Abstract

Data transmission security is an essential part of wireless network engineering. Since access to the network cannot be restricted physically, cryptographic methods must be used to protect transmitted data and network elements. Aspects that should be considered are data confidentiality, data authenticity and service availability .Systems designed today should be made secure enough for the future users to feel safe to use them.

The third generation (3G) systems will provide high speed mobile access to Internet based services. One can expect high speed access to the Internet, entertainment, information and e-commerce services wherever he is.3G technologies will greatly improve the use of radio spectrum allowing operators to send data across wireless networks at up to 2 Mbps. The evolution from 2G to 3G will introduce threats and opportunities of the Internet to the world of mobile communications . The 3G systems have to adopt a new policy and build an Internet alike security architecture.

Lot of research work is being done in the areas of performance evaluation of software ciphering, end-to-end security for 3G networks ,Low power encryption and VLSI as well as DSP implementation of 3G security algorithms.

Major contributions of this thesis are : Comprehensive study of 3G mobile network security features, Review of 3G communication protocols and cryptographic algorithms, Implementation considerations for cryptographic algorithms, Implementation of major algorithms on MATLAB/SIMULINK ,DSP and VLSI platforms and their integration with communication protocols, Comparative analysis of various implementations for encryption speed and memory requirements and Development of GUI based demonstration program for the work reported in the thesis for academic use.