

## **Analysis OF Wimax Under Jamming Effect for Various Antennas**

Leena K Parmar

*Department of Electronics and Communication Engineering, L D Collage of Engineering, Ahmedabad, Gujarat, India*

---

**Abstract:** *Use of Internet is increasing day by day. Wi-Fi provides wireless access to the internet but range is limited to certain meters only. So concept of WiMAX is introduced to increase the range. WiMAX[1] means worldwide interoperability for microwave access. WiMAX is also known as wireless broadband. The WiMAX based on IEEE 802.16, has been one of the most important technologies in communication networks providing voice, data and video services with different type of QoS (Quality of Service) during last few years. The main purpose of this paper is to see and evaluate the performance of a WiMAX physical layer scenario for various modulation schemes, in the presence and absence of jammer. The simulator encompasses the blocks that build the physical layer of IEEE 802.16e. BER results are presented with the presence of jamming under different digital modulations schemes as well as different antennas. Simulation approach is main concern here. OPNET MODELER is the software used for the simulation purpose.*

**Keywords**–*WiMAX, Physical Layer Jamming, Scrambling, OPNET MODELER, Modulation Schemes.*

---

### **I. Introduction**

IEEE 802.16 is the standard for WiMAX. WiMAX is also known as wireless broadband. IEEE 802.16-2004 is known as fixed WiMAX and IEEE 802.16-2005 is known as mobile WiMAX [1]. In wired networks physical layer threats are not important but in wireless air is used as medium so physical layer threats comes into picture. In wireless jamming and scrambling are considered as physical layer threats. Here simulation approach is used to see the performance of the IEEE 802.16-2004 system in jamming and scrambling environment [8], [10]. By introducing a source of noise strong enough to significantly reduce the capacity of the WiMAX channel jamming effect can be achieved. The information and equipment required to perform jamming are easy to acquire. Theoretically jamming can be resist by increasing the power of signals or increasing the bandwidth of signals. The practical options include a more powerful WiMAX transmitter, a high gain WiMAX transmission antenna, or a high gain WiMAX receiving antenna. It is easy to detect jamming in WiMAX Communications as it can be heard by the receiving equipment. Law enforcement can also be involved to stop jammers. Since jamming does not pose a significant impact on both the WIMAX users and systems because it is easy to detect and address. Scrambling is usually instigated for short intervals of time and is targeted to specific WiMAX frames or parts of frames [3] [9]. WiMAX scramblers can selectively scramble control or management messages with the aim of affecting the normal operation of the network. Slots of data traffic belonging to the targeted SSs can be scrambled selectively, forcing them to retransmit. Noise jamming and multi-carrier jamming are considered here for simulation approach. Noise jamming is used to jam the particular band of frequencies. In noise jamming carrier frequency and bandwidth of the targeted system should be known. In multi-carrier jamming the frequencies of carriers of targeted system should be known. Simulation approach is easy compare to practical approach. The issues related to practical approach will be described in the later part.

### **II. The Investigated Physical Layer**

The primary operation bands of IEEE 802.16-2004 include 10-66 GHz licensed bands, frequencies below 11GHz and license-exempt frequencies below 11GHz (primarily 5-6 GHz) [1]. According to these operation bands, IEEE 802.16-2004 PHY defines five specifications for different operation scenarios. Among them, Wireless MAN-OFDM PHY is based on orthogonal frequency-division multiplexing (OFDM) technology and designed for NLOS operation in the frequency bands below 1GHz. It is selected to be the air interface of the system under investigation in this paper. At the transmitter side, the information data first undergoes channel coding composed of randomization, forward error correction (FEC), and interleaving. Randomizer uses a Linear Feedback Shift Register (LFSR) to scatter long data strings of zeros or ones. Forward error correction concatenates an outer Reed-Solomon encoder with an inner rate compatible convolution encoder. FEC helps to correct the errors in subcarriers to a certain limit. The interleaver takes two permutations to rearrange the subcarriers so that the burst errors are distributed more uniformly at the demodulation input [2]. After channel coding, data bits are mapped and

modulated onto the allocated subcarriers by BPSK, 16-QAM and 64-QAM modulation. Subsequently, data are transmitted by OFDM method. In the receiver side, all the procedures carried out in the transmitter side are implemented again but in a reverse direction. One OFDM symbol can be divided into two parts in time domain: the cyclic prefix (CP) time and the useful symbol time. The cyclic prefix locates in the beginning of the symbol and is a duplication of the tail of the useful symbol, which is introduced to mitigate the effect of multipath. In frequency domain, an OFDM symbol is composed of a series of subcarriers. In Wireless MAN-OFDM PHY, the number of subcarriers is 256. As shown in Fig. 1, three types of subcarriers can be categorized: 192 data subcarriers carrying payload, 8 pilot subcarriers mainly for channel estimation, and 56 null subcarriers for guarding purpose. The pilot subcarriers distribute evenly among the data subcarriers. This is standard symbol in frequency domain.

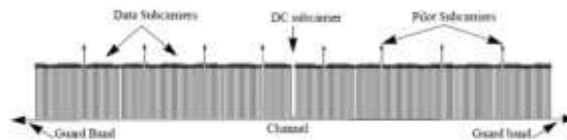


Figure 1: OFDM symbol Frequency domain description

Channel estimation is mandatory for the OFDM systems employing coherent detection. Comb type pilot channel estimation is capable of collecting instant information of the channel and therefore used in this research. The channel estimation for the payload subcarriers is achieved by interpolation, using the channel information obtained at the 8 pilot subcarriers.

### III. Simulation

Simulation can be done in any software but the procedure remains same. For simulation some parameters are taken from the standard and some parameters are varied to get the appropriate results. Modulation parameters used in the simulation are listed in the Table.1.

Table 1: Parameters Used in Simulation Algorithm [7]

Modulation	Code rate for convolution coding
BPSK	1/2
QPSK	1/2
QPSK	3/4
16-QAM	1/2
16-QAM	3/4
64-QAM	2/3
64-QAM	3/4

The computer simulation in this paper is generated using OPNET MODELER. . The multipath channel is simulated as a frequency selective, slow fading channel by snapshot method. The parameters adopted in the simulation are listed in Table.2[12].

Parameters	Standard value for simulation
Channel bandwidth	20 MHz
Number of carriers	200
CP ratio	1/4
OFDM symbol duration	102 μs
Number of FFT points	256
Sampling factor n	28/25
SNR	20 db

The values of parameters are taken from standards decided by IEEE 802.16. All this values are considered for the simulation and remains same for number of scenarios. For comparison of scenarios to be simulated the selection of values is important. Noise jamming and multi-carrier jamming can be simulated if system bandwidth and carrier bandwidth is known.

#### IV. Mathematics Involved

There are several QOS (quality of service) parameters to evaluate the system performance under jamming. The formula given below is useful to define jamming type.

$$\frac{B_j}{B_{vs}} = \frac{\text{Jammerbandwidth}}{\text{Victimsystembandwidth}} \dots\dots\dots(1)$$

Mainly jamming is of basic 2 types. If the ratio BJ/BVS is less than 0.2 jamming is considered to be spot (narrow band) jamming and if ratio BJ/BVS is greater than 1, barrage ( wide band) jamming [7]. Packet error rate and signal to jamming ratio is used to evaluate the system performance. system performance can be evaluate from several other QOS parameters like throughput, delay and traffic related parameters. The packet error rate can be calculated by the formula given below.[13]

$$PER = \frac{\text{errormouspacket}}{\text{packetsent}} \dots\dots\dots(2)$$

Signal to noise ratio is given by the following equation. Here noise power is jamming signal power.

$$SNR = \frac{\text{Signalpower}}{\text{Noisepower}} \dots\dots\dots(3)$$

#### V. Design Of Scenario & Jammer In Opnet Modeler

In this thesis fixed NLOS WiMAX system is simulated under jamming. Single carrier jamming scenario is shown in figure 3.

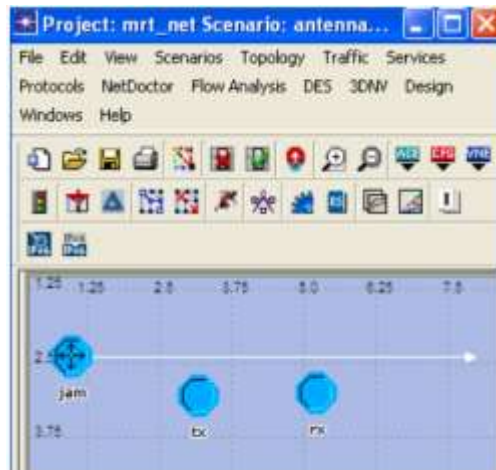


Figure 3: Scenario used for single carrier jamming.

The transmitter node model of jammer is given in the figure 4.



Figure 4: Transmitter node model of jammer.

The tx\_gen is processor module which calculates the information that the antenna needs to point at a target: latitude, longitude, and altitude coordinates[14]. The pointing processor convert this calculation by using a Kernel Procedure, a node's position in a subnet (described by the x position and y position attributes) into the global coordinates that the antenna requires[14]. The radio\_tx is radio transmitter module which transmits packets to the antenna at 1024 bits/second, using 100 percent of its channel bandwidth[14]. For each arriving candidate packet, the radio receiver module consults several properties to determine if the packet's average bit error rate (BER) is less than a specified threshold. If the BER is low enough, the packet is sent to the sink and destroyed. The ant\_tx is antenna module which models the directional gain of a physical antenna by referencing its pattern attribute. The antenna uses two different patterns: the isotropic pattern (which has uniform gain in all directions) and a directional pattern. Antenna pattern editor is also provided in the software. Antenna pattern is important in the design of jammer. By using this software antenna

pattern can be designed to utilize power effectively. Introduction to design of jammer is given in this paper. It is not possible to include step by step procedure. The idea is given here how to design jammer using opnet modeler

### VI. Results

In this paper the scenario as shown in fig 3 has been implemented and jammer is moving toward subscriber station and then moving away. It is used to build single carrier jamming. The result shown in Fig 5.1 Throughput(packets/sec) for different modulation schemes like BPSK, 64-QAM, 16-QAM. It indicates that bit error rate is lowest in BPSK and BER is highest in 64-QAM.

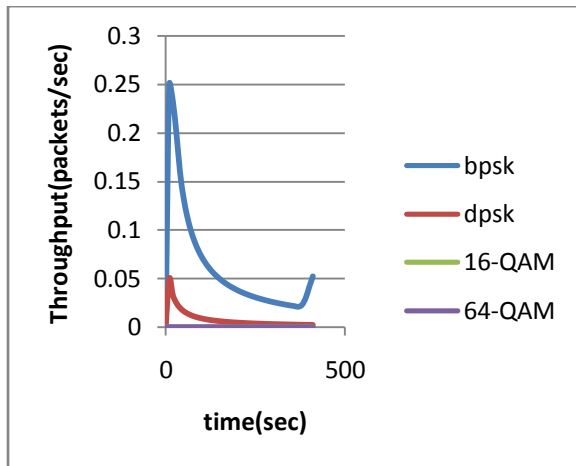


Figure 5.1: Throughput Vs Simulation time

In communication networks, throughput is the average rate of successful message delivery over a communication channel [16]. Throughput is usually measured in bits/sec or packet/sec. Hence from above Figure 5.2 we can conclude that as BER increases Throughput decreases. Modulation scheme BPSK has the lowest BER compared to other modulation schemes and therefore it has highest throughput under jamming effect. And BER of 64-QAM is highest so it has the lowest throughput.

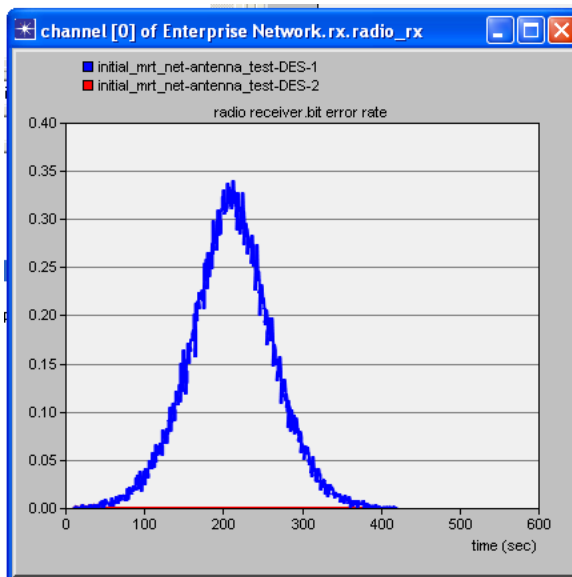


Figure 6.1: BER Vs Simulation time

DES-1: Isotropic antenna  
DES-2: Directional antenna

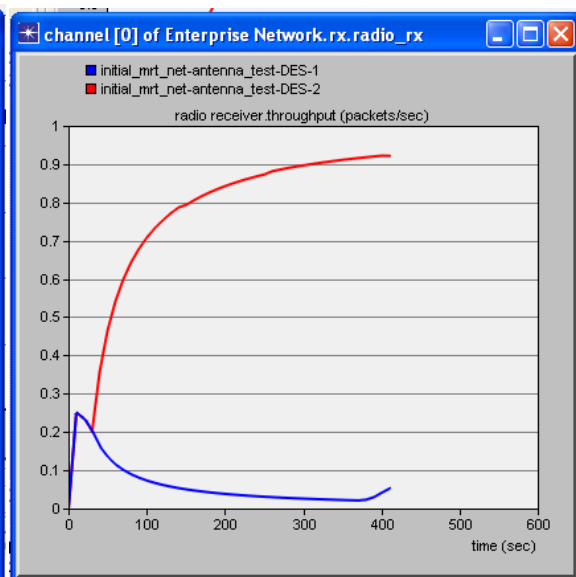


Figure 6.2: Throughput Vs Simulation time

DES-1: Isotropic antenna  
DES-2: Directional antenna

Third result shown in Fig. 6.1 is taken using the same scenario but the antennas used in subscriber stations are changed to see the impact antennas under jamming. Fig. 6.1 shows the BER vs. simulation time for different

antenna used at receiver side under jamming effect. Jammer has isotropic antenna. It shows that directional antenna performs well under jamming because whenever jammer come in the direction of the antenna then only it affect the system. Result shows when jammer is out of direction of antenna the BER goes down.

## VII Conclusion

If channel conditions are poor (if channel is not capable to resist jamming effect) then BPSK is used and if channel quality improves (if channel is capable to resist jamming effect) then 16-QAM or 64-QAM is used. Directional antenna gives better performance than isotropic antenna. The thesis shows results for fixed NLOS only. Jamming effect on Mobile NLOS can be simulated by same set of parameters but some additional parameters related to mobility must be considered. MAC layer threats can be simulated by considering standard parameters and the work done here provides base for the same.

## References

- [1] Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed, *Fundamentals of WiMAX Understanding Broadband Wireless Networking*: Prentice-Hall.
- [2] Simon Haykin, Michael Moher, *Modern Wireless communication*, Prentice-Hall.
- [3] Syed Ahson, Mohmmad Ilyas, Syed Ahson, Mohammad Ilyas, *WiMAX Standards and Security*. Boca Raton: CRC Press, 2008.
- [4] Taeshik Shon and Wook Choi (2007), "An Analysis of Mobile WiMAX security: Vulnerabilities and Solutions"
- [5] LUO Cuilan (2009), "A Simple Encryption Scheme Based on WiMAX", Department of Electronics Jiangxi University of Finance and Economics Nanchang, China .
- [6] Boris Makarevitch, "Jamming Resistant Architecture for WiMAX Mesh Network", communications Laboratory Helsinki University of Technology.
- [7] Juan Li, Sven-Gustav Häggman (2006), "Performance of IEEE 802.16 Based System in Jamming Environment and Its Improvement With Link Adaption", The 17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'06).
- [8] Mahmoud Nasreldin, Heba Aslan, Magdy El-Henna wy, Adel El-Hennawy (2008), "WiMAX Security", 22nd International Conference on Advanced Information Networking and applications.
- [9] White paper by Motorola (2007), "WiMAX Security for Real- World Network Service Provider Deployments".
- [10] Rakesh Kumar Jha and Dr Upena Dalal "Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN)" International Conference on Recent Trends in Information, Telecommunication and Computing, IEEE Xplore, Kerala, March 2010.
- [11] IEEE 802.16 Working Group. IEEE 802.16-2004 Local and metropolitan area networks - Part 16: Air interface for fixed broadband wireless access systems IEEE Standard for Local and Metropolitan Area Networks[S]: IEEE Computer Society Press.
- [12] IEEE 802.16 Working Group. IEEE 802.16e-2005 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for combined Fixed and Mobile Operation in Licensed Bands[S]: IEEE Computer Society Press.
- [13] Rakesh Kumar Jha and Dr. Upena Dalal "A Performance Comparison With Modulation Schemes In WiMAX Physical Layer Security Aspect" Published by International Journal of Computer Applications (0975 – 8887) ,Volume 6– No.8, September 2010.
- [14] Hardik Patel, MTec Thesis, "WiMAX Physical Layer Security Aspects: Simulation and Testing Using OPNET MODELER 14.5" Sardar Vallabhbhai National Institute Of Technology, 2010
- [15] Anand Nayyar, "Performance Analysis of WiMAX Physical Layer for various Modulation Schemes ". Jalandhar 2008
- [16] n.wikipedia.org