WiMAX and Its Security Issues: Performance Analysis, Cross Layer Optimization and Security issues

Rakesh Kumar Jha, Upena D Dalal
Department of Electronics and Communication Engineering, SVNIT Surat, India
upena_dalal@yahoo.com, Jharakesh.45@gmail.com

Abstract. We have proposed Location based network (LBN) for WiMAX and observed the performance and optimized the network with security issues. The scope of this paper is designed the network with optimal BS (Base Station) with case study of one district analysis (Jalgaon, Maharashtra, India) in first phase. After that we observed the performance analysis with QoS (quality of service) with different scheduling aspects of WiMAX Technology. In Second phase we have designed Location Based network (i.e Surat, India is Location for study in our case).Once the network has designed we have optimized the network with Power Optimization and Cross Layer (PHY-MAC Layer) Optimization. In third or in last phase we have done the performance analysis of security expects in PHY Layer (Jamming) and Network Layer (Misbehavior Node) since we know that MAC Layer of WiMAX is well secured so PHY and Network Layer is most sensitive as far as security concerns. There has been a rapid growth in various wireless networks in recent years. Along with that the demand for wireless data services and multimedia applications has grown. To provide better service to meet the growing demand, there has been lot of research in the field of QoS. The scheduling policy i.e. the algorithm to allocate slots is not defined in WiMAX specifications It is open for alternative implementation. Resource Allocation for Downlink OFDMA in WiMAX Systems is very important. Location Based Performance of WiMAX Network for QoS with Optimal Base Stations (BS) with respect number of users and demand is new and a part of Next Generation Network (NGN). Network optimization and security expect played major role to adopt new technology. Security is an important concern for the network operator and the network user. In rough environments where there is constant traffic, a jamming attack causes serious problems; therefore measures to prevent these attacks are required. The purpose of this thesis is to explore the underlying principles of jamming attacks (i.e., the effects of modulation techniques, inter arrival times of packets, transmitter’s and jammer’s power) using OPNET as the simulation tool. This work will be helpful so that in future research a useful, practical and effective solution can be created to countermeasure the effects of jamming attacks. The objective here is to understand, modify, and employ the models in OPNET 14.0 to simulate jamming attacks and understand the limitations of the available models. After PHY Layer attack we have done the work on misbehavior node i.e Network Layer attack. In the next phase we are doing the work on adaptive power optimization on the BS with Proportional algorithm or Hidden Markov model. As far as security concerns our next work on how we can protect misbehavior attack and An Effective Defense Mechanism for Detection of DDoS Attack on Application Layer Based on Hidden Markov Model

Keywords: WiMAX, PHY Layer, MAC Layer, Network Layer, LBN, Security, HARQ, ARQ