4G Wireless Systems

Next-Generation Wireless Working Group
Jawwad Ahmad, Ben Garrison, Jim Gruen, Chris Kelly, and Hunter Pankey

May 2, 2003

Contents

1 Introduction **3**

2 Economic Impact **3**
2.1 Advantages of 4G . . . 3
2.2 Problems with the Current System . . . 3
2.3 Barriers to Progress . . . 5

3 Wireless Security **6**
3.1 History . . . 6
3.2 Stakeholders in Wireless Security . . . 7
3.3 Information Security Model . . . 7
3.4 Wireless Security Issues . . . 7
3.5 Security Analysis . . . 9
3.5.1 Objectives . . . 9
3.5.2 Threats . . . 9
3.5.3 Security Architecture . . . 10

4 Current Technology **10**
4.1 TDMA . . . 10
4.2 CDMA . . . 11

5 4G Hardware **13**
5.1 Ultra Wide Band Networks . . . 13
5.2 Smart Antennas . . . 14

6 4G Software **15**
6.1 Software Defined Radio . . . 15
6.2 Packet Layer . . . 16
6.3 Packets . . . 16
6.3.1 Advantages . . . 16
6.3.2 Disadvantages . . . 18
6.4 Implementation of Packets . . . 18
6.4.1 Current System: IPv4 . . . 18
6.4.2 Recommended System: IPv6 . . . 19
6.4.3 Voice over IP (VoIP) . . . 19
6.5 Encryption . . . 19
6.6 Flexibility . . . 20
6.7 Anti-Virus . . . 20

7 Conclusion **21**

List of Figures

1 Cellular Provider System Upgrades 4
2 Information Security Model 8
3 Time Division Multiple Access 11
4 Sending Data using Code Division Multiple Access 12
5 Receiving Data using Code Division Multiple Access 12
6 UWB Spectrum Usage 13
7 Switched Beam Antenna 14
8 Adaptive Array Antenna 15
9 Packet with 896-bit payload 18

List of Tables

1 Cellular Providers and Services 4
2 The Cellular Industry as a Game 5

1 Introduction

Consumers demand more from their technology. Whether it be a television, cellular phone, or refrigerator, the latest technology purchase must have new features. With the advent of the Internet, the most-wanted feature is better, faster access to information. Cellular subscribers pay extra on top of their basic bills for such features as instant messaging, stock quotes, and even Internet access right on their phones. But that is far from the limit of features; manufacturers entice customers to buy new phones with photo and even video capability. It is no longer a quantum leap to envision a time when access to all necessary information — the power of a personal computer — sits in the palm of one's hand. To support such a powerful system, we need pervasive, high-speed wireless connectivity.

A number of technologies currently exist to provide users with high-speed digital wireless connectivity; Bluetooth and 802.11 are examples. These two standards provide very high-speed network connections over short distances, typically in the tens of meters. Meanwhile, cellular providers seek to increase speed on their long-range wireless networks. The goal is the same: long-range, high-speed wireless, which for the purposes of this report will be called 4G, for fourth-generation wireless system. Such a system does not yet exist, nor will it exist in today's market without standardization. Fourth-generation wireless needs to be standardized throughout the United States due to its enticing advantages to both users and providers.

2 Economic Impact

2.1 Advantages of 4G

In a fourth-generation wireless system, cellular providers have the opportunity to offer data access to a wide variety of devices. The cellular network would become a data network on which cellular phones could operate — as well as any other data device. Sending data over the cell phone network is a lucrative business. In the information age, access to data is the "killer app" that drives the market. The most telling example is growth of the Internet over the last 10 years. Wireless networks provide a unique twist to this product: mobility. This concept is already beginning a revolution in wireless networking, with instant access to the Internet from anywhere.

2.2 Problems with the Current System

One may then wonder why ubiquitous, high-speed wireless is not already available. After all, wireless providers are already moving in the direction of expanding the bandwidth of their cellular networks. Almost all of the major cell phone networks already provide data services beyond that offered in standard cell phones, as illustrated in Table 1.

Unfortunately, the current cellular network does not have the available bandwidth necessary to handle data services well. Not only is data transfer slow — at the speed of analog modems — but the bandwidth that is available is not allocated efficiently for data. Data transfer tends to come in bursts rather than in the constant stream of voice data. Cellular providers are continuing to upgrade their networks in order to meet this higher demand by

Table 1: Cellular Providers and Services

Cellular provider	Features
Sprint	e-mail, pictures, games, music, Internet
AT&T	e-mail, games, music
Verizon	e-mail, pictures, games, music, Internet
Nextel	e-mail, pictures, games, music, Internet
T-Mobile (VoiceStream)	e-mail, pictures, games, music, Internet
Cingular	text messaging

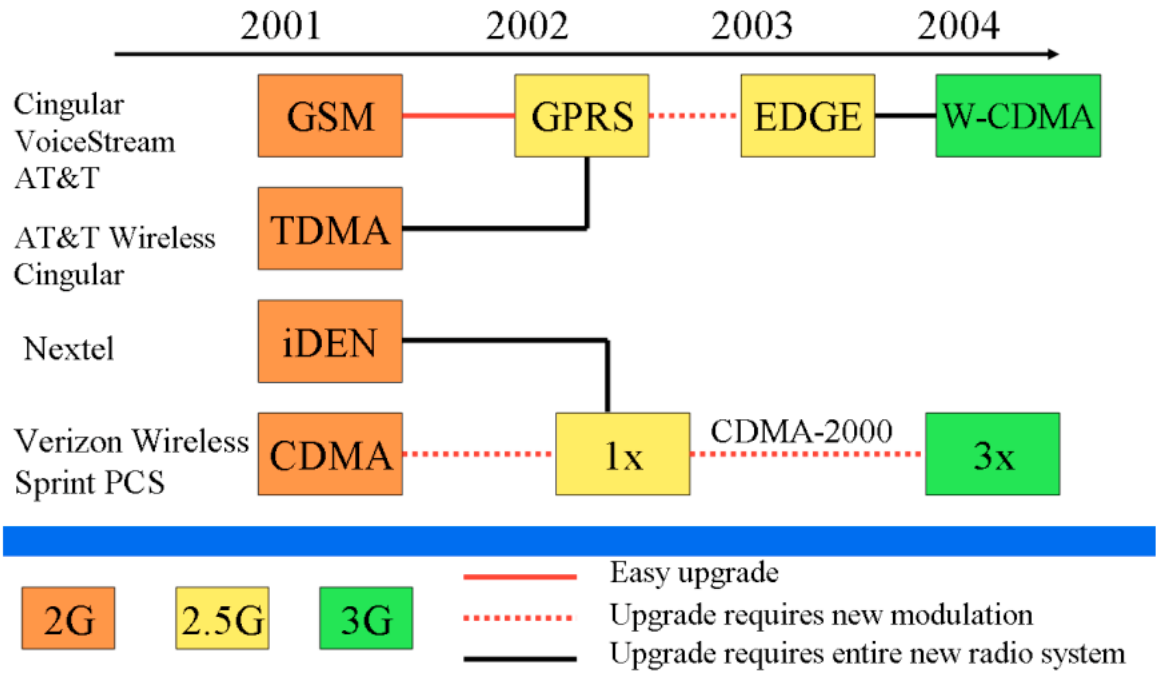

Figure 1: Cellular Provider System Upgrades

switching to different protocols that allow for faster access speeds and more efficient transfers. These are collectively referred to as third generation, or 3G, services. However, the way in which the companies are developing their networks is problematic — all are currently proceeding in different directions with their technology improvements. Figure 1 illustrates the different technologies that are currently in use, and which technologies the providers plan to use.

Although most technologies are similar, they are not all using the same protocol. In addition, 3G systems still have inherent flaws. They are not well-designed for data; they are improvements on a protocol that was originally designed for voice. Thus, they are inefficient with their use of the available spectrum bandwidth. A data-centered protocol is needed.

If one were to create two identical marketplaces in which cellular providers used 3G and 4G respectively, the improvements in 4G would be easy to see. Speaking on the topic of 3G, one of the worlds leading authorities on mobile communications, William C.Y. Lee, states

Table 2: The Cellular Industry as a Game

Players	The cellular providers
Strategies	Upgrade to 4G, or make small incremental changes
Outcome	This can be simplified to the cost of conversion. The cost of conversion (because of economies of scale), depends on the number of companies that actually convert to 4G — networking equipment and wireless access equipment will get cheaper as more of them are produced and bought by the cellular providers.

that 3G would be "a patched up system that could be inefficient", and it would be best if the industry would leapfrog over 3G wireless technology, and prepare for 4G (Christian). 4G protocols use spectrum up to 3 times as efficiently as 3G systems, have better ways of handling dynamic load changes (such as additional cellular users entering a particular cell), and create more bandwidth than 3G systems. Most importantly, fourth-generation systems will draw more users by using standard network protocols, which will be discussed later, to connect to the Internet. This will allow simple and transparent connectivity.

2.3 Barriers to Progress

This begs the question: Why are cellular providers not moving to 4G instead of 3G? A marketplace like the cellular industry can be modeled as a game, as seen in Table 2.

There are three basic paths the game can take:

Nobody makes the conversion to 4G All end up upgrading to 2.5G and 3G services. The upgrades are incremental, and don't require a complete reworking of the system, so they are fairly cheap — the equipment required is already developed and in mass production in other places in the world.

Everyone makes the conversion to 4G The equipment and technology needed for 4G will be cheap, because of all of the cellular manufacturers investing in it. Cellular providers will market additional services to its customers.

Some of the players make the conversion to 4G Because not all of the players have chosen 4G, the equipment will be more expensive than the second scenario. Even though converters will be able to sell more services to their customers, it will not be enough to cover the higher costs of converting to 4G.

Therefore, if a player chooses the 4G strategy, but nobody else follows suit, that player will be at a significant disadvantage. No cellular provider has incentive to move to 4G unless all providers move to 4G. An outside agent — the national government — must standardize on 4G as the wireless standard for the United States.

Of course, legitimate concerns can be posed to the idea of implementing 4G nationwide. A common concern is the similarity of this proposal to the forced introduction of HDTV

in the US, which has (thus far) failed miserably. There are two key differences, however, between 4G and HDTV. The first is the nature of the service providers. There are many small television broadcasters in rural areas whose cost of conversion would be as much as 15 years of revenue. The cellular industry, however, does not have this problem. The players are multi-billion dollar companies, who already have enough capital; continual network upgrades are part of their business plan. Our proposal is simply choosing a direction for their growth.

An often overlooked area of financial liability for cellular providers is in the area of information security. Providers could lose money through fraudulent use of the cellular system or unauthorized disclosure of user information over the airwaves. Both of these cases could be caused by an insecure wireless system. This lesson was learned during the use of the first generation of cellular phones in the United States: If a standard is to be set nationwide, it must be secure.

3 Wireless Security

3.1 History

The original cellular phone network in the United States was called the Analog Mobile Phone System (AMPS). It was developed by AT&T and launched in 1983. AMPS operated in the 800 MHz range, from 824-849 MHz and 869-894 MHz. The lower band was used for transmissions from the phone to the base station, and the upper band was for the reverse direction (Leon-Garcia and Widjaja 2000). This allows full duplex conversation, which is desirable for voice communications. The bands were divided into 832 subchannels, and each connection required a pair: one each for sending and receiving data. Each subchannel was 30 KHz wide, which yielded voice quality comparable to wired telephones. The subchannels were set up so that every subchannel pair was exactly 45 MHz apart (Leon-Garcia and Widjaja 2000). Several of the channels were reserved exclusively for connection setup and teardown. The base station in a particular cell kept a record of which voice subchannel pairs were in use.

Though usable, this system included a number of security flaws. Because each phone transmitted (like any radio transmitter) in the clear on its own frequency, the phones in this system "were almost comically vulnerable to security attacks" (Riezenman 2000, 40). The crime of service theft plagued cellular service providers, as individuals with radio scanners could "sniff" the cellular frequencies and obtain the phone identification numbers necessary to "clone" a phone (Riezenman 2000, 39). The abuser could then use this cloned phone to make free telephone calls that would be charged to the legitimate user's account. In an attempt to stem these attacks, service providers worked with Congress to punish such abuse. Congress passed a law in 1998 to make owning a cellular scanner with intent to defraud a federal crime (Riezenman 2000, 40). Unfortunately, punitive legislation was not enough to solve the problem; a new standard was needed. To create a new standard, engineers needed to start anew, examining each part of the current system.

3.2 Stakeholders in Wireless Security

In attempting to avoid security problems like those that plagued the first-generation cellular systems, engineers must design security into any new technology it cannot be added as an afterthought. Unfortunately, this is no easy task. Implementing good security requires that security be designed into every aspect of the system; otherwise, a security leak exists. Thus, the following entities must cooperate to create the secure wireless system:

- Government regulator
- Network infrastructure provider
- Wireless service provider
- Wireless equipment provider
- Wireless user (Russell 2001, 172)

3.3 Information Security Model

Before seeking to design and implement wireless security, however, one first needs to understand what this elusive concept of security really means. In this case, wireless security is really a combination of wireless channel security (security of the radio transmission) and network security (security of the wired network through which the data flows). These collectively can be referred to as "wireless network security" (Russell 2001, 173). But this still does not explain the security aspect. In a digital realm, security almost always means "information security." Therefore, we can use the information security model proposed by the National Security Telecommunications and Information Systems Security Committee (NSTISSC), as seen in Figure 2: Along the top edge of the cube are the three states information can be in, while the rows on the left side of the cube are the information characteristics that the security policy should provide. The columns on the right side of the cube detail the three broad categories of security measures that can be pursued to protect the information. The cube is thus split into 27 smaller cubes, each of which must be examined for risks and solutions in any extensive security audit. This document, on the other hand, is not meant to contain such an audit, but rather to present the major issues of wireless security, the objectives of future wireless technology, and the security measures needed to reach those goals.

3.4 Wireless Security Issues

Wireless systems face a number of security challenges, one of which comes from interference. As more wireless devices begin to use the same section of electromagnetic spectrum, the possibility of interference increases. This can result in a loss of signal for users. Moreover, an abuser can intentionally mount a denial-of-service attack (lowering availability) by jamming the frequencies used. Iowa State University professor Steve Russell comments that "an RF engineer using $50 worth of readily-available components can build a simple short-range jammer for any of the common microwave frequencies" (Russell 2001, 174).

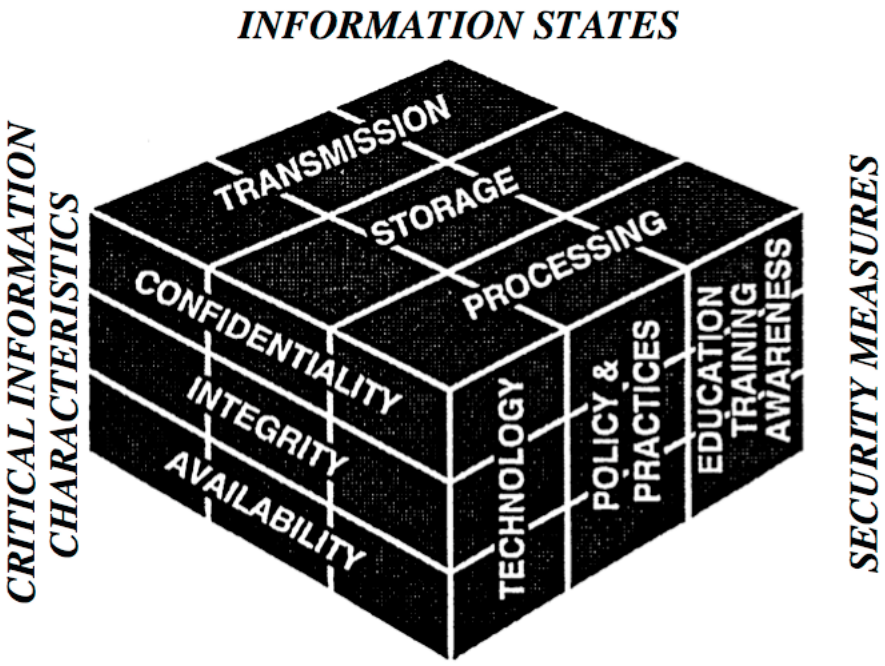

Figure 2: Information Security Model

Physical security can pose problems as well. Cellular phones and other handheld devices were designed to be small and mobile, but this also means that they are more likely than other pieces of technology to get lost or stolen, and thieves can easily conceal them. Because of their size, these devices often have extremely limited computing power. This could manifest itself in lower levels in the encryption that protects the information (NIST, U.S. Dept. of Commerce , 5-26). As encryption is improved in the same device, speed is consequently lowered, as is available bandwidth (Russell 2001, 174).

Other software issues can open security holes as well. For example, many handheld wireless devices include the ability to download and run programs, some of which may not be trustworthy. Even the core operating system software may not be secure; engineers may have rushed to release it in order to offer new features in the competitive handheld device market. Perhaps most damaging, the users typically lack awareness that any of these security issues may be present in their wireless handheld device (NIST, U.S. Dept. of Commerce , 5-27).

These security issues serve as a reminder that designing for security is never a finished process. Every new technology must be analyzed for security issues before it is fully implemented. Even then, one must keep a careful eye on any new issues that may develop.

3.5 Security Analysis

3.5.1 Objectives

The first step in analyzing cellular wireless security is to identify the security objectives. These are the goals that the security policy and corresponding technology should achieve. Howard, Walker, and Wright, of the British company Vodafone, created objectives for 3G wireless that are applicable to 4G as well:

- To ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation.
- To ensure that the resources and services provided to users are adequately protected against misuse or misappropriation.
- To ensure that the security features are compatible with world-wide availability...
- To ensure that the security features are adequately standardized to ensure world-wide interoperability and roaming between different providers.
- To ensure that the level of protection afforded to users and providers of services is considered to be better than that provided in contemporary fixed and mobile networks...
- To ensure that the implementation of security features and mechanisms can be extended and enhanced as required by new threats and services.
- To ensure that security features enable new 'e-commerce' services and other advanced applications(Howard, Walker, and Wright 2001, 22)

These goals will help to direct security efforts, especially when the system is faced with specific threats.

3.5.2 Threats

Because instances of 4G wireless systems currently only exist in a few laboratories, it is difficult to know exactly what security threats may be present in the future. However, one can still extrapolate based on past experience in wired network technology and wireless transmission. For instance, as mobile handheld devices become more complex, new layers of technological abstraction will be added. Thus, while lower layers may be fairly secure, software at a higher layer may introduce vulnerabilities, or vice-versa. Future cellular wireless devices will be known for their software applications, which will provide innovative new features to the user. Unfortunately, these applications will likely introduce new security holes, leading to more attacks on the application level (Howard, Walker, and Wright 2001, 22). Just as attacks over the Internet may currently take advantage of flaws in applications like Internet Explorer, so too may attacks in the future take advantage of popular applications on cellular phones. In addition, the aforementioned radio jammers may be adapted to use IP technology to masquerade as legitimate network devices. However, this would be an extremely complex endeavor. The greatest risk comes from the application layer, either from faulty applications themselves or viruses downloaded from the network.

3.5.3 Security Architecture

The above topics merely comprise a brief overview of some of the issues involved in wireless handheld device security. They by no means define a complete security solution for 4G wireless security. Rather, these topics serve as examples of some of the more prominent security problems that currently exist or may exist in future wireless systems. A more thorough security analysis is needed before a 4G wireless system can be implemented. This should lead to a 4G security architecture that is:

Complete The architecture should address all threats to the security objectives. Unfortunately, it may be difficult to avoid missing some features when there are so many independent parts of the 4G system.

Efficient Security functionality duplication should be kept to a minimum. Again, this may be difficult given the number of independent functions.

Effective Security features should achieve their purpose. However, some security features may open up new security holes.

Extensible Security should be upgradeable in a systematic way.

User-friendly End users should have to learn as little about security as possible. Security should be transparent to the user; when interaction must be involved, it should be easy to understand (Howard, Walker, and Wright 2001, 26).

These objectives were taken into account when the current generation of cellular technology was designed. This generation, referred to as 2G, has worked well; though it is showing its age, it is still in use.

4 Current Technology

Most modern cellular phones are based on one of two transmission technologies: time-division multiple access (TDMA) or code-division multiple access (CDMA) (Riezenman 2000, 40). These two technologies are collectively referred to as second-generation, or 2G. Both systems make eavesdropping more difficult by digitally encoding the voice data and compressing it, then splitting up the resulting data into chunks upon transmission.

4.1 TDMA

TDMA, or Time Division Multiple Access, is a technique for dividing the time domain up into subchannels for use by multiple devices. Each device gets a single time slot in a procession of devices on the network, as seen in Figure 3. During that particular time slot, one device is allowed to utilize the entire bandwidth of the spectrum, and every other device is in the quiescent state.

The time is divided into frames in which each device on the network gets one timeslot. There are n timeslots in each frame, one each for n devices on the network. In practice, every device gets a timeslot in every frame. This makes the frame setup simpler and more

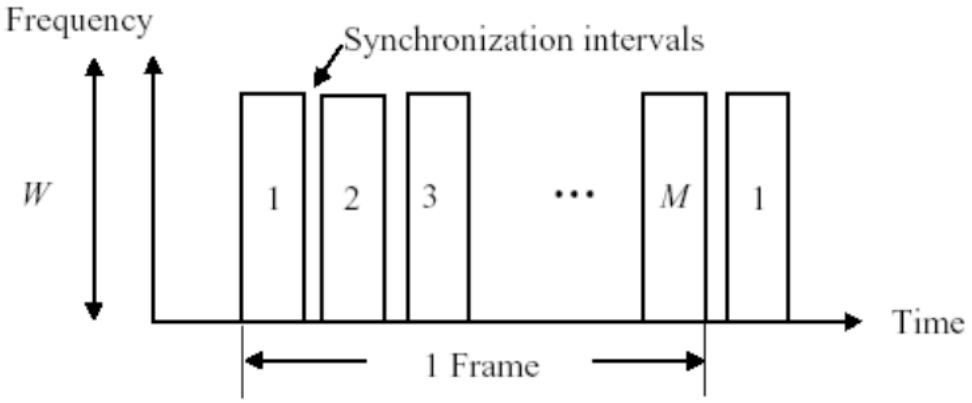

Figure 3: Time Division Multiple Access

efficient because there is no time wasted on setting up the order of transmission. This has the negative side effect of wasting bandwidth and capacity on devices that have nothing to send (Leon-Garcia and Widjaja 2000).

One optimization that makes TDMA much more efficient is the addition of a registration period at the beginning of the frame. During this period, each device indicates how much data it has to send. Through this registration period, devices with nothing to send waste no time by having a timeslot allocated to them, and devices with lots of pending data can have extra time with which to send it. This is called ETDMA (Extended TDMA) and can increase the efficiency of TDMA to ten times the capacity of the original analog cellular phone network.

The benefit of using TDMA with this optimization for network access comes when data is "bursty." That means, at an arbitrary time, it is not possible to predict the rate or amount of pending data from a particular host. This type of data is seen often in voice transmission, where the rate of speech, the volume of speech, and the amount of background noise are constantly varying. Thus, for this type of data, very little capacity is wasted by excessive allocation.

4.2 CDMA

CDMA, or Code Division Multiple Access, allows every device in a cell to transmit over the entire bandwidth at all times. Each mobile device has a unique and orthogonal code that is used to encode and recover the signal (Leon-Garcia and Widjaja 2000). The mobile phone digitizes the voice data as it is received, and encodes the data with the unique code for that phone. This is accomplished by taking each bit of the signal and multiplying it by all bits in the unique code for the phone. Thus, one data bit is transformed into a sequence of bits of the same length as the code for the mobile phone. This makes it possible to combine with other signals on the same frequency range and still recover the original signal from an arbitrary mobile phone as long as the code for that phone is known. Once encoded, the data is modulated for transmission over the bandwidth allocated for that transmission. A block diagram of the process is shown in Figure 4.

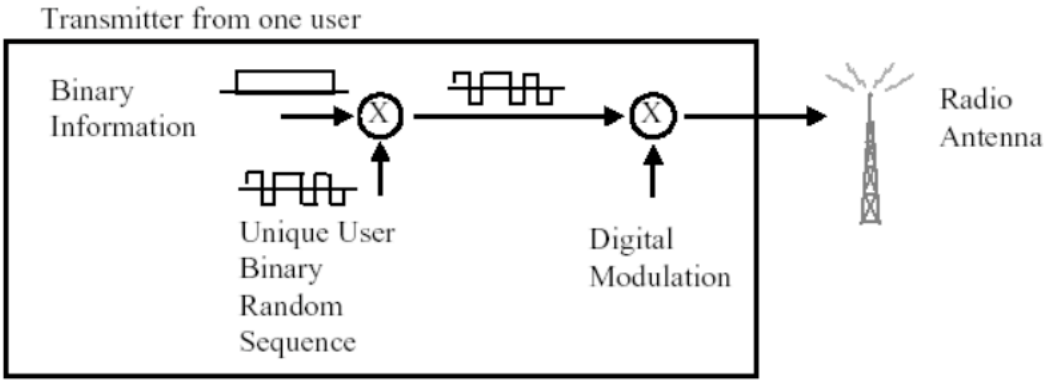

Figure 4: Sending Data using Code Division Multiple Access

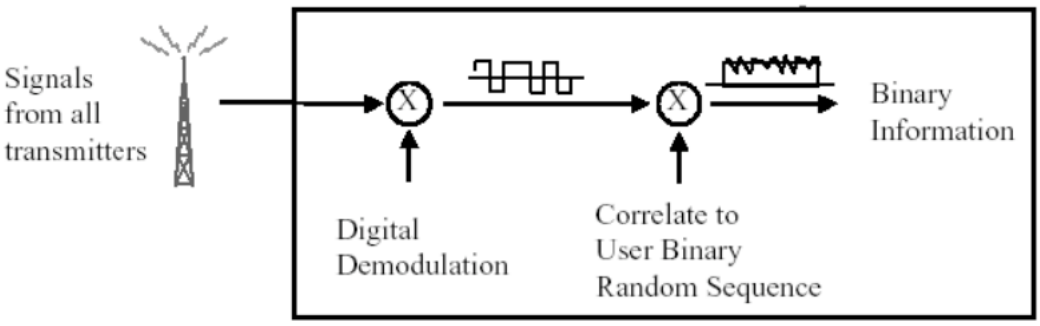

Figure 5: Receiving Data using Code Division Multiple Access

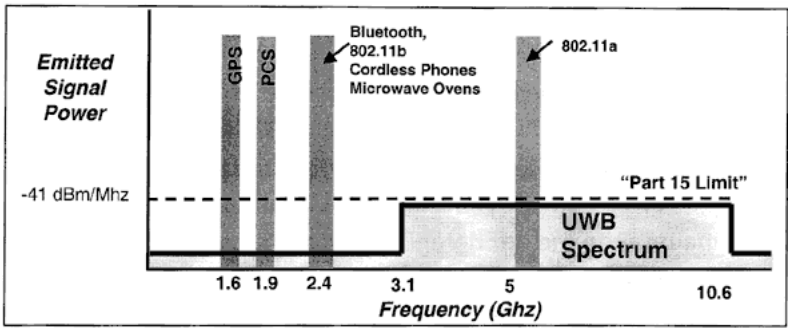

Figure 6: UWB Spectrum Usage

The process for receiving a signal is shown in Figure 5. Once the signal is demodulated, a correlator and integrator pair recovers the signal based on the unique code from the cellular phone. The correlator recovers the original encoded signal for the device, and the integrator transforms the recovered signal into the actual data stream.

CDMA has been patented in the United States by Qualcomm, making it more expensive to implement due to royalty fees. This has been a factor for cellular phone providers when choosing which system to implement.

By keeping security in mind while designing the new system, the creators of 2G wireless were able to produce a usable system that is still in use today. Unfortunately, 2G technology is beginning to feel its age. Consumers now demand more features, which in turn require higher data rates than 2G can handle. A new system is needed that merges voice and data into the same digital stream, conserving bandwidth to enable fast data access. By using advanced hardware and software at both ends of the transmission, 4G is the answer to this problem.

5 4G Hardware

5.1 Ultra Wide Band Networks

Ultra Wideband technology, or UWB, is an advanced transmission technology that can be used in the implementation of a 4G network. The secret to UWB is that it is typically detected as noise. This highly specific kind of noise does not cause interference with current radio frequency devices, but can be decoded by another device that recognizes UWB and can reassemble it back into a signal. Since the signal is disguised as noise, it can use any part of the frequency spectrum, which means that it can use frequencies that are currently in use by other radio frequency devices (Cravotta).

An Ultra Wideband device works by emitting a series of short, low powered electrical pulses that are not directed at one particular frequency but rather are spread across the entire spectrum (Butcher). As seen in Figure 6, Ultra Wideband uses a frequency of between 3.1 to 10.6 GHz.

The pulse can be called "shaped noise" because it is not flat, but curves across the spectrum. On the other hand, actual noise would look the same across a range of frequencies — it has no shape. For this reason, regular noise that may have the same frequency as the

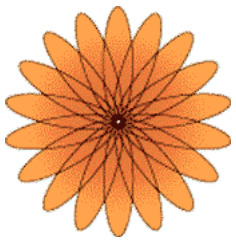

Figure 7: Switched Beam Antenna

pulse itself does not cancel out the pulse. Interference would have to spread across the spectrum uniformly to obscure the pulse.

UWB provides greater bandwidth — as much as 60 megabits per second, which is 6 times faster than today's wireless networks. It also uses significantly less power, since it transmits pulses instead of a continuous signal. UWB uses all frequencies from high to low, thereby passing through objects like the sea or layers of rock. Nevertheless, because of the weakness of the UWB signal, special antennas are needed to tune and aim the signal.

5.2 Smart Antennas

Multiple "smart antennas" can be employed to help find, tune, and turn up signal information. Since the antennas can both "listen" and "talk," a smart antenna can send signals back in the same direction that they came from. This means that the antenna system cannot only hear many times louder, but can also respond more loudly and directly as well (ArrayComm 2003).

There are two types of smart antennas:

Switched Beam Antennas (as seen in Figure 7) have fixed beams of transmission, and can switch from one predefined beam to another when the user with the phone moves throughout the sector

Adaptive Array Antennas (as seen in Figure 8) represent the most advanced smart antenna approach to date using a variety of new signal processing algorithms to locate and track the user, minimize interference, and maximize intended signal reception (ArrayComm 2003).

Smart antennas can thereby:

- Optimize available power
- Increase base station range and coverage
- Reuse available spectrum
- Increase bandwidth
- Lengthen battery life of wireless devices

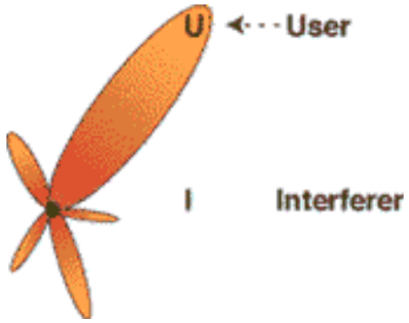

Figure 8: Adaptive Array Antenna

Although UWB and smart antenna technology may play a large role in a 4G system, advanced software will be needed to process data on both the sending and receiving side. This software should be flexible, as the future wireless world will likely be a heterogeneous mix of technologies.

6 4G Software

4G will likely become a unification of different wireless networks, including wireless LAN technologies (e.g. IEEE 802.11), public cellular networks (2.5G, 3G), and even personal area networks. Under this umbrella, 4G needs to support a wide range of mobile devices that can roam across different types of networks (Cefriel). These devices would have to support different networks, meaning that one device would have to have the capability of working on different networks. One solution to this "multi-network functional device" is a software defined radio.

6.1 Software Defined Radio

A software defined radio is one that can be configured to any radio or frequency standard through the use of software. For example, if one was a subscriber of Sprint and moved into an area where Sprint did not have service, but Cingular did, the phone would automatically switch from operating on a CDMA frequency to a TDMA frequency. In addition, if a new standard were to be created, the phone would be able to support that new standard with a simple software update. With current phones, this is impossible. A software defined radio in the context of 4G would be able to work on different broadband networks and would be able to transfer to another network seamlessly while traveling outside of the user's home network.

A software defined radio's best advantage is its great flexibility to be programmed for emerging wireless standards. It can be dynamically updated with new software without any changes in hardware and infrastructure. Roaming can be an issue with different standards, but with a software defined radio, users can just download the interface upon entering new territory, or the software could just download automatically (Wang 2001).

Of course, in order to be able to download software at any location, the data must be formatted to some standard. This is the job of the packet layer, which will split the data into small "packets."

6.2 Packet Layer

The packet layer is a layer of abstraction that separates the data being transmitted from the way that it is being transmitted. The Internet relies on packets to move files, pictures, video, and other information over the same hardware. Without a packet layer, there would need to be a separate connection on each computer for each type of information and a separate network with separate routing equipment to move that information around. Packets follow rules for how they are formatted; as long they follow these rules, they can be any size and contain any kind of information, carrying this information from any device on the network to another.

Currently, there is little fault tolerance built into cellular systems. If a little bit of the voice information is garbled or lost in a transfer between locations, or if interference from other devices somehow affects the transmission, there is nothing that can be done about it. Even though the loss is usually negligible, it still can cause major problems with sensitive devices and can garble voice information to a point where it is unintelligible. All of these problems contribute to a low Quality of Service (QoS).

6.3 Packets

6.3.1 Advantages

There are many advantages of packets and very few disadvantages. Packets are a proven method to transfer information. Packets are:

More Secure Packets are inherently more secure for a variety of reasons:

- A predictable algorithm does not split packets — they can be of any size and contain any amount of data. Packets can also travel across the network right after each other or separated by packets from other devices; they can all take the same route over networks or each take a different route.
- The data in packets can be encrypted using conventional data encryption methods. There are many ways to encrypt data, including ROT-13, PGP, and RSA; the information in a packet can be encoded using any one of them, because a packet doesn't care what kind of data it carries. Within the same packet, no matter how the data segment is encrypted, the packet will still get from one place to the other in the same way, only requiring that the receiving device know how to decrypt the data.
- There is no simple way to reconstruct data from packets without being the intended recipient. Given that packets can take any route to their destination, it is usually hard to piece them together without actually being at their intended destination. There are tools to scan packets from networks; however, with the volume of packets that networks receive and the volume of packets per each communication, it would take a large amount of storage and processing power to effectively "sniff" a packet communication, especially if the packets were encrypted.

More Flexible Current technologies require a direct path from one end of a communication to the other. This limits flexibility of the current network; it is more like a large number

of direct communication paths than a network. When something happens to the path in the current system, information is lost, or the connection is terminated (e.g. a dropped call). Packets only require that there is an origin, a destination, and at least one route between them. If something happens to one of the routes that a packet is using, the routing equipment uses information in the packet to find out where it is supposed to go and gives it an alternate route accordingly. Whether the problem with the network is an outage or a slowdown, the combination of the data in the packet and the routing equipment lead to the packet getting where it needs to go as quickly as possible.

More Reliable Packets know general things about the information they contain and can be checked for errors at their destination. Error correction data is encoded in the last part of the packet, so if the transmission garbles even one bit of the information, the receiving device will know and ask for the data to be retransmitted. Packets are also numbered so that if one goes missing, the device on the receiving end will know that something has gone wrong and can request that the packet(s) in question be sent again. In addition, when something does go wrong, the rest of the packets will find a way around the problem, requiring that only the few lost during the actual instant of the problem will need to be resent.

Proven Technology Packets are the underlying technology in essentially all data based communication. Since the beginning of the Internet over 30 years ago, packets have been used for all data transmission. Technologies have evolved to ensure an almost 100% QoS for packet transmission across a network.

Easier to Standardize Current technologies use a variety of methods to break up voice communication into pieces. None of these are compatible with each other. Packets, however, are extremely compatible with various devices. They can carry different types of information and be different sizes, but still have the same basic makeup to travel over any network using any of the methods of transmission. Essentially, this enables different technologies to be used to handle the same fundamental information (Howstuffworks.com). An example of the format of a packet carrying 896 bits of actual information can be seen in Figure 9: The "Protocol" section would contain whatever information was needed to explain what type of data was encoded; in the case of voice using Voice over IP (VoIP), it would read: H.323 (Protocols.com).

Extensible As shown by the growth of the Internet over the past few years, the capacity of packets is expandable. They have moved from carrying short text messages to carrying video, audio, and other huge types of data. As long as the capacity of the transmitter is large enough, a packet can carry any size of information, or a large number of packets can be sent carrying information cut up into little pieces. As long as a packet obeys the standard for how to start and end, any data of any size can be encoded inside of it; the transmission hardware will not know the difference.

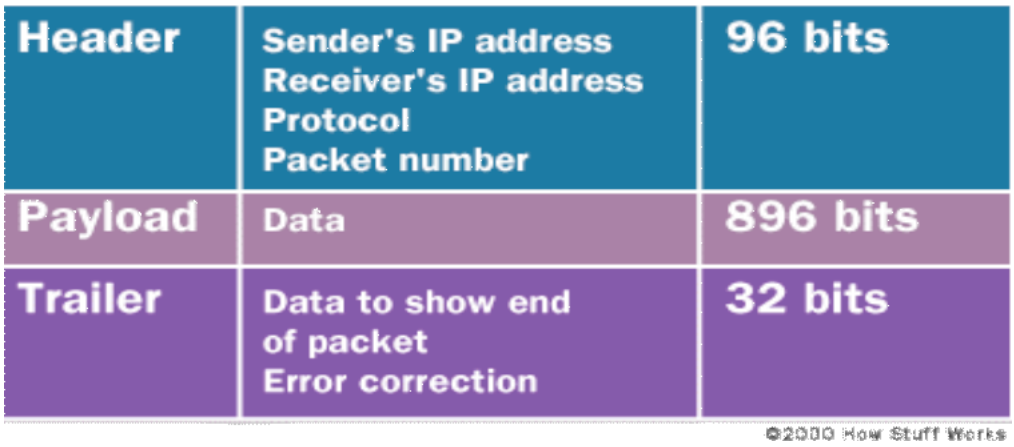

Figure 9: Packet with 896-bit payload

6.3.2 Disadvantages

Unfortunately, to use packet, all cellular hardware will need to be upgraded or replaced. Consumers will be required to purchase new phones, and providers will need to install new equipment in towers. Essentially, the communication system will need to be rebuilt from the ground up, running off of data packets instead of voice information. However, given the current pace of technological development, most consumers buy new phones every six to twelve months, and providers are constantly rolling out new equipment to either meet expanding demand or to provide new or high-end services. All networks will be compatible once the switch is completed, eliminating roaming and areas where only one type of phone is supported. Because of this natural pace of hardware replacement, a mandated upgrade in a reasonable timeframe should not incur undue additional costs on cellular companies or consumers.

The technological disadvantage of using packets is not really a disadvantage, but more of an obstacle to overcome. As the voice and data networks are merged, there will suddenly be millions of new devices on the data network. This will require either rethinking the address space for the entire Internet or using separate address spaces for the wireless and existing networks.

6.4 Implementation of Packets

6.4.1 Current System: IPv4

Currently, the Internet uses the Internet Protocol version 4 (IPv4) to locate devices. IPv4 uses an address in the format of xxx.xxx.xxx.xxx where each set of three digits can range from 0 to 255 (e.g 130.207.44.251). Though combinations are reserved, but this address format allows for approximately 4.2 billion unique addresses. Almost all IP addresses using IPv4 have been assigned, and given the number of new devices being connected to the Internet every day, space is running out. As people begin to connect refrigerators, cars, and phones to the Internet, a larger address space will be needed.

6.4.2 Recommended System: IPv6

The next generation addressing system uses the Internet Protocol version 6 (IPv6) to locate devices. IPv6 has a much larger address space. Its addresses take the form x:x:x:x:x:x:x:x where each x is the hexadecimal value that makes up one eighth of the address. An example of this is: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 (The Internet Engineering Task Force Network Working Group). Using this address format, there is room for approximately $3.40 * 10^{38}$ unique addresses. This is approximately $8.05 * 10^{28}$ times as large as the IPv4 address space and should have room for all wired and wireless devices, as well as room for all of the foreseeable expansion in several lifetimes. There are enough addresses for every phone to have a unique address. Thus, phone in the future can use VoIP over the Internet instead of continuing to use their existing network.

6.4.3 Voice over IP (VoIP)

Voice over IP is the current standard for voice communication over data networks. Several standards already exist for VoIP, the primary one being International Multimedia Telecommunications Consortium standard H.323. VoIP is already in use in many offices to replace PBX-based systems and by several companies that offer cheap long distance phone calls over the Internet, such as Net2Phone and Go2Call. VoIP allows for flexibility the same way that data packets do; as far as the network is concerned, VoIP packets are the same as any other packet. They can travel over any equipment that supports packet-based communication and they receive all of the error correction and other benefits that packets receive. There are many interconnects between the data Internet and the phone network, so not only can VoIP customers communicate with each other, they can also communicate with users of the old telephone system.

One other thing that VoIP allows is slow transition from direct, connection based communication to VoIP communication. Backbones can be replaced, allowing old-style telephone users to connect to their central office (CO) the same way. However, the CO will then connect to an IPv6 Internet backbone, which will then connect to the destination CO. To the end user, there will not seem to be any difference, but the communication will occur primarily over a packet-based system, yielding all of the benefits of packets, outside of the short connections between either end of the communication and their CO.

Of course, in order to keep curious users from listening in by "sniffing," all data, including voice, should be encrypted while in transit.

6.5 Encryption

Two encryption/decryption techniques are commonly used: asymmetric and symmetric encryption. Symmetric encryption is the more traditional form, where both sides agree on a system of encrypting and decrypting messages — the reverse of the encryption algorithm is the decryption algorithm. Modern symmetric encryption algorithms are generic and use a key to vary the algorithm. Thus, two sides can settle on a specific key to use for their communications. The problem then is the key transportation problem: How do both sides get the key without a third party intercepting it? If an unauthorized user receives the key, then he too can decrypt the messages.

The solution to this problem is asymmetric encryption. In symmetric encryption, the encryption and decryption algorithms are inverses, but the key is the same. In asymmetric encryption, the keys are inverses, but the algorithm is the same. The trick is that one cannot infer the value of one key by using the other. In an asymmetric (also called public-key) system, an end user makes one key public and keeps the other private. Then all parties know the algorithm and the public key. If any party wishes to communicate with the users, that party can encrypt the message using the public key, and only the user (with her private key) can decrypt the message. Moreover, the user can prove that she generated a message by encrypting it with her private key. If the encrypted message makes sense to other parties when decrypted with the public key, then those parties know that the user must have generated that message (Dankers, Garefalakis, Schaffelhofer, and Wright 2002, 181).

Situations exist in cellular wireless systems where either symmetric or asymmetric keys are particularly useful. Asymmetric keys are useful for one-time connections, especially when used to create a symmetric key for an extended connection. Meanwhile, symmetric keys are smaller and faster, and thus are strongly preferred if key transportation is not a problem. An excellent example of this is the GSM system's subscriber information card placed into each phone. The card holds a unique symmetric key for each subscriber.

6.6 Flexibility

In reality, however, the usage of different encryption schemes depends on many factors, including network data flow design. Thus, it is important that the encryption method be able to change when other determining factors change. Al-Muhtadi, Mickunas, and Campbell of University of Illinois at Urbana-Champaign showed great foresight in admitting that "existing security schemes in 2G and 3G systems are inadequate, since there is greater demand to provide a more flexible, reconfigurable, and scalable security mechanism as fast as mobile hosts are evolving into full-fledged IP-enabled devices" (Al-Muhtadi, Mickunas, and Campbell 2002, 60).

Unfortunately, IPv6 can only protect data in transmission. Individual applications may contain flaws in the processing of data, thereby opening security holes. These holes may be remotely exploited, allowing the security of the entire mobile device to be compromised. Thus, any wireless device should provide a process for updating the application software as security holes are discovered and fixed.

6.7 Anti-Virus

As wireless devices become more powerful, they will begin to exhibit the same security weaknesses as any other computer. For example, wireless devices may fall victim to trojans or become corrupt with viruses. Therefore, any new wireless handheld device should incorporate antivirus software. This software should scan all e-mail and files entering through any port (e.g. Internet, beaming, or synchronizing), prompting the user to remove suspicious software in the process. The antivirus software should also allow secure, remote updates of the scanning software in order to keep up with the latest viruses (NIST, U.S. Dept. of Commerce , 5-34).

7 Conclusion

Consumers demand that software and hardware be user-friendly and perform well. Indeed, it seems part of our culture that customers expect the highest quality and the greatest features from what they buy. The cellular telephone industry, which now includes a myriad of wireless devices, is no exception.

Meanwhile, competition in the industry is heating up. Providers are slashing prices while scrambling for the needed infrastructure to provide the latest features as incentives, often turning to various 3G solutions. Unfortunately, this will only serve to bewilder customers in an already confusing market.

Customers want the features delivered to them, simple and straightforward. Wireless providers want to make money in a cutthroat industry. If the U.S. government wants to help, the best way to help all parties is to enforce 4G as the next wireless standard. The software that consumers desire is already in wide use. The transmission hardware to take it wireless is ready to go. And we have the security practices to make sure it all works safely. The government need only push in the right direction; the FCC need only standardize 4G in order to make the transition economically viable for all involved.

This is a need that demands a solution. Today's wired society is going wireless, and it has a problem. 4G is the answer.

Works Cited

Al-Muhtadi, J., D. Mickunas, and R. Campbell. "A lightweight reconfigurable security mechanism for 3G/4G mobile devices." *IEEE Wireless Communications* 9.2 (2002): 60–65.

ArrayComm. "IEC: Smart Antenna Systems." *International Engineering Consortium* (2003). 6 April 2003. <http://www.iec.org/online/tutorials/smart_ant/topic01.html>.

Butcher, Mike. "UWB: widening the possibilities for wireless." *New Media Age*. 5 April 2003. <http://www.uwb.org/news/articles/04_2002/NewMediaAgeAprilil402.pdf>.

Cefriel. "4th Generation Networks (4G)." *Cefriel*. 6 April 2003. <http://www.cefriel.it/topics/interest/default.xml?id=106&tid=13>.

Christian, Bruce. "Intellectual Capital: William C.Y. Lee Looks Ahead to 4G Wireless." *Phone+*. 3 April 2003. <http://www.phoneplusmag.com/articles/131feat3.html>.

Cravotta, Nicholas. "Ultrawideband: the next wireless panacea?." *EDN.com*. 5 April 2003. <http://www.uwb.org/files/October2002/EDNOct1702.pdf>.

Dankers, J., T. Garefalakis, R. Schaffelhofer, and T. Wright. "Public key infrastructure in mobile systems." *Electronics & Communication Engineering Journal* 14.5 (2002): 180–190.

Howard, P., M. Walker, and T. Wright. "Towards a coherent approach to third generation system security." *3G Mobile Communication Technologies* (2001): 21–27.

Leon-Garcia, Alberto and Indra Widjaja. *Communication Networks: Fundamental Concepts and Key Architectures*. Boston: McGraw Hill, 2000.

NIST. "Wireless Network Security.". <http://cs-www.ncsl.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf>.

Protocols Directory Voice over IP. "Protocols Directory Voice over IP." *Protocols.com*. 21 March 2003. <http://www.protocols.com/pbook/VoIP.htm>.

RFC1884. "RFC# 1884: IP Version 6 Addressing Architecture." *The Internet Engineering Task Force Network Working Group*. <http://www.ietf.org/rfc/rfc1884.txt>.

Riezenman, M.J. "Cellular security: better, but foes still lurk.." *IEEE Spectrum* 37.6 (2000): 39–42.

Russell, S.F. "Wireless network security for users." *Information Technology: Coding and Computing* (2001): 172–177.

Wang, Jiangzhou. *Broadband Wireless Communications: 3G, 4G and Wireless LAN*. Boston: Kluwer Academic Publishers, 2001.

What is a Packet? "What is a Packet?." *Howstuffworks.com*. 21 March 2003. <http://computer.howstuffworks.com/question525.htm/printable>.