2Mbps and complementary code keying (CCK) for 5.5Mbps and 11Mbps, still some packets with bad bytes pass to link layer. These packets cannot pass CRC check, hence discarded. It could also be inferred that probability of packet drop increases/decreases with data rate, modulation and encoding techniques the transmission is using. It is also worth mentioning that DSSS is relatively more robust than CCK due to 11-chips per bit that are spread on 22 MHz band. CCK uses 4bits/8chips or 8bits/8chips. However, autocorrelation properties of CCK make it quite robust.

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1. Conclusion

In this work, we proposed a multi-modal radio jamming detection scheme for 802.11b networks. Major contribution of the work is the classification of jamming attacks with accuracy and low false alarm rate. Instead of performing simulations, real test bed has been developed for launching different jamming attacks with software defined radio (SDR) on USRP. Similarly, the detector node collected the readings equipped with USRP and Python scripts. This multi-parameter detection model not only enhanced the accuracy of detection but also led to classification of jamming attacks. The proposed mathematical model is first attempt towards solid foundation for classification of jamming attacks. It takes into account PDR, signal strength variation and pulse width and yields results that comply with experimental results.

7.2. Future Works

This work is performed with single transmitter and receiver. However, it could be extended for more than two nodes to monitor the PDR and signal strength variation in case of more than one transmitting node. Signal strength variation becomes complex when more than two transmitting nodes involves and jammer is also present on the channel. Another aspect is to mathematically model the collision probability and extend the equations that compute PDR in chapter 6.

APPENDIX A

Continuous-Time Markov Chains

Let us have a continuous time stochastic process {X(t), t≥0}. This process takes values from set of positive integers. This process is said to be continuous time Markov chain (CTMC) if it satisfy following conditions:

$$\forall\, \mathrm{w}, \mathrm{t}\ \geq 0$$

$$\text{and} \qquad \forall\, \mathrm{i}, \mathrm{j}, \mathrm{x}(f),\ 0\ \leq \mathrm{f} < \mathrm{w}$$

$$\text{Then } P\,\{\,X\,(t+w) =\ j\,|\,X(w) = i, X(f) =\ x(f),\ 0\ \leq f\ < w\,\}\ = P\,\{\,X(t+w) = j\ Xw{=}i\}\ \_\_\_\_\_\text{(A.1)}$$

In other words, continuous time Markov chain is a process have memory less property in which conditional distribution of the future X(t+w) and past X(f) only depends on the present state and independent of the past.

In addition, if,

$$P\,\{\,X\,(t+w)\,|\,X(w)\} = P\,\{\mathrm{X(t)}\} \qquad \forall\, \mathrm{w}, \mathrm{t}\ \geq 0\ \ \_\_\_\_\_\_\_\_\ \text{(A.2)}$$

The above equation depicts the random variable, t, is memory less and is independent of current state w of the process.

We will use these concepts in memory less random jammers where the jam and sleep states are independent of each other.

Birth Death Process Standard Equation

The standard equation for backward birth death process is given below:

$$P'_{ij}(t) = \lambda_i P_{i+1,j}(t) + \mu_i P_{i-1,j}(t) - (\lambda_i + \mu_i) P_{ij}(t), \quad i>0 \quad \_\_\_\_\_\_ \text{(A.3)}$$

Where λ is birth rate, ⍰ is death rate and t is any time. Formal proof of the above equation could be found in Chapter 6 of [18].

Uniformization

Let P_{ii} is a state that some process does not leave and it is always assumed that $P_{ii} = 0$. It means that at some particular time the probability for a process to remain in the same state is zero. However it is not always the case. Consider $q_i \leq q$, where q is the total transition rate of a process and $q_{i\,/}\,q$ is the actual rate with which the process leaves the current state i and transits to some other state j. The remaining (1-qi/q) are the fictitious transitions that keep the process in the same state.

It could be said that any Markov chain satisfying the condition of $q_i < q$ is said to be a process that spends exponential amount of time in state i and then transits to state j with probability P^*_{ij}, where

$$P^*_{ij} = \begin{cases} 1 - \frac{qi}{q}\,, & j = i \\ \frac{qi}{q}\, P_{ij}, & j \neq i \end{cases} \quad \_\_\_\_\_\_\text{(A.4)}$$

The n-stage transition probabilities can be calculated using

$$P_{ij}(t) = \sum_{n=0}^{\infty} P_{ij}^{*n} \ e^{-qt} \ \frac{(qt)^n}{n!} \text{\_\_\_\_\_\_\_\_\_}(A.5)$$

The process of introducing fictitious transitions from a state to itself to uniformize the rate of transition is called uniformization. We will use the concept of uniformization in modeling behavior of channel unaware random jammers.

References

1- W. Xu, W. Trappe, Y. Zhang, and T. Wood.” The Feasibility of Launching and Detecting jamming Attacks in Wireless Networks”. In *ACM MOBIHOC*, 2005.

2- E. Bayrataroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa (2008). "On the Performance of IEEE 802.11 under Jamming", in Proceedings of IEEE Infocom'08

3- Ali Hamieh, Jalel Ben-Othman:,”Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution” ICC 2009: 1-6

4- X. Zou and J. Deng, "Detection of Fabricated CTS Packet Attacks in Wireless LANs," in Proc. of 7th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE '10), Houston, TX, USA, November 17-19, 2010. Invited Paper

5- E. Garcia-Villegas, M.Gomes “Detecting and Mitigating the Impact of Wideband Jammers in IEEE 802.11 WLANS” , in proceeding of acm 2010

6- Ming Yu, Wei Su, M. Zhou, “A New Approach to Detect Radio Jamming Attacks in Wireless Networks”, IEEE 2010

7- Abid Hussain, Nazar Abbas Saqib, “Protocol aware shot-noise based radio frequency jamming method in 802.11 networks. 1-6”,In Proceedings of the 8th International Conference on Wireless and Optical Communications Networks, WOCN 2011, Paris, France, 24-26 May 2011. IEEE 2011

8- Pelechrinis, K, Iliofotou, M, Krishnamurthy, V. “Denial of Service Attacks in Wireless Networks: The case of Jammers”, IEEE, May 2010

9- D. Thuente, M. Acharya, "Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks", MILCOM 2006

10- E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the Performance of IEEE 802.11 under Jamming", in Proc. INFOCOM, 2008, pp.1265-1273.

11- http://en.wikipedia.org/wiki/Shot

12- G.Bianchi, “Performance analysis of the ieee802.11 distributed coordination function,” IEEE Journal on Selected Areas in Communications, vol. 18, no. 3, 2000

13- David J. Thuente and Mithun Acharya, “Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks” in proceedings of IEEE MILCOM, 2006, Washington D.C USA

14- http://en.wikipedia.org/wiki/Modulation

15- http://www.egr.msu.edu/waves/people/Ali.htm

16- S. A. Khayam a, S. Karandea, H. Radhaa, and D. Loguinov, “Performance analysis and modeling of errors and losses over 802.11b LANs for high bit-rate real-time multimedia,” Signal Processing: Image Communication, vol. 18, no. 7, pp. 575–595, 2003

17- O Alay, T Korakis, Y Wang and S Panwar,“ An Experimental Study of Packet Loss and Forward Error Correction in Video Multicast over IEEE 802.11b Network**,”** Proceedings of 6th IEEE Consumer Communications and Networking Conference (CCNC 2009), Las Vegas NV, pp.1-5, 10-13 January 2009

18- Rose Sheldon M., “Introduction to Probability Models, 7th Edition”, Chapter 6

19- Acharya, M., T. Sharma, D. Thuente, D. Sizemore, “Intelligent Jamming in 802.11b Wireless Networks”, OPNETWORK 2004, August 2004.