2 Fundamentals of Wireless Communications

D. Shen and V.O.K. Li

The University of Hong Kong, Pokfulam Road, Hong Kong

2.1 Introduction

Since the introduction of the first generation cellular networks in the 1980s, there has been tremendous growth in wireless communications. In 1992 the first commercial GSM network was launched, which marked the beginning of era of digital cellular networks. Since 2003, Hutchinson has launched 3G services in Hong Kong, UK, and Italy. Today, wireless communication devices have penetrated almost every corner of the world and have become an indispensable part of our daily life. In this chapter, we present a brief overview of 2G/2.5G and 3G wireless communication systems, with particular focus on security-related aspects.

2.2 Global System for Mobile Communication

Global System for Mobile Communication (GSM), is currently the most widely used wireless technology. The number of global GSM customers is estimated to be over 1 billion as of the first quarter of 2004, accounting for over 70% of the global market share.

GSM was proposed in Europe (in fact, the initials were originally derived from Groupe Special Mobile) and was under standardization by the European Telecommunication Standards Institute (ETSI). Currently, the work has largely been transferred to third generation partnership project (3GPP).

2.2.1 Overview

Currently, GSM operates in frequency bands of 400, 800, 900, 1,800, and 1,900 MHz. A GSM channel has a bandwidth of 200 kHz. The modulation scheme is Gaussian minimum shift keying (GMSK), which is a type of continuous 7-phase modulation scheme. Since GMSK has a constant amplitude envelope, it is desirable for simple amplifiers. At the same time, it has a narrow power spectrum with low adjacent channel interference. The duplexing scheme is frequency division duplexing (FDD), with the uplink channel and downlink channels located in different frequency bands. Since the uplink time slot is about three time slots later than the corresponding downlink slot, the mobile station (MS) does not have to send and receive at the same time, thus reducing system design complexity and cost.

In Fig. 2.1, we illustrate the processing of a GSM voice call. At the transmitter, the voice is first digitized and source encoded. Then channel coding (convolutional coding) and interleaving are applied for error correction. To achieve confidentiality over the air interface, encryption is performed. After modulation, the user signal is transmitted over the multipath fading channel. At the receiver, the received signal is first demodulated, and then decrypted. After deinterleaving and channel decoding, source decoding is conducted to restore the speech.

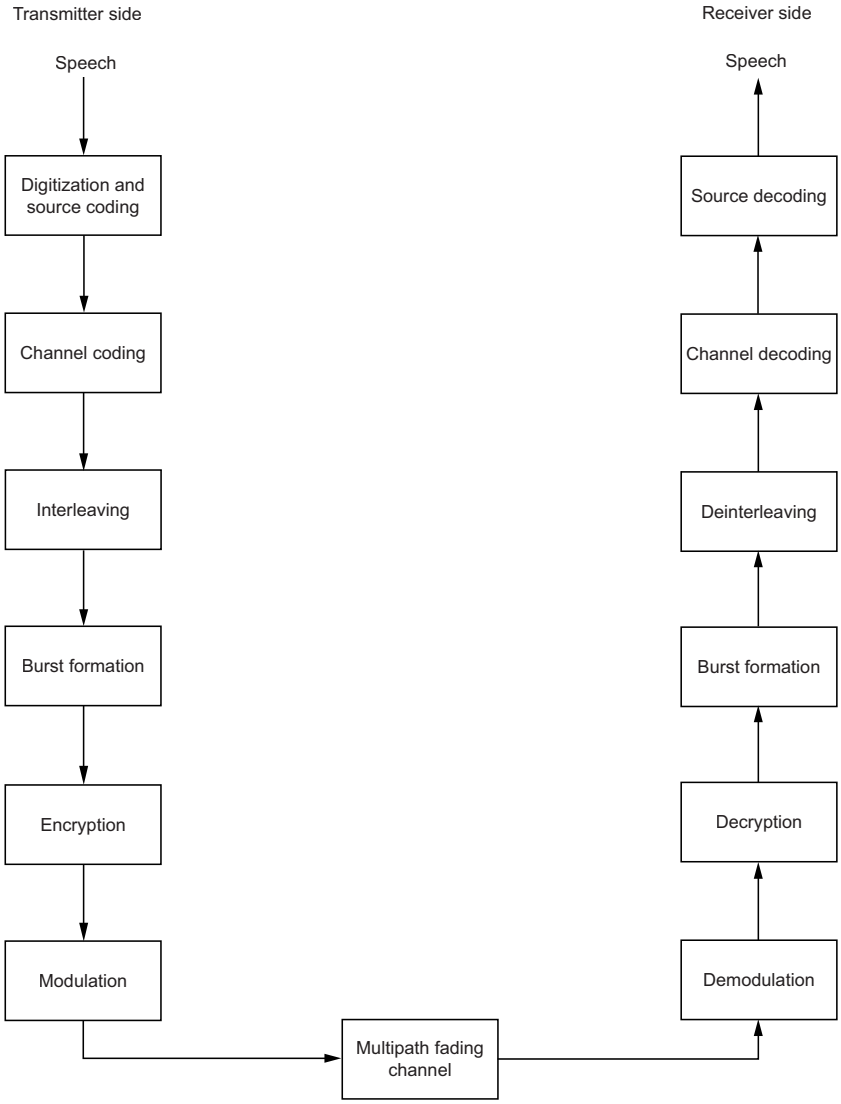

Fig. 2.1. Processing of a voice call