CELLULAR TECHNOLOGY AND SECURITY

Author: RYAN JONES

As we head into the 21st century, wireless communications are becoming a household name. We are going to explore the advent of analog cellular, security flaws and fixes, as well as the dawning of a new age with the proliferation of digital cellular technology.

ADVENT OF CELLULAR TECHNOLOGY

What was the purpose of the first cellular phones? They allowed business people access to a phone while in their automobile. The first cell phones had to be installed in cars at a price of $3000 or more. Only sales people, and business travelers could justify the price for the service. Through time, the cost of cell phone technology began to decrease, and the market began to expand.

Cell phones were still only available in cars, until the early 1990's when more advanced technology arrived, whereby spectrum capacity was expanded. In the past, the only way to allow more users into a fixed amount of spectrum, was to decrease the amount of bandwidth allocated to each user. The only problem with giving each user a smaller slice of the pie, was that the channels carried less information, and their was an increased chance for multipath fading. Increased demand for mobile telephone caused a battle between users for the band of frequencies allocated to mobile communications by the FCC. When the wireless sector realized that they would not be able to meet the demand, the industry came up with the "cellular" concept.

CELLULAR CONCEPT

The cellular concept allows different frequencies to be utilized more than once. Instead of using one channel to carry a user's information from one mobile destination to another mobile or stationary point, cellular radio uses a multitude of channels to pass along a user's information. Each geographic service area is divided into hexagonal cells.(figure #1) Most cellular providers have seven different channels that they have divided the mobile frequency spectrum into, and each cell is designated one channel. As you can see from figure #1, the hexagonal pattern does not allow similar channels to border one another.

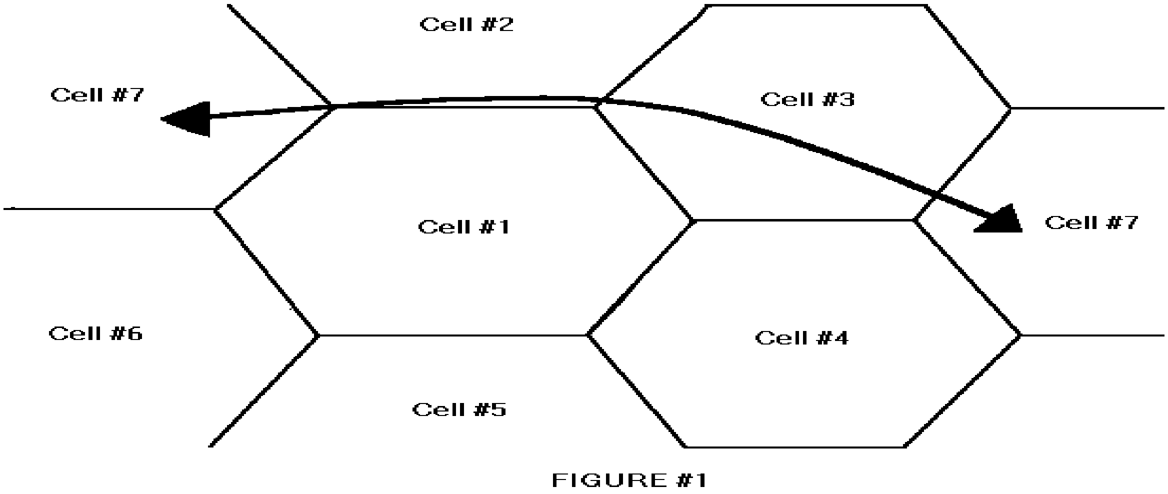


FIGURE #1

For the cellular concept to work, whereby signals from one cell did not carry over several cells, two limitations had to be met. Firstly, the base station and the mobile transmitters had to be low power. The base stations power had to be less than 100 Watts, and the mobile transmitters were required to be less than 10 Watts. The other prerequisite, was that the frequency band used had to be well suited for communications over short distances. The 800 Mhz and 900 Mhz bands offered such a characteristic.

Experts contended that this technology would allow for limitless expansion. If there were too many users in one cell using one channel, the cellular carrier would be able to decrease the size of their cells. A reduction in cell size of 50%, increased the load by 4. However, there are a few problems associated with this idea. The largest problem for cellular providers is cost. With a reduced cell layout, the carrier would have to add more hardware at a cost of $300 to $500 thousand per cell site. As well, carriers would have to buy up more real estate, and install more land lines dedicated to carrying the phone signals back to their switching stations. Hand-off also becomes more difficult as the network becomes more concentrated.

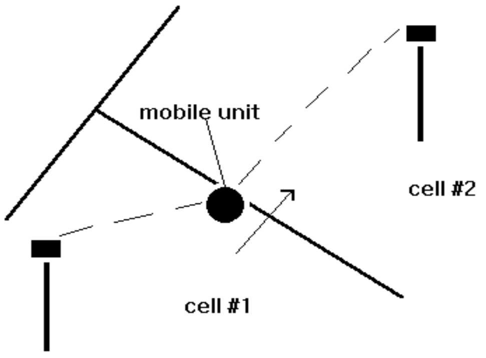
ANALOG CELLULAR

The most widely used cellular today, still uses an analog platform (although this is changing rapidly). Analog simply means that the signals transmitted form the mobile to the base station and vice versa are electromagnetic waves which carry directly measurable information. Meaning that the information is not encoded for transportation, and does not need to be decoded at the receiver.

AMPS (Advanced Mobile Phoned Service) is the standard for analog cellular systems. It uses FDMA (Frequency Division Multiple Access) to divide up the radio spectrum into 30 Khz slices. Some systems use N-AMPS (Narrowband-AMPS) where the spectrum is divided up into 10 Khz slices. Each slice represents one channel within a cell. Only one user may use this channel at one time. No other user may access the channel until the original call is terminated or handed off.

ANALOG HAND-OFF

Hand-off (figure #2) occurs when a mobile transmitter leaves one cell and enters another. Analog cellular systems take approximately 200 milliseconds to do a hand-off, which is heard as a delay by users. Hand-offs increase with a decrease in cell size, and analog cellular has more dropped calls and noise due to hand-off, compared to TDMA and CDMA technology used in digital cellular (explored on pg. 7)



Handoff
Figure #2

The number of hand-offs which occur, depend upon the speed of the mobile unit, and the area which the mobile transmitter is being utilized in. For example, a car moving at 65 m.p.h. on a rural freeway will have a hand-off every 9 minutes, whereas a car moving at 65 m.p.h. on an urban freeway will have a hand-off every minute (figure #3). These hand-offs are then multiplied by the number of moving mobile users in a cell at any given time.

Case	Speed (mph)	Speed (kmh)	Cell Radius (km)	Hand-offs
Freeway, rural	65	104	16	0.33
Freeway, urban	65	104	1.6	3.25
Streets, urban	30	48	1	2.4
Pedestrian, urban	1.5	2.4	1	0.12
Pedestrian, microcell	1.5	2.4	0.1	1.2

*Number of cells transited is approximated by 0.65*velocity*T/R
T=duration of call (3 mins. was used above) R=radius of cell

Figure #3
Hand-off Frequency

Hand-off entails:

1. In the beginning, one cell services the mobile unit.
2. Base stations monitor the quality of the air-link and determines when the cell in use is deteriorating, and if the mobile unit would better be served by a new cell.
3. The old base station passes information to the new base station, to allow the new cell to identify the mobile, and to begin hand-off.
4. The mobile is informed of the hand-off.
5. The new cell begins to service the mobile, and the mobile recognizes the new cell.
6. The old cell is allowed to discontinue service to the mobile.

There are multiple problems associated with hand-off using AMPS analog technology:

1. The hand-offs between cells are “hard.” This means that communication is interrupted during cell transfer.
2. The mobile unit can communicate with only one station at a time, therefore there is never a simultaneous link between the mobile and the two cells involved in the hand-off. This results in dropped calls, and in the “hard” transfer.
3. The base stations do the quality air-link testing, and not the mobile, resulting in a less accurate measurement. The base stations cannot distinguish between the desired

signal and an interference signal, and therefore, the stations measurement of transmission power can be deceiving.

ROAMING

When users travel outside of their service provider's area, they are considered a roaming mobile. When licenses were sold to carriers, it was done on a city by city basis, and therefore, roaming happens frequently, once a user leaves his/her vicinity. This represents a problem for cellular providers, as they want to provide a seamless network for their users. Roaming creates more opportunities for access fraud, and makes it a challenge for a carrier to redirect incoming calls to the roaming mobile unit through a series of successful hand-offs between the mobile's home company cells and the host carrier's cells.

SECURITY ISSUES

With the advent of cellular phones, came a new generation of thieves. It is estimated that everyday in the United States, $2 million is lost to cellular fraud. Due to the exponential growth of cellular phone use (17000 new subscribers each day in the U.S.), carriers and the law are having a hard time catching and prosecuting criminals. Only one hacker is caught each day, and cellular users and carriers are responsible for the bill. There are three basic types of security breaches:

1. Access Fraud
2. Subscription Fraud
3. Stolen Phones

ACCESS FRAUD

There are two types of access fraud. Cloning and tumbling are the most prevalent forms of cellular fraud. Cloning occurs when a "bandit" reprograms a cellular phone with another user's ESN (electronic serial number) or MIN (mobile identification number) and then proceeds to use the cloned phone. All the while, the true owner of the ESN is billed for the use of the clone phone. Most of the reprogrammed clone phones are then sold at bargain rates to international call users.

Tumbling phones are cell phones where the "bandit" continuously changes the ESN or MIN after every call while roaming. With the phone on the move in between cells, and out of the home carrier's territory, the constant tumbling of the ESN or MIN perplexes cellular computers just long enough to allow the bandit to place illegal calls.

How do "bandits" get a hold of ESN's or MIN's? It is a very simple process when the user employs an analog cellular phone. All it takes is for the thief to own a radio frequency scanner or a UHF receiver, and for them to tune into the proper frequency as to allow them to pick up a cellular radio channel. While cell phones are "on", or when they send a call, the mobile unit sends it's ESN or MIN over the airwaves to the base station for identification purposes. As an example of how easy it is for a thief to gain access to someone's ESN or MIN, imagine that you are speeding along an urban highway, and your cell phone is on, but not in use. It is however, transmitting your ESN every couple of seconds to the closest base station. As you pass under an overpass, someone sitting in the shadows just read your ESN using a simple radio scanner. That number is then used to clone your phone, and you receive a bill at the end of the month with calls which you never placed. El Salvador? Dominican Republic? China? You never called these destinations but a cloned phone did, using your ESN. In addition, your ESN may also be obtained off of your phone battery, or off of your cellular phone contract.

Once a thief has your ESN, they remove the original chip from the phone which they are cloning, and replace it with a chip programmed with your ESN. Cell phones are supposed to be manufactured so that an attempt to reprogram them would result in irreparable damage, but savvy thieves and poorly fastened chips have allowed cloning to go on with unimaginable success.

SUBSCRIPTION FRAUD

Subscription fraud occurs when people use fake identifications to purchase cellular accounts, and they do not pay their bill. Since the first bill usually arrives after one month of service, and de-activation comes after several defaults, illegal users have time to accumulate extensive cellular phone bills.

PHONE THEFT

Phone theft is similar to a stolen credit card. Thieves use the phone until the cellular carrier is alerted of the theft. Once the carrier is alerted, they proceed to de-activate the account of the stolen cell phone. The largest problem involved here, is that most people report the phones stolen after they have been missing for a couple of days. By that time, thieves can charge hundreds of dollars in calls, that the cellular carrier and all users must pay for.

TIPS FOR USERS

There are a number of things that users may do to combat clone/tumbling fraud and overall privacy:

1. Use the lock function on the cell phone when not in use. This prevents anyone from using the phone without the proper code to unlock the phone.
2. Report frequently dropped or interrupted calls to the cellular carrier.
3. Remove the ESN from the battery in the phone. Not all phones will have an ESN on the battery, but some older models do.
4. Check your monthly bill thoroughly. Most thieves are smart enough to keep calls discreet enough so that billed users do not notice extra calls.
5. Ask your carrier to eliminate access to international destinations which you have no intention on calling.
6. Never discuss financial or secret matters over a cellular network. NEVER dispense a credit card number over the air-waves.

SECURITY DEVICES OFFERED BY CELLULAR CARRIERS

The following security packages are the ones most widely used by cellular providers, such as: AT&T, GTE, Sprint, etc.. Each product description is the actual one provided for consumers by the supplier.

"*FraudBuster*™ performs real-time subscriber call analysis utilizing artificial intelligence to detect and prevent wireless fraud. Coral's fraud detection/prevention solution offers comprehensive (post-call) processes to detect fraud, alert the network operator, and update cellular switches or home location registers. Users can configure a range of responses to FraudBuster's alerts. At the individual subscriber level, FraudBuster offers detection and prevention of the three most common types of wireless fraud: subscriber fraud, clone phones, and tumbler phones. The FraudBuster software solution has unique functionality and antifraud algorithms that may be updated to combat new and future types of fraud.

FraudBuster's features include:

1. A subscriber usage-pattern database
2. Customer call analysis
3. Velocity checking
4. Geographic dispersion checking
5. Extensive proprietary antifraud algorithms
6. Artificial intelligence"

"*CloneGuard*™ is a fraud analysis and control product that uses real-time billing data to detect aberrant calling. It alerts wireless operators of fraud on their networks as it happens and provides a support system to help them deal with occurrences of fraud. CloneGuard uses real-time billing record collection, along with sophisticated algorithmic analysis, to rapidly identify fraudulent situations involving unusual usage patterns or usage inconsistencies."

"*CreditGuard*™ is a system designed to continuously monitor wireless customers and automatically alert the carrier when a pre-defined credit limit has been exceeded. CreditGuard uses real-time rating capabilities. This system allows carriers to protect against subscription fraud and to offer service to credit-risky customers with a limited financial risk"

"*CloneDetector*™ system, one of the industry's most advanced fraud detection systems. By using powerful artificial intelligence technology, it automatically alerts wireless providers to counterfeit fraud on an individual switch basis and on an intercarrier or intracarrier switch basis. It also provides nationwide protection against roaming fraud."

"*FraudManager(SM)* service, the industry's first pre-call roaming validation service based on advanced Interim Standard 41 (IS-41). It has been installed by nearly 100 carriers in almost 700 markets -- including the top 200 in the U.S."

"*StatChek*™ service, automatically checks the status of a cellular phone prior to activation. It ensures that the cellular phone being activated has not been reported as stolen or used fraudulently in other markets."

"*FraudForce(SM)* services, an integrated line of fraud control services, which fights clone fraud and evolving forms of fraud by giving carriers the flexibility to implement customized solutions that meet their changing business needs. The product line includes FraudInterceptor(SM) service, which lets home carriers block, restrict and reinstate roamers in carrier-selected high fraud markets. It routes restricted roamers to FruadChallenger(SM) service, another product in the FraudForce line"

"*FraudChallenger*, an automated challenge and response system, verifies restricted roamers routed through a Personal Identification Number (PIN) entry or through interaction with carrier’s customer service representatives. Carriers have the option to route roamers to customer service representatives at GTE’s national FraudProtection (SM) Center to personally interact with roamers to verify authenticity”

Another security package which is very popular with cellular carriers is Authentication. It works by transmitting a series of encoded passwords between the mobile phone user and the cellular network every time a call is sent or received. Authentication uses an extremely complex, and undisclosed secret code and number based on an algorithm known only by the individual cellular phone and the wireless network. Every time a call is place, the wireless network asks a series of questions to the mobile unit. If the cellular phone cannot answer the encoded questions correctly, the call is immediately disconnected, and the network is alerted of the invalid user.

FUTURE OF CELLULAR TECHNOLOGY

The future is moving away from analog based technologies, and into the digital realm. Digital communications use a series of transmitted bits (1’s and 0’s) instead of a radio frequency wave. Radio frequency information is encoded into a stream of bits, with each set of bits representing a piece of the analog frequency information. The bits are then transmitted through to a receiver, where the bits are decoded back into an analog signal, which the user can understand.

There are three competing technologies as we head into the 21st century. GSM (Global System for Mobile Communications) is the standard in Europe, and TDMA (Time Division Multiple Access) and CDMA (Code Division Multiple Access) are competing with GSM for the North American market. Multiple access simply refers to the ability of a system to support multiple, simultaneous users on the same channel, instead of just one user in the case of analog AMPS.

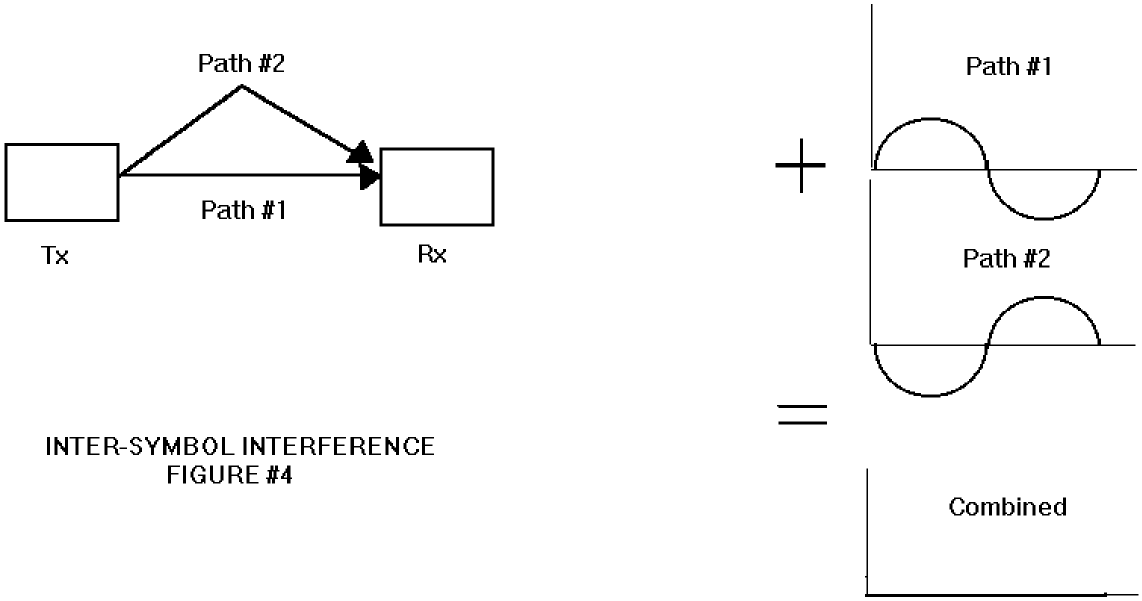
The U.S. is five years behind Europe in introducing wireless systems, because of a lack of standards. The European community decided on the GSM standard in 1988, so that the technology could be used anywhere within the 15 nation region. In the U.S. however, the FCC (Federal Communications Commission) decided to auction off radio spectrum for digital purposes, and then allow the carriers to choose their system’s technology. This has resulted in a conflict in technologies whereby, 24% of the country is covered by GSM, 14% by TDMA, and 57% by CDMA. The largest problem created by this scenario, is that users can expect more difficulties when roaming, as these technologies are currently incompatible with each other, and with analog technology. CDMA and TDMA are newer than GSM, and both offer more capacity, however the next generation of GSM will match the capacity of TDMA. The majority of the U.S. market is looking towards CDMA as the technology of the future.

GSM (the first generation digital science) is a digital based cellular system which offers three times the capacity of analog systems, thus allowing more users. It also offers a wide variety of new services such as improved authentication to prevent cloning, international roaming and compatibility with land line ISDN (Integrated Services Digital Network).

GSM has two problems associated with it. Firstly, a high percentage of signals from mobiles near the edge of a cell cross over into the time slots of mobiles near the cell’s base station, causing interference in the mobile near the base station. This problem is also seen in CDMA, and both technologies have solution to the problem with a method of adjusting for delayed signal propagation, but the technique is not 100% flawless. Secondly, GSM handsets send out low end frequency bursts when transmitting which interfere with electronic devices nearby, such as hearing aids and pacemakers.

TDMA (second generation digital science) increases channel capacity by cutting up each signal and assigning each piece to a different time slot. This technology increases the capacity of the cellular system by three over analog. TDMA also offers increased security, as well as enhanced sound and e-mail capabilities.

The largest problem with TDMA is that it experiences ISI (Inter-Symbol Interference) where a signal origination from a mobile, or a base station takes different paths to its destination, and when it arrives, the same signal, taking different paths may interfere with each other by being out of phase (figure #4). The receiver then has a tough time identifying correct adjacent symbols. To battle this problem, TDMA has to relinquish some of its capacity availability by making each symbol longer in duration.



INTER-SYMBOL INTERFERENCE
FIGURE #4

CDMA (third generation digital science) is the most popular technology used in North America. CDMA was developed by the military for uses in anti-jamming (it is difficult to jam CDMA due to spread spectrum technology), ranging (ability to know when a signal will be received over a certain distance), and secure transmissions of information (spread spectrum signals are extremely tough to detect).

“Spread Spectrum” spreads information contained by a certain signal over a much larger bandwidth than the original signal. Each user’s signal starts at a standard rate of 9600 bits per second, and then this information is spread to a higher rate of 1.23 Mega bits per second. A digital code is then applied to each individual’s signal and all of the users are grouped together into one channel. At the receiver, the digital codes are removed after identifying each individual user’s signal, and the original signals are separated from each other and spread back to a rate of 9600 bps.

NEW DIGITAL SECURITY

The latest security invention for digital phone security is the “Clipper Chip.” AT&T have developed a Telephone Security Device which brings advanced encryption technology to cellular phones. The transmitting phone’s digital signal is encrypted using a government approved algorithm, and is decrypted at the receiving end by a Telephone Security Device which is easily attached to a portable phone. The “Clipper Chip” technology allows encryption to prevent unauthorized access to data transmitted over air waves, while at the same time it allows the federal, state and local government agencies to decrypt at will, in order to intercept incriminating phone conversations. Due to the ability of the government to eaves drop, many users are reluctant to use the technology.

CONCLUSION

Today, the cellular world is facing some major changes. There is a move from analog technology to digital technology, and there is a high investment in securing information. “Bandits” steal $2 million a day from cellular carriers and users, not to mention information which could be harmful in many other areas besides fiscal. Digital technology along with the “Clipper Chip” and other security software packages hope to quell the advantages held by thieves. Only time will tell how successful carriers will be in enhancing their security measures, and in which direction the world will take with digital technology standards.

GLOSSARY

AMPS - Advanced mobile phone service. It is the analog standard for North America.
Bandwidth - Measured in Hertz, it is a measurement of an amount of frequency spectrum.
Base Station - The transmitter/receiver which is present in each cell.
CDMA - Code division multiple access is a low powered spread spectrum technology which offers greater channel capacity over analog AMPS, TDMA and GSM. It uses bits to assign a code to each signal and then spreads the signal over a wide spectrum, thus allowing for multiple users to be carried simultaneously.
Cell - The geographic area covered by a single receiver/transmitter.
Channel - The bandwidth of the radio frequency spectrum which information occupies. Measured in Hertz.
ESN - Electronic serial number. It is the number which a mobile transmits to base stations to identify itself.
FCC - Federal Communications Commission. They are the U.S. government’s agency responsible for allocating radio spectrum to the communications industry.
FDMA - Frequency division multiple access. Same technology as TDMA.
GSM - Global system for mobile communications. It is the European digital standard.
Hand-off - The process of transferring a mobile unit’s home base station from one cell to another.
ISI - Inter-symbol interference. Signals take a multitude of paths from the transmitter to the receiver, and sometimes, the signals arrive out of phase with each other at the receiver, and make it difficult for the receiver to make the correct decision on what it is accepting.

Spectrum - The entire range of electromagnetic waves which are produced and transmitted by sources such as the sun and cellular phones. Throughout the spectrum, EM waves have different wavelengths, which correspond to different frequencies, High frequencies show up as light, and the lower frequencies are used for communication purposes.
Spread Spectrum - A technology invented by the military, whereby radio signals are spread throughout a spectrum in order to make jamming and interference of a signal difficult.
TDMA - Time division multiple access increases a channel's capacity by cutting signals into pieces and assembling each piece into a different time slot. Allows one channel to carry multiple users simultaneously.

BIBLIOGRAPHY

Interview, Chris Marchuk, Access Fraud Division, Telus Mobility Canada, June 7th, 1997.

Network Security (Data and Voice Communications), Fred Simonds, McGraw-Hill, 1996.

Network Security (How to Plan for It and Achieve It), Richard H. Baker, McGraw-Hill, 1995.

Policing the Digital World, Vic Sussman, U.S. News and World Report, Dec. 6, 1993.

Uncle Sam, Please Pick a Cell Phone Standard, Catherine Arnst, Business Week, Feb. 6, 1997.

Wire Pirates, Paul Wallich, Scientific American, Aug., 1993.

Wireless: The Revolution in Personal Telecommunications, Ira Brodsky, Artech House Publishers, 1995.

Wireless Communications (Future Directions), Jack M. Holtzman and David J. Goodman, Kluwer Academic Publishers, 1993.

Wireless Personal Communications (The Future of Talk), Ron Schneiderman, IEEE Press, 1994.

www.att.com/PRESS/1094/941010.nsa.html.

www.ba.com//nr/96/feb/2-29 cellfraud.html.

www.cdg.org/a_ross Arthur H. M. Ross, Ph.D., 1996.

www.teledotcom.com/0896/features/tdc 0896fraud4.html

www.wireless-gte.com