UNIQUE SECURITY FEATURES OF CDMA

MAMUN UR RASHID (M..Sc. in Telecommunication Engineering), Lecturer, Southern University
MD. ASADUZZAMAN KHAN (M..Sc. in Telecommunication Engineering), Lecturer, Southern University Bangladesh

ABSTRACT
Security system is a very essential term in wireless communication like multiple accesses. When we go through multiple access method we will find TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access) are working with time & frequency respectively. For security purpose TDMA and FDMA have to apply additional security features to keep those channels secure. Whereas in CDMA (Code Division Multiple Access) it has its own coding technique and it gives us auto security for data. The security features are coming from PN Sequence (for spreading), Walsh code (for channel coding) and power control. In this sequence CDMA is developed for further wireless communication such as 3G and 4G which overcomes GSM technique.

INTRODUCTION

One of the most important concepts to any cellular telephone system is that of "multiple access", meaning that multiple, simultaneous users can be supported. In other words, a large number of users share a common pool of radio channels and any user can gain access to any channel (each user is not always assigned to the same channel). A channel can be thought of as merely a portion of the limited radio resource which is temporary allocated for a specific purpose, such as someone's phone call. A multiple access method is a definition of how the radio spectrum is divided into channels and how channels are allocated to the many users of the system.

CDMA is a "spread spectrum" technique in which each phone in a cell uses a distinct code known to the base station to communicate with the base station. All frequencies in one cell can be used in other cells. Code division multiple access (CDMA) is a channel access method utilized by various radio communication technologies. We should not confuse it with the mobile phone standards called cdmaOne and CDMA2000 (which are often referred to as simply CDMA). This uses CDMA as an underlying channel access method. One of the basic concepts in data communication is the idea of allowing several transmitters to send information simultaneously over a single communication channel. This allows several users to share a bandwidth of frequencies. CDMA employs spread-spectrum technology and a special coding scheme (where each transmitter is assigned a code) to allow multiple users to be multiplexed over the same physical channel. CDMA is a form of "spread-spectrum" signaling, since the modulated coded signal has a much higher data bandwidth than the data being communicated.[1]

A simple example to the problem of multiple accesses is a room (channel) where people wish to communicate with each other. To avoid confusion, people could take turns speaking (time division), speak at different pitches (frequency division), or speak in different languages (code division). CDMA is the last example where people speaking the same language can understand each other, but not other people. Similarly, in radio CDMA, each group of users is given a shared code. Many codes occupy the same channel, but only users associated with a particular code can understand each other.

Multiple Access Comparison

A common multiple access method employed in new digital cellular systems is Time Division Multiple Access (TDMA). TDMA digital standards include North American Digital Cellular (known by its standard number IS-54), Global System for Mobile Communications (GSM), and Personal Digital Cellular (PDC).
TDMA systems commonly start with a slice of spectrum, referred to as one "carrier". Each carrier is then divided into time slots. Only one subscriber at a time is assigned to each time slot, or channel. No other conversations can access this channel until the subscriber's call is finished, or until that original call is handed off to a different channel by the system

It is easier to understand CDMA if it is compared with other multiple access technologies. The following sections describe the fundamental differences between a Frequency Division Multiple Access Analog technology (FDMA), a Time Division Multiple Access Digital technology (TDMA) and a Code Division Multiple Access Digital technology (CDMA).

FDMA - Frequency Division Multiple Access is used for standard analog cellular. Each user is assigned a discrete slice of the RF spectrum. FDMA permits only one user per channel since it allows the user to use the channel 100% of the time. Therefore, only the frequency "dimension" is used to define channels.

TDMA - Time Division Multiple Access the key point is to make is that users are still assigned a discrete slice of RF spectrum, but multiple users now share that RF carrier on a time slot basis. Each of the users alternates their use of the RF channel. Frequency division is still employed, but these carriers are now further sub-divided into some number of time slots per carrier [2].

A user is assigned a particular time slot in a carrier and can only send or receive information at those times. This is true whether or not the other time slots are being used. Information flow is not continuous for any user, but rather is sent and received in "bursts." The bursts are re-assembled at the receiving end, and appear to provide continuous sound because the process is very fast.

CDMA - Code Division Multiple Access uses a multiple access spectrum spreading technique called Direct Sequence (DS). Each user is assigned a binary, Direct Sequence code during a call. The DS code is a signal generated by linear modulation with wideband Pseudorandom Noise (PN) sequences. As a result, DS CDMA uses much wider signals than those used in other technologies. Wideband signals reduce interference and allow one-cell frequency reuse. There is no time division, and all users use the entire carrier, all of the time.

SECURITY SYSTEM IN WIRELESS COMMUNICATION

We will find some common characteristics in Wireless devices. Important one is that they broadcast information over radio waves. Though they may be encoded differently (some analog, some digital), all radio waves are broadcast in all directions from the point of transmission. This means that any receiver within range that is tuned into the frequency of the signal will receive it. Systems administrators are not able to identify who has accessed the signal, which means that inadvertent disclosure to unauthorized parties is easily possible.

Any time wireless technology is used to transmit personal information, that information must be strongly protected to guard against unauthorized access to the contents of the signal. Sometimes, the mere existence of the signal can divulge personal information. This is the case, for example, with cell phone or other mobile transmissions that reveal a person’s location and movement patterns.[3] Wireless data networking links computers without wires. Because of its low cost, a wide range of individuals, many of whom are not networking specialists, now useWi-Fi equipment. Wireless routers, for example, are increasingly common in home or small office computer networks. If the data are not encrypted the information systems can run the risk of disclosing entire databases of personal data. To prevent data leakage from wireless access points it is vital to secure the entire network, rather than only specific devices.

Cellular phones are rapidly converging and may be regarded as a single category. They can be used not only for voice transmission, but also as wireless modems or web browsers. When used to transmit or store email or instant messages, these devices can pose risks. Security features include the encryption of transmissions, password protection, and automated data wiping. It is also important not to use cell phones to discuss personal or sensitive business information in public places. When using data features on cellular phones do not let their small size deceive you into treating the data with less care than you would on your desktop computer or laptop.

However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level.[4]

SECURITY FEATURES OF CDMA

CDMA has several unique features that make it a cost-effective, high quality wireless solution. In this module we will learn those features especially the security and how they provide advantages in wireless communication. With the advent of second-generation digital technology platforms like TDMA/CDMA, operators were able to enhance their network security by using improved encryption algorithms and other means. Privacy is the inherent property of CDMA technology. CDMA phone calls will be secure from the casual eavesdropper since, unlike an analog conversation, a simple radio receiver will not be able to pick individual digital conversations out of the overall RF radiation in a frequency band.

During the encoding of the radio link from the base station to the mobile, CDMA adds a special "pseudo-random code" to the signal that repeats itself after a finite amount of time which is used to scramble voice and data transmissions. By this Base stations distinguish themselves from each other with the help of transmitting different portions of the code at a given time. Because the signals of all calls in a coverage area are spread over the entire bandwidth, it creates a noise-like appearance to other mobiles or detectors in the network as a form of disguise, making the signal of any one call difficult to distinguish and decode. In other words, the base stations transmit time offset versions of the same pseudo-random code. In order to assure that the time offsets used remain unique from each other, CDMA stations must remain synchronized to a common time reference.

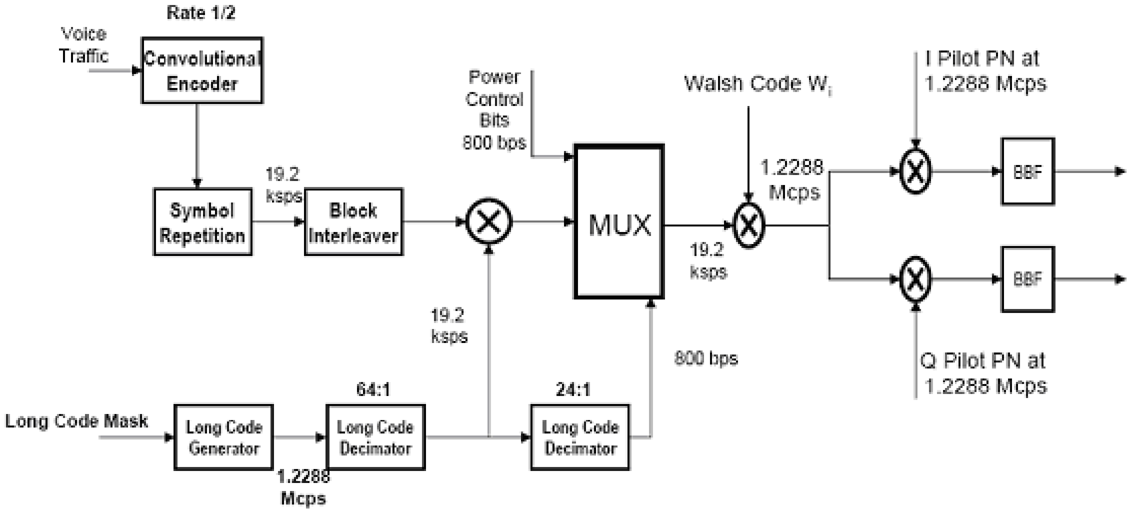

Figure 1: Forward Traffic Control channel in CDMA

CDMA air interface is inherently secure and is clearly superior to first-generation analog and Time Division Multiple Access (TDMA) systems.

The inherent security of CDMA air interface comes from spread spectrum technology and the use of Walsh codes. The soft handoff capability is also a unique feature of CDMA that allows a mobile to connect to as many as six radios in the network, each with its own Walsh code. This means that someone attempting to eavesdrop on a subscriber’s call has to have several devices connected at exactly the same time in an attempt to synchronize with the intended signal. In addition, CDMA employs a fast power control, 800 times per second, to maintain its radio link. It is difficult for a third party to have a stable link for interception of a CDMA voice channel, even with a full knowledge of a Walsh code. Synchronization is critical, as without this synchronization, the listener only hears noise. In order to provide dynamic time-varying power control, the coding and modulation scheme should be designed such that the power control layer is transparent to the decoder; that is, the decoder should not need to know the amount of signal scaling injected by power control in order to perform detection. A simple modulation scheme satisfying this criterion is M-ary PSK: scaling an MPSK signal constellation also scales the degree of noise immunity, as desired, yet leaves the decision regions invariant. [5]

Downlink power control algorithms have been studied and evaluated in this work like The distributed balancing (DB) power control algorithm that is an adaptive approach that uses the received SIR(signal-to-interference ratio) at the mobiles to adjust the transmitted of the base station in order to achieve better global transmission quality, i.e., for the entire network. The algorithm calculates the optimal transmit power assignment for each mobile within the cell, taking into consideration all the neighboring cells. The optimal transmit power assignment for a mobile is proportional to ratio of the total received power of the mobile to the link gain between its base station and itself. [6]

For CDMA 1xEV-DO, the high speed data technology, the forward link utilizes rate control instead of power control and time division multiplexing instead of spreading codes. However, it still has inherent security that protects the identity of users and makes interception very difficult. At last we can say that the TCP has developed for giving the data transmission reliability in wire communication in that sense CDMA has been viewed as the faster technology for some time, despite the fact that GSM is available in more countries. The most recent upgrade to CDMA is CDMA2000 or EVDO, an acronym which stands for Evolution Data Optimized. EVDO operates in much the same way as the standard Internet Protocol (IP) or Transmission Control Protocol (TCP) does.[7] Data exchanged between the phone and the network is transmitted in packets which conserves bandwidth and theoretically increases average speeds across the network. Also new generation’s wireless communication is going to depend on CDMA like WCDMA in 3G as well as 4G.

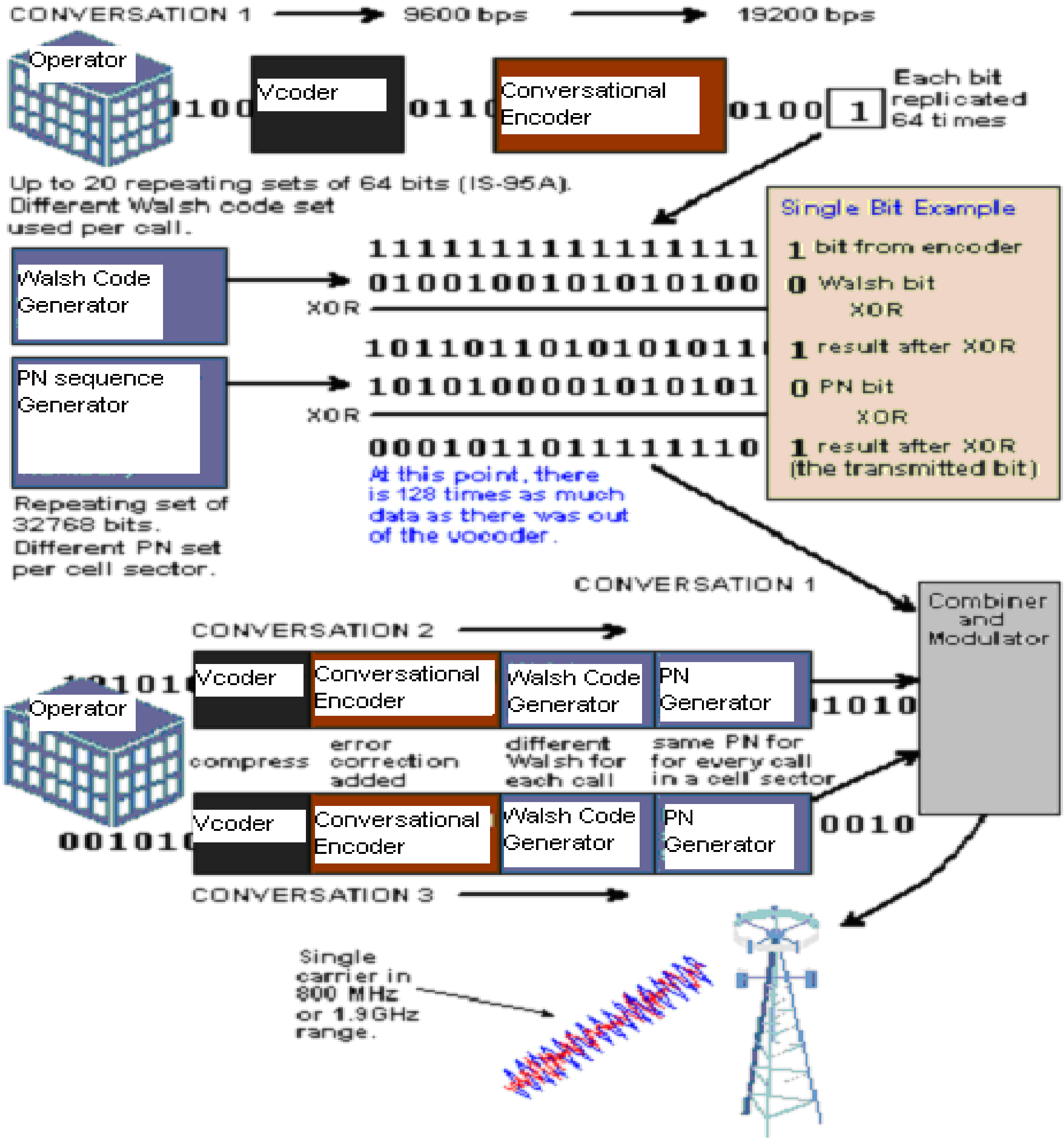

Figure 2: Transmitting CDMA conversation from the Base Station

REFERENCES:

[1] www. wekepida.com

[2] Wireless Communication and Networks, by William Stealing, Edition 4th

[3] Wireless Communication Technologies: Safeguarding Privacy & Security by Ann Cavoukian, Ph.D.Information and Privacy Commissioner/Ontario Fact Sheet Nov14 2007.

[4] Security Aspects of Mobile Wireless Networks, by Mullaguru Naidu, Qualcomm Inc July 2002.

[5] Power Control for Variable QOS on a CDMA Channel, Louis C. Yun and David G. Messerschmitt, Department of Electrical Engineering and Computer Sciences University of California at Berkeley, Berkeley, CA 94720.

[6] Chung-Ju Chang and Fang-Ching Ren. Downlink Power Control in DS/CDMA Cellular Mobile Radio Network. In *Proc.* 3rd International Conf. on Universal Personal Communications (ICUPC'94), pages 89–93, San Diego, CA, 1994.

[7] Wireless Network Security 802.11, Bluetooth and Handheld Devices, Tom Karygiannis & Les Owens, National Institute of Standards and Technology Gaithersburg, MD 20899-8930, November 2002