CHAPTER 6

CONCLUSION

Being a wireless technology, WiMAX is also susceptible to attacks. We proposed a security scheme to enhance the capabilities and functionality of the WiMAX Network so that there will be secure interchange of data. In the proposed scheme ECC encryption was used instead of RSA. ECC has a key size (163 bits) lesser than that of RSA (1024) and it provides same strength as of RSA. In our proposed scheme we used the OMAC (One Key CBC MAC) as hashing function. OMAC algorithm is very simple and it provides pretty good prevention against the replay attacks. Due to mutual authentication in the proposed scheme Man in the Middle Attack and Rouge Base Station attacks can be prevented. Time Stamps and nonce were also used in the proposed scheme to prevent the DoS and Replay attacks. Thus the proposed security scheme is safe and data can be exchanged securely.

Decision regarding gateway relocation can be taken by the ASN in WiMAX network. A consideration is made in this thesis that the load is very heavy on the ASN gateway due to which gateway relocation will be performed by the connected MSs forcefully. This thesis proposes an AMST based algorithm for ASN gateway relocation which is used for proper selection of MSs to perform gateway relocation and also selects the appropriate time for gateway relocation. Suitable selection of mobility method (ASN or CSN connected mobility) can be selected by the ASN gateway depending on the AMST of MS and the load on the gateway. The results clearly shows that load on ASN gateway can be reduced using AMST based algorithm and load on gateway is more stable than the Proper C4 mobility and predictive ASN gateway relocation algorithm. Moreover it reduces the handover time compared to other Methods of mobility.
Future Scope

Computer based simulation tools were used to obtain the results and these results were not verified in the real environment, thus in future we can try to implement our proposed schemes in the real environment to obtain the real environment results.