A Performance Comparison With Modulation Schemes In WiMAX Physical Layer Security Aspect

Rakesh Kumar Jha
Department of Electronics and Communication Engineering,
SVNIT Surat, INDIA

Dr. Upena D. Dalal
Department of Electronics and Communication Engineering,
SVNIT Surat, INDIA

ABSTRACT

This paper presents WiMAX physical layer threats jamming and scrambling. The performance of the system was found out to greatly differ with the use of different jamming signals, allowing central areas to be identified, where system development should be focused on. In addition, from the basic theory point of view, rather surprising results where also found. The work should give a clear picture of how the studied WiMAX system performs under jamming as well as without the presence of jamming. The results show that some forms of interference degrade the performance of the system rapidly, thus the form of incoming jamming should be known and considered before deploying the system. Noise jamming, multi-carrier jamming and scrambling are discussed here. The issues related to jamming and jamming reduction techniques are also covered. Jamming and scrambling can destroy communication in the targeted area. Multi-carrier jamming is challenge in WiMAX because WiMAX is having OFDM based physical layer. 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]. Jamming is achieved by introducing a source of noise strong enough to significantly reduce the capacity of the WiMAX channel. The information and equipment required to perform jamming are not difficult to acquire. Resilience to jamming can be augmented by increasing the power of signals or increasing the bandwidth of signals via spreading techniques such as frequency hopping or direct sequence spread spectrum. 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 is fairly easy to detect and address, so it does not pose a significant impact on both the WIMAX users

and systems. 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 convolutional 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.
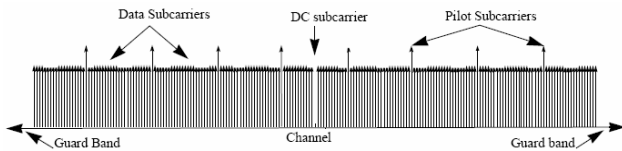

Figure 1: OFDM symbol Frequency domain description

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. Besides jamming, the system in the simulation is subjected to multipath fading and additive white Gaussian noise. 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.

Table 2: Physical Layer Parameters and Their Values for Simulation [7]

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. But in practical there are so many issues related to antennas which will be discussed later.

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.

$$\frac{B_J}{B_{VS}} = \frac{Jammerbandwidth}{Victimsystembandwidth} \dots\dots\dots\dots(1)$$

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

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

The measurement was conducted by transmitting constant length (8 kb) UDP (User Datagram Protocol) packets over the connection, with a constant transmission rate of 95 % of the measured maximum throughput allowed by the selected modulation/coding combination. The transmission rate was selected 5 % lower than the maximum to make sure that no errors occur because of the small fluctuations in the system capacity caused by the software, computers, network adapters' etc. signal to noise ratio is given by the following equation. Here noise power is jamming signal power.

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

V. DESIGN OF JAMMER IN OPNET MODELER

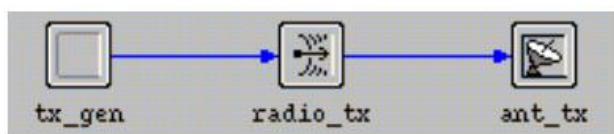The transmitter node model of jammer is given in the figure.

Figure 2: 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. The pointing processor makes this calculation by using a Kernel Procedure that converts a node's position in a subnet (described by the x position and y position attributes) into the global coordinates that the antenna requires.

The radio_tx is radio transmitter module which transmits packets to the antenna at 1024 bits/second, using 100 percent of its channel bandwidth. 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
Results are generated by the software simulation. Performance of the IEEE 802.16 system is measured in terms of the QOS parameters. With out jamming throughput is maximum (97%) and packet error rate is minimum. The result of video conferencing is shown below. Video conferencing application is simulated using WiMAX for one minute with parameters defined in simulation section.
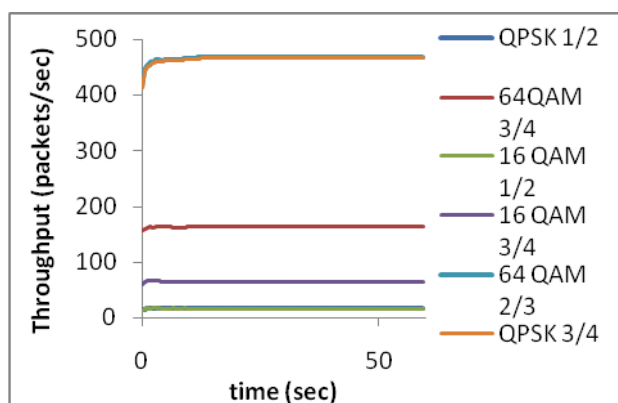

Figure 3: Result of video conferencing application using WiMAX for period of one minute without jamming.

With jamming the throughput of the system decreases and packet error rate increases. Jamming power required for certain values of PER and specific modulation schemes are given below. Modulation and simulation parameters are described in simulation section.

Table 3: Jamming power (dB) required for specific modulation scheme and PER in downlink

PER	QPSK 1/2	QPSK 3/4	16 QAM 3/4	64 QAM 2/3	64 QAM 3/4
5%	-35.8	-40.1	-43.8	-42	-43.3
30%	-34.8	-39	-42.7	-40.6	-41.9
60%	-33.8	-38.5	-41.9	-39.8	-41.2

The result shows that jamming power increases for higher values of PER for particular modulation scheme. As jamming power is increased PER also increases so throughput decreases. Signal to noise ratio decreases as the jamming power increases. Simulated results give idea about the practical scenario. Practical results may be different from simulated results but concept remains same.

VII. ISSUES AND OVERVIEW OF JAMMING REDUCTION TECHNIQUES
There are number of issues related to practical approach. Simulation approach is easy but not reliable because the results depend on the software and its limitation. In simulation some results may not be generated but it is cost effective solution. In practical there are so many issues related to antennas used to produce jamming signal. The placement of jamming antenna and its polarization also affects in practical case. Scrambling is very difficult to simulate because it targets the part of packet [3]. Practical approach is very useful to perform scrambling. Smart antennas are not included in the software but it can be used practically. Polarization of the victim system antenna and jamming antenna is not matched then it results in the loss of power. Some practical parameters can not be included in software. There are several techniques to reduce the jamming.

A. BEAMFORMING
It is the technique to improve the directionality of the antenna. This technique is useful in the base station which uses sector pattern instead of the Omni directional antenna. Let's consider three sector of base station antenna. If jamming antenna is in sector one then the other two sectors are less affected by the jammer. This technique is useful in reducing jamming effect but it can not remove it. This technique is very difficult to implement because reduction of the main lobe of antenna is complicated.

B. JAMMING RESISTANT ARCHITECTURE
This jamming resistant architecture is also used to reduce the jamming effects [6]. In this architecture more than one base station is used in one cell. All subscriber stations are connected in mesh topology including base stations which is serving in particular cell. Let's consider two base stations in one cell. If jamming is introduced and one base station fails then the all subscriber stations served by that base station are automatically

connected to other base station. There is one major problem in this architecture related to scheduling. Scheduling is the mechanism which is used by the base station to assign the resources to the subscriber stations. There are more than one base stations in one cell so distributed scheduling must be used. Distributed scheduling is very complicated so it is very difficult to design it. Scheduling is the mechanism which is used by the base station to assign the resources to the subscriber stations.

C. OFDM-CDMA
OFDM and CDMA can be combined to reduce the jamming effect. CDMA has anti-jamming capability which can be used with OFDM. This is very new technique and implementation is possible.

VIII. CONCLUSION
The performance of the WiMAX (IEEE 802.16) is degraded under jamming. Jamming can be detected easily but it affects the system badly and sometimes system may fail. In this paper, the performance of IEEE802.16-2004 based system under both multi-tone pilot and partial-band jamming are evaluated with the aid of computer simulations. The results show that the simulated throughput versus jamming power curves descends faster for weaker modulation/coding modes, indicating that weaker modes possess lower tolerance to jamming. Saturation phenomena to most of the jamming scenarios are observed for system operating. It proves the necessity and robustness of this newly defined operation mode. Multi-tone pilot jamming affects the system more severely than partial-band jamming under the same jamming power. In multi-tone pilot jamming, the number of jammed pilots decides the jamming severity and jamming 8 (full) pilots degrades the system to the most. In partial band jamming, system performance is degraded by either increased power of sub jammer or increased number of sub jammer, depending on the level of jamming power.

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 Enviornment 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-Hennawy, 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,kerela,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, Suresh Limkar and Dr. Upena Dalal "A Performance Comparison of Routing Protocols(DSR and TORA) for Security Issue In MANET(Mobile Ad Hoc Networks) " IJCA Special Issue on MANETs (2):78–83, 2010. Published by Foundation of Computer Science.

Mr. Jha Rakesh presently is full time Research Scholar at S. V. National Institute of Technology, Surat, INDIA. He has completed his B.Tech. (Hons in Electronics) from Bhopal and obtained M.Tech. (Wireless Communications) from NIT, Jalandhar, India.He have done live project in development and support both in Industries also. He has published many conferences and journal papers at national and international level including Scientific Research Journal. His one concept related to Router of Wireless Communication is accepted by ITU (International Telecommunication Union).He is now pursuing PhD in S. V. National Institute of Technology, Surat, INDIA. Surat. His research interest's area is Wireless and Optical Communication. Currently he is doing his research work in WiMAX and its Security issues. He is working on OPNET simulation and NS2 tools for Wireless Communication.

https://sites.google.com/site/jharakeshnetworkcom/

Dr. (Mrs.) U. D. Dalal presently working as Associate Professor in Electronics Engineering Department of S. V. National Institute of Technology, Surat, INDIA. She has 18 years of academic experience. She completed her B.E. (Electronics) from SVRCET, Surat in 1991 and obtained M.E. (Electronics & Communications) from DDIT, Gujarat with Gold Medal. She is also awarded with 5th N.V. Gadadhar memorial Award by IETE. She has published many conference and journal papers at national and international level. She has guided many UG and PG projects, dissertations and seminars in the area of advance communication systems. She has completed Ph.D. in 2009 and guides 5 research scholars presently. Her book on "Wireless Communication" is published by Oxford University Press in July 2009. One more book edited by her and Dr Y P Kosta titled "WiMAX New Developments" is published by Inteh, Vienna, Austria. She is honored by "Rashtriya Gaurav Award" by India International Friendship Society. Recently she is received Best Technical Woman award by Divyabhaskar.