Chapter 1
Introduction

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 [2].Systems designed today should be made secure enough for the future users to feel safe to use them.

First generation (1G) cellular systems such as Nordic Mobile Telephone (NMT), Advanced Mobile Phone System (AMPS) and Total Access Communication System (TACS) are nowadays considered quite insecure. The cloning of the analog terminals is possible and in some systems widespread. Terminal cloning compromises the security of charging, which leads to loss of profit and reduces consumer's trust on mobile service. In many cases ,the lack of security has been the main reason for the decision to prematurely close the 1G networks.

Second generation (2G) mobile communication systems use digital radio transmission techniques and digital speech coding.2G systems were designed primarily for voice ,although they now also support a limited amount of low speed data communication . The 2G systems include the GSM family which has been adopted worldwide, Personal Digital Communications (PDC) used in Japan and IS-136 TDMA and IS-95 CDMA used in the US. The use of digital technology enhances security in two principal ways [2] :

- Digital technology allows the use of cryptographic methods for authentication and encryption
- Monitoring digital transmission on the radio interface requires specialized equipment which are not freely available.

GSM based mobile systems provide mobile user authentication and security over the radio interface as an integrated part of the system. The GSM security [3],[4] is based on trust between network operators and on a shared secret key (Ki) stored on the user's SIM and in the Authentication Centre (AuC) of the operator. Authentication and data encryption is achieved by distributing

triplets to the network elements serving the mobile network. The encryption algorithm used in GSM are of the A5 type with effective key length of 54 bits. In the packet mode of GSM called GPRS (General Packet Radio Service),payload packets are encrypted between the Mobile station and serving router thus covering the link between the router and the Base station.

The third generation (3G) [5] systems will provide high speed mobile access to Internet based services.3G services will add an invaluable mobile dimension to services that are already an integral part of modern business life. 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 will be IP based and at least partially connected to the Internet. IP networks are open networks which do not separate signaling from user data. This allows malicious users to exploit the faults of protocol stacks to gain access to data or network resources. The 3G systems have to adopt a new policy and build a Internet alike security architecture (firewalls , virtual private networking ,end-to-end encryption etc.)

Implementing security in wireless systems is a difficult and challenging task owing to mobility of users and network components and the fact that wireless medium is susceptible to eavesdropping, espionage and fraud. The inherent security problems of mobile networks are due to

- User mobility – requires global authentication for security and privacy
- Network components- mobile hosts are resource deficient in order to perform computations for security and privacy
- Wireless connectivity- requires additional communication and computing because of high bit error rate

Security in wireless systems can be studied at various levels namely:

- Framework/Organizational: deals with the architecture of the security system and includes security rules, management of security modules
- Technical: deals with the implementation issues including mechanisms and paradigms

- Physical: deals with the physical security of the equipment and installations.

Communications on shared media like radio communication are no longer private. Privacy and authentication are lost unless some method is established to regain it. Cryptography provides the solution to regain control over privacy and authentication. All digital mobile systems provide security through some kind of encryption system. Data can be encrypted in many ways, but algorithms used for secure data transfer fall into one of the two broad categories : Symmetric and Asymmetric .Both rely on performing mathematical operations using a secret number known as a key. Symmetric algorithms depend on both parties knowing the keys. Larger key means better encryption. DES and A5 are examples of symmetric algorithms. The difficulty with symmetric algorithms is that both parties need to have a copy of the key. To transmit the key freely over the air would render the whole exercise pointless. Asymmetric algorithms use two separate keys for encryption and decryption. Usually , the encryption key can be publicly distributed, while the recipient holds the decryption key securely. RSA is an example of asymmetric algorithm.

The following is a list of examples of wireless security breaches and thefts which are major contributors to the loss of revenue for cellular operators:

- Equipment theft and modification
- Theft of air time
- Breaches in network security, causing loss of confidential information
- Breaches in the integrity of billing systems
- Misuse of customer database information
- Vandalism at cell sites
- Loss of customer and industry confidence

1.1 Motivation : Security is becoming a major cost factor in the industry , since the cellular carriers have been diverting much of the income to tracking down these problems. The money that is being diverted is obviously better suited to network enhancements than to problem resolution.

UMTS (Universal Mobile Telecommunications System) requires that end users of the system are authenticated. Cryptography provides the required

solutions for network operators and subscribers. One of the major security features of 3GPP system specifications (Release 1999) is mutual authentication. The authentication mechanism of UMTS involves Home Environment (HE), Serving Network (SN) and terminal containing USIM. (Universal Subscriber Identity Module) The serving network checks the subscriber's identity by a challenge and response mechanism. The terminal also checks that the serving network has been authorized by the home network to do so. For radio access network encryption and protection, the most important one is the 128 bit secret key which is shared between USIM smart card in user's terminal and Authentication Center in user's home network. The keys used in encryption and integrity protection are derived from this key. Data is transferred encrypted between a terminal and a radio network controller (RNC) .Encryption and integrity protection are symmetric operations, thus exactly same algorithm is executed both in terminal and in RNC. The confidentiality algorithm f8 is a stream cipher being able to encrypt/decrypt blocks of data between 1 and 20000 bits in length[7]. Algorithm takes five input parameters and generates random looking mask that is applied to the plaintext .Internally f8 uses KASUMI block cipher[16] .KASUMI block cipher is applied as many times as necessary and one KASUMI round produces 64-bit mask. KASUMI is an 8 rounds Fiestel network with a block size of 64 bits and a key length of 128 bits. The designers of KASUMI specially tailored it to achieve high throughput on both hardware and software platforms. Integrity algorithm f9 is used to implement the integrity protection between a terminal and a network. Sending party uses f9 to generate message authentication code (MAC-I) and receiving party uses f9 as well to verify the identity of the sender. It also takes five input parameters and produces the integrity code that is appended to the end of signaling message. KASUMI algorithm is also utilized in f9.The result of integrity verification is a 32 bit integrity code MAC-I.

Lot of research work is being done in the following areas [12] - [17],[20]

- Performance evaluation of software ciphering in radio network controller
- End –to-end security for 3G networks
- Low power encryption

- DSP/ VLSI implementation of encryption algorithms
- MATLAB and SIMULINK implementation of encryption algorithms

The field of implementing cryptographic algorithms on special platforms is very active. However, the research done on implementation of cryptographic scheme on a DSP is limited. There are only one to two research papers about implementation of AES candidates on a DSP [20]. Present research also explores the various trade-offs in applying Field Programmable Gate Arrays(FPGAs) ,Digital Signal Processors(DSPs) and Application Specific Integrated Circuits (ASICs) to the design of a mobile communication unit .This research studies focus on encryption for mobile communication [36]. There are research papers on VLSI implementations of KASUMI block cipher [38], [43], [45] . However, very few research papers describe about MATLAB and DSP implementation of 3G security algorithms. The powerful simulation tool SIMULINK is nowadays used for 3G wireless system simulation but its use in study of encryption and decryption has been negligible. The tremendous computing power of MATLAB can be used for implementing various cryptographic algorithms and can be further extended to SIMULINK for system level studies [42], [43]

Based on study of research work already done in above mentioned areas, authors were motivated to take up research work in the area of implementation of cryptographic algorithms on various platforms . Their relative merits and demerits were of prime importance so as to integrate them with communication protocols in various layers of the network.

1.2 Major Contributions of the Thesis:

Major contributions of this thesis are :

- Comprehensive study of 3G mobile network security features
- Review of 3G communication protocols
- Review of 3G cryptographic algorithms
- Implementation considerations for cryptographic algorithms
- Implementation of major algorithms on MATLAB,DSP and VLSI platforms and their integration with communication protocols

- Comparative analysis of various implementations which are done by authors and those already done by researchers
- Development of GUI for encryption/decryption algorithms for academic use

1.3 Organization of the Thesis:

The thesis is organized in total ten chapters as described below :

Chapter: 1 It provides details about motivation for research work , major contributions of the thesis and organization of the thesis.

Chapter: 2 It gives details about vision for 3G mobile systems, Existing mobile network architecture, Evolution to 3G networks and comparison of 2G and 3G networks .

Chapter: 3 It describes Privacy needs of a wireless system, Examples of wireless security breaches and thefts, General objectives of 3G security features and UMTS access security .

Chapter: 4 It describes UTRAN protocol structure and protocols in Physical Layer, MAC Layer and RLC Layer . Mobile IP architecture and protocol stack are also discussed in this particular chapter.

Chapter: 5 It gives details about cryptographic algorithms for Confidentiality , Integrity, Authentication and Key Generation . Besides discussing the core algorithm KASUMI, we discuss functions, operations, interfaces and requirements for f8 and f9 algorithms. AES and IDEA algorithms for enhanced security of 3G networks are also discussed.

Chapter: 6 It describes software implementation of algorithms which includes MATLAB/SIMULINK and DSP implementations. The Algorithms implemented in MATLAB are AES, KASUMI, f8 and f9. SIMULINK blocks for f8 and f9 are designed. DSP implementation includes AES, IDEA, KASUMI, f8, f9 and MILENAGE. GUI based demonstration program developed in MATLAB is discussed at last in this chapter. This GUI based program can be used as an academic tool.

Chapter: 7 It describes hardware (VLSI) implementation of algorithms using VHDL programming .Important considerations and advantages of

hardware implementation are also mentioned in this chapter. KASUMI , f8,f9 and IDEA algorithms are implemented in hardware .

Chapter: 8 It describes integration of cryptographic algorithms in network architecture as per 3GPP integration guidelines.

Chapter: 9 It contains discussion of the results and conclusions derived from results .It also discusses the scope of future work. Comparisons of MATLAB, DSP and VLSI Implementations are done. Important conclusions regarding integration of these algorithms in network architecture are given in this chapter.

Chapter: 10 It contains Bibliography.