Conclusions and Future Scope
7.1 Conclusions

WiMAX is one of the most emerging technologies that enable ubiquitous delivery of broadband wireless access in this modern era of communication for mobile as well as fixed users. The real success of this technology is that it provides services to users according to their demand. In order to guarantee QoS to its users, WiMAX addresses multiple constraints. Being a wireless technology it has to deal with transmission error rates which may cause hindrance in achieving QoS requirements. Also, as the users are mobile, so there are constant changes in routes which result in handover delays from one route to another which are unavoidable and negatively affect real time services. With mobility, providing proper security to the users is necessary. On the other hand, QoS provisioning and security guarantee are always contrary to each other.

In order to investigate QoS parameters in WiMAX networks QualNet 7.3.1 wireless network simulator was used. Simulation studies were carried out on different types of traffic and different simulation scenarios. The results obtained after the simulations revealed that Constant Bit Rate traffic can be best served by Unsolicited Grant Service (UGS) flow as it serves the traffic in the most optimum way. Similarly, the simulation investigations on Variable Bit Rate traffic show that it is served in the most optimum way by the real time Polling Service (rtPS) flow whereas File Transfer Protocol is best served by non real time Polling Service (nrtPS) flow.

A comparison of various investigated encryption algorithms used for network security have been explained in brief. Also a security mechanism has been proposed and its working has also been illustrated. The performance parameters; encryption time, decryption time and throughput have been evaluated for the proposed algorithm and other investigated algorithms i.e. DES, 3DES, AES, serpent, blowfish and RC4 for various types of data blocks. Results revealed that the proposed algorithms showed better results as compared to other algorithms. Hence the proposed algorithm can be used for encryption of any type of data blocks.

A brief description of various encryption techniques is provided. The thesis deals with investigation of security techniques in WiMAX networks. For this, various scenarios are simulated using MATLAB 8.3 R2014a. The simulations are carried out with and without using AES, DES, RSA and proposed RSA encryption algorithm for three different modulation techniques BPSK, QPSK and QAM with code rates of \( \frac{1}{2} \) in order to investigate their impact on WiMAX networks. Results of these simulations
revealed that information is more secure after using the encryption standard. Out of all encryption techniques investigated, the proposed RSA technique demonstrated better results with respect to all performance parameters in WiMAX scenarios.

Investigations were also carried out to analyse the impact of jamming in WiMAX networks. Results reveal that proposed RSA algorithm works in a much better way than other prevalent encryption algorithms. Hence, proposed RSA can be used as a simple and efficient technique to recover from jamming in WiMAX networks.

### 7.2 Future Scope

In the new era of communication, WiMAX (IEEE 802.16) is the most emerging technology that enables ubiquitous delivery of broadband wireless access for fixed and mobile users. It is a more innovative and commercially viable alternative to cable modems and DSL technologies as it is cost effective, easy to implement, high performance and high resource utilization technology. Even though, a lot of research has already been conducted but as it is a challenging topic, future work should include studying the quality of service parameters in great detail so that this emerging technology can provide excellent services to the users and that too at very cheap rates. Further work can be carried out by studying QoS parameters by varying antenna heights and for different simulation areas. Also, various different types of traffic like VoIP can be evaluated over different service flows and the impact of various schedulers on services can be investigated. Further work could be carried out by considering more number of nodes and also by taking into account various encryption algorithms and also analysis could be done by selecting more number of parameters, so as to judge effectiveness of algorithms. New security solutions should be proposed as these networks are prone to variety of malicious attacks by the attackers. In order to make this emerging technology a real success, research should be carried out to combat all the loopholes prevailing in this ubiquitous technology.