MOBILE TECHNOLOGY AND SAFETY

H. Radha Krishnan

Assistant Professor, Department of Electronics
G. Venkataswamy Naidu College (Autonomous), Kovilpatti.
E-mail: hradhakrishnan11@gmail.com

Received: September 06, 2024, **Accepted**: January 01, 2024, **Online Published**: February 15, 2024

ABSTRACT

Many users hesitate to use technology because the government can listen to conversations. Major developments are currently occurring in the cellular industry. Analog to Digital technology is being replaced, and there has been a major investment in information security. Cellular technology enables communication by establishing a secure two-way radio between the mobile device and the wireless network. It repeatedly utilizes radio frequencies (radio channels) in a market with minimum interference to service several simultaneous discussions. Wireless communication is becoming more and more common as the twenty-first century begins. The evolution of analog cellular, security concerns and remedies, and the advent of a new age with the deployment of digital cellular technology will all be covered in this article.

Keywords: Cellular Technology, Analog to Digital Transition, Information Security, Wireless Communication, Digital Cellular Technology, and Radio Frequencies.

Introduction

In the ever-evolving telecommunications landscape, mobile technology is a cornerstone of modern communication, transforming how we interact, conduct business, and navigate our daily lives. The advent of cellular technology, a remarkable leap from tethered lines to the freedom of wireless

communication, marked the beginning of this transformative journey. However, the transition from analog to digital cellular systems did not merely enhance connectivity; it reshaped the security paradigms within the mobile communication domain.

This paper delves into the significant transition from analog to digital cellular technology, underscoring the pivotal shifts in communication efficiency, security concerns, and the continuous evolution toward more advanced, secure, and reliable forms of mobile communication. With the government's capacity to monitor conversations leading to a hesitant adoption of technology by users and the burgeoning investment in information security shaping the cellular industry's trajectory, understanding the complexities of this evolution becomes paramount.

Through a comprehensive exploration, this study aims to dissect the progression of mobile technology from its analog roots to the digital age, spotlighting the dual challenges of enhancing communication security and safeguarding user privacy. By examining the cellular concept, analog versus digital technologies, and the inception of security measures designed to combat fraud and unauthorized access, this paper endeavors to provide a holistic view of the mobile technology landscape. Moreover, it seeks to offer insights into future advancements, emphasizing the need for innovation in security measures to address emerging threats in an increasingly digital world.

As we stand on the cusp of new technological horizons, with digital cellular technology paving the way for unprecedented connectivity, the implications for security, privacy, and communication efficiency invite rigorous scrutiny. This paper endeavors to contribute to the ongoing dialogue on mobile technology and safety, aiming to illuminate the path forward in navigating the complex interplay between technological advancement and security imperatives in mobile communication.

Next Generation of Cellular Technology

What use did the first cell phones serve? They provided access to a phone for persons who were conducting business while driving. First-generation cell phones cost at least $3000 to install in vehicles. The cost of the service was only acceptable to salespeople and business travelers. Cell phone technology's price started to drop over time, and the market started to grow.

Before the advent of more advanced technology and expanding the spectrum's capacity in the early 1990s, cell phones were still only available in automobiles. In

the past, the only way to fit more users onto a certain spectrum was to reduce the bandwidth allotted to each user. The channels carried less information, and there was a higher likelihood of multipath fading, which was the main drawback of offering each user a smaller slice of the pie.

Due to the increased demand for mobile phones, the FCC's band of frequencies set aside for mobile communications conflicted with other users. The idea for "cellular" emerged from the wireless industry's realization that it would not be able to satisfy demand.

Cellular Conceptions

The cellular approach allows for the recurrent employment of a variety of frequencies. Cellular radio uses many channels to transmit a user's information instead of delivering data over one channel between one mobile location and another fixed location. Hexagonal-shaped cells divide up each geographic service area. In Figure #1, each cell is assigned one of the seven channels most cellular providers have created for the mobile frequency spectrum. Figure #1 illustrates how similar channels cannot border in a hexagonal pattern.

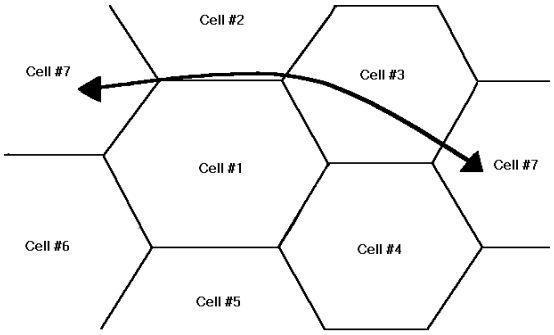


FIGURE #1

The cellular concept barred messages from one cell from influencing other cells by requiring the fulfillment of two conditions. First, low-power transmitters for the base station and mobile devices were required. The mobile transmitter power had to be less than 10 Watts, whereas the power of the base station had to be fewer than 100 Watts. Additionally, the frequency spectrum utilized has to be suitable for short-range communications. This function was present in both the 800 MHz and 900 MHz bands.

The argument put forth by experts was that this technology would permit unending expansion. Cellular carriers could reduce the size of their cells if there were too many users on one channel in a given cell. The load increased by four when the cell size was cut in half. However, this concept comes with a few things that could be improved. Cost is the main issue for mobile service providers. The carrier would need to invest $300,000 to $500,000 per cell site in additional hardware if the cell layout was reduced. Additionally, carriers

would need to install more landlines specifically designed to carry phone signals back to their switching stations and purchase more real estate. As the network grows, hand-off also gets more challenging.

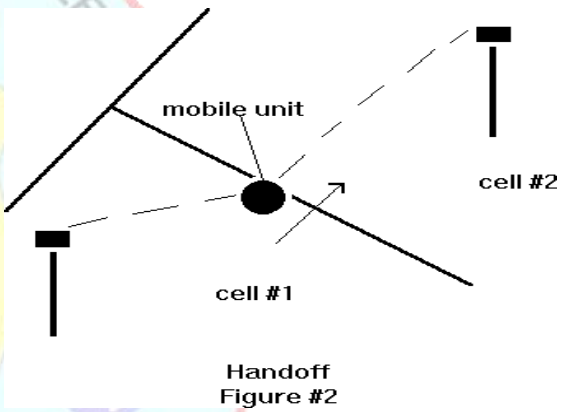
Analog Mobile

Despite its rapid change, the most common cellular technology today still operates analogously. In this statement, "analog" refers to straightforward electromagnetic waves that transmit information that can be measured directly from the mobile device to the base station and vice versa. As a result, the data does not need to be decoded at the receiver and is not encoded for conveyance.

AMPS (Advanced Mobile Phone Service) is the ideal cellular protocol for analog systems. The frequency division multiple access, or FDMA, method divides the radio spectrum into 30 KHz slices. Some systems use N-AMPS (Narrowband-AMPS), which divides the spectrum into 10 KHz slices. Within a cell, one channel equals one slice. Only one user at a time may utilize this channel. No other user can utilize the channel before the initial call is stopped or transferred.

Off In Analog Hand

A mobile transmitter hands off (Figure #2) when it exists one cell enters another. Users experience a delay when using analog cellular systems because the hand-off takes about 200 milliseconds to complete. As cell size decreases, there are more hand-offs, and analog cellular experiences more noise and dropped calls due to hand-offs than digital cellular, which uses TDMA and CDMA technology.



Handoff
Figure #2

A predetermined number of hand-offs may occur, depending on the speed of the mobile unit and the surroundings in which the mobile transmitter is being utilized. For instance, on an urban expressway, handoffs for a car traveling at 65 mph would occur every minute instead of every 9 minutes on a rural route (figure #3). The number of mobile users actively moving in a cell at any given time is multiplied by the number of handoffs.

Case	Tempo (mph)	Speed (Kmh)	Cell Radius (Km)	Hand-offs
Highway in Remote area	65	104	16	0.33
Urban Freeway	65	104	1.6	3.25
Urban Streets	30	48	1	2.4
Urban Pedestrian	1.5	2.4	1	0.12
Microcell Pedestrian	1.5	2.4	0.1	1.2

*The number of cells transited is approximately 0.65*velocity*T/R

T = duration of call 93 mins was utilized above

R = radius of the cell

Hand Off Includes

1. A single cell initially provides service to the mobile unit.
2. Base stations regularly assess the quality of the air link to determine whether the existing cell is deteriorating and whether a new cell would be better for the mobile unit.
3. For the new base station to identify the mobile and begin the handoff, the old base station sends data so that it can do so.
4. The hand-off is communicated to the mobile.
5. The mobile recognizes the new cell as it starts to service the mobile.
6. Service to the mobile may be terminated by the old cell.

Using AMPS analog technology for hand-off has several drawbacks, including:

7. The transition between cells is “hard.” communication is therefore broken during cell transfers.
8. There is never a simultaneous link between the mobile unit and the two cells participating in the hand-off because it can only connect to one station at a time. This leads to dropped calls and the “hard transfer.
9. Since base stations test the quality of the airlink than mobile devices, measurements are less accurate. Base station’s estimations of transmission power can be off because they can’t tell the difference between a desired signal and an interference signal.

Roaming

Mobile users are called roaming when they leave the service provider’s coverage area. Because carriers were given licenses on a city-by-city basis when they purchased them, roaming occurs frequently once a user leaves their immediate area. Since cellular service providers aim to offer a seamless network to their customers,

this presents a challenge. Incoming calls to the roaming mobile unit must be successfully transferred from the host carrier's cells to the home company's cells in a series of successful hand-offs. This increases the potential for access fraud.

Security Concerns

A new species of burglars emerged due to the development of mobile phones. It's estimated that cellular fraud costs US$2 million every day. Due to the exponential expansion of cell phone use (17000 new customers are sold daily in the U.S), carriers and the law have difficulty catching and convicting violators. Cell phone customers are still liable for costs even if only one hacker is captured each day. Most security issues can be divided into three groups.

1. Fraudant access
2. Fraud involving mobile subscriptions
3. Stolen equipment

Access to The Calling System

Access Fraud can take two different forms. The two most popular methods of cellular fraud are cloning and tumbling. Before utilizing the duplicated gadget, a "bandit" programs a mobile phone with the ESN (Electronic Serial Number) or MIN (Mobile Identification Number). Another user went through the process of "cloning." The legitimate owner of the ESN is still being charged for using the counterfeit phone during this time. Most reprogrammed clone phones are subsequently offered to consumers who place international calls at substantial discounts.

When roaming, cell phones behave like "tumbling phones" and change their ESN or MIN after each cell. The bandit can momentarily make unlawful calls while the phone is traveling between cells and outside of the home carrier's coverage area due to the frequent tumbling of the ESN or MIN, which confuses cellular computers.

How do "bandits" get into possession of ESNs or MINs? The procedure is fairly simple when using an analog cell phone. To pick up a cellular radio channel, the burglar merely needs a UHF receiver, a radio frequency scanner, and knowledge of the correct frequency/ the mobile unit communicates its ESN or MIN to the base station over the airways for identification whenever a cell phone is "on" or places a call. Consider the following illustration to illustrate how simple it is to get a person's ESN or MIN from a burglar: Your cell phone is on but not in use as you speed down a city street, but your ESN is being sent.

When burglars get their hands on your ESN, they swap out the phone's

original chip for one encoded. Clever thieves and poor chip assembly have allowed cloning to continue with inconceivable success, even though cell phones are meant to be difficult to reprogram without causing reversible damage.

Fake Subscriptions

When people purchase cell phone accounts using false identification and fail to pay their bills, this is known as subscription fraud. Because deactivation occurs after numerous defaults and the first payment often arrives after one month of service, unauthorized users have time to rack up substantial cell phone bills.

Mobile Theft

The original chip in the phone that a thief is coupling is swapped out for a chip that has been programmed with your ESN once they get your ESN. Even though it is impossible to reprogram a cell phone without incurring permanent harm, shrewd thieves and poor chip assembly have made it possible for cloning to continue with unfathomable success.

Recommendation for Users

Users can take the following actions to protect their privacy overall and fight clone/tumbling fraud:

1. When not in use, the cell phone's lock feature makes it impossible for anyone to use the phone without the correct unlock code.
2. Inform the cellular provider of frequently dropped or interrupted calls.
3. Take the ESN out of the phone's battery. Some older phones have an ESN on the battery, though not all do.
4. Carefully review your monthly bill. Most thieves are cunning enough to make undetectable calls to users who have been charged for them.
5. Request that access to overseas phone numbers that you won't be dialing be blocked by your provider
6. Never talk about personal or monetary issues on a mobile network. NEVER provide your credit card number over the phone, radio, or TV

Technologies for Security Available From Cellular Transporters

Cellular service providers use the most well-liked security packages, including AT&T, GTE, Sprint, etc. The supplier genuinely describes each product to buyers. "FraudBusterTM uses artificial intelligence to perform real-time subscriber call analysis to identify and stop wireless fraud. Coral's fraud detection/prevention system offers extensive (post-call) processes that enable fraud detection, network operator reporting, and updating

cellular switches or home location registers.

Users can configure several responses to Fraud Buster notifications. Fraud Buster offers subscriber fraud, clone phones, and tumbler phones as three of the most prevalent types of wireless fraud at the individual subscriber level. The FraudBuster software system includes unique capabilities and updatable antifraud algorithms to handle established and new fraud types.

The features of FraudBusterInclude

1) A database of subscriber usage patterns
2) A call analysis of customers
3) Evaluating velocity
4) Investigating regional disparity
5) Comprehensive proprietary antifraud algorithms Artificial Intelligence."

Using real-time billing data, the fraud analysis and control tool CloneGuard TM may identify erroneous calls. It offers a system of support to assist wireless operators in dealing with fraud situations and warns them when fraud happens on their networks. Thanks to powerful algorithmic analysis and real-time billing data gathering, CloneGuard can instantly identify fraudulent circumstances, including aberrant usage patterns or inconsistent consumption.

CreditCuard TM is a technology that continuously monitors wireless users and alerts the carrier when a pre-set credit limit is reached. Credit Guard uses tools to provide real-time ratings. This technology enables carriers to reduce their financial risk while eliminating subscription fraud and supplying consumers who pose a credit risk.

The Clone DetectoerTm technology is one of the most effective fraud detection tools now on the market. Employing powerful artificial intelligence capabilities immediately notifies wireless operators of counterfeit fraud on an inter or intercarrier switch basis. Additionally, it provides a nationwide defense against roaming fraud.

The groundbreaking interim standard 41(IS – 41) is the foundation for FraudManager (SM), the industry's first pre-call roaming validation solution. In around 700 markets, including the top 200 in the US, it has been implemented by about 100 carriers.

The StatChekTM service automatically confirms a cell phone's status before activation. It ensures the mobile device isn't being used fraudulently or has yet to be reported stolen in other areas.

Fraud Manager (SM) is based on the cutting-edge interim standard 41(IS-41). Seven hundred market totals, with the top 200 in the US included. About 100 carriers

have implemented it. The StatChekTM service automatically confirms a cell phone's status before activation. It ensures the mobile device isn't being used fraudulently or has yet to be reported stolen in other areas. Clone fraud and other developing types of fraud are thwarted by FraudForce(SM) services, a comprehensive range of fraud control services, allowing carriers to implement specialized solutions that satisfy their changing business demands. Home carriers can prohibit, limit, and allow roamers in the carrier-selected high fraud markets thanks to the Fraudinterceptor (SM) service. Sent to the FRaudChallenger (SM) service, another product in the FraudForce family, are restricted roamers.

A Personal Identification Number (PIN) must be entered, or a carrier customer care agent must be contacted; the automated challenge and response system Fraudchallanger examines restricted roamers. Carriers can send roamers to GTE's worldwide fraud protection (SM) center's customer care agents so that they can speak with them directly and confirm their validity.

Authentication is a unique security package that mobile-operated companies find quite useful. Every time a call is made or received, encrypted passwords are transmitted to the cellular network and a mobile phone user. A very sophisticated secret code and number are used for authentication, based on a method accessible only via the wireless network and the specific mobile phone. The wireless network frequently questions the mobile device when a call is placed. If the cell phones cannot correctly respond to the encoded questions, the call is instantly terminated, and the network is alerted of the invalid user.

Cellular Technology's Feature

In the following years, analog-based technologies will be supplanted by digital ones. Digital communication uses a series of transmitted bits (1s and 0s) instead of a radio frequency wave. Each set of bits in a stream used to encode radio frequency data represents analog frequency data. After transmission, the bits are taken up by a receiver and translated into an understandable analog signal.

There are now three competing technologies as the twenty-first century gets started. The Global System for Mobile Communication (GSM), which is the industry standard in Europe, competes with the Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) technologies in North America. Numerous access indicates that a system can accommodate multiple concurrent users on the same channel

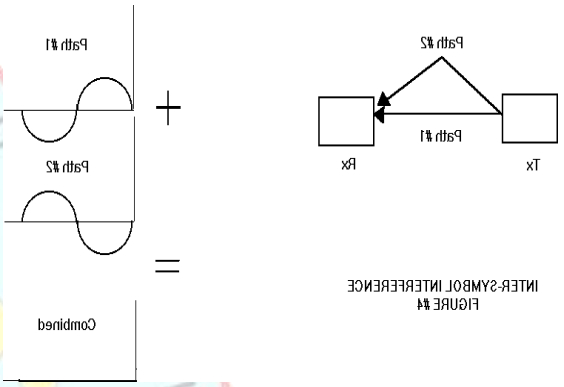
instead of just one, as opposed to analog AMPS.

GSM, the first generation of digital cellular technology, is based on digital technology and supports three times as many users as analog systems. Also available is a vast array of brand-new features, including enhanced authentication to avoid duplication, global roaming, and support for landline ISDN (Integrated Features Digital Network).

Two problems with GSM need to be fixed. Mobiles adjacent to a cell's base station frequently experience signal interference from mobiles near the edge of the cell because their signals frequently cross over into certain time slots. Although the technology could be more flawless, both methods provide a way to account for delayed signal propagation, a problem that also affects CDMA. Second, GSM handsets produce low-end frequency bursts during transmission that might disrupt neighboring electrical devices such as pacemakers and hearing aids.

By dividing each signal into its time slot, the second generation of digital technology, or TDMA, boosts channel capacity. Compared to analog, this method triples the capacity of the cellular system; TDMA provides stronger security and better email and sound capabilities.

Inter-symbol Interference (ISI): The fundamental issue with TDMA is that it can cause signal interference when a signal from a mobile or base station travels down different paths to its destination and, once there, the same signal traveling down several paths may interface with itself by



INTER-SYMBOL INTERFERENCE
FIGURE #4

traveling out of phase (figure #4).it thus becomes difficult for the recipient to identify the right neighboring symbols. To address this problem, TDMA must prolong each symbol, which reduces some of its capacity availability.

CDMA (third-generation digital science) is North America's most widely used technology. The military developed CDMA for use in secure information transmission (spread spectrum signals are extremely challenging to detect), range (the capacity to predict when a signal will be received over a particular distance), and anti-jamming (CDMA is tough to jam due to spread spectrum technology).

Spread spectrum enables the information in a transmission to be

dispersed over a much wider bandwidth than the original signal. Before beginning at a standard rate of 9600 bits per second, the signal for each user is first stretched out at a greater rate of 1.23 Megabits per second. The signals of all users are then integrated into a single channel after each signal has been assigned a digital code. After the digital codes have been eliminated and the signals of each user have been identified, at the receiver, the original signals are split up and re-spread at a rate of 9600 bps.

Digital Security in The Present

The "Clipper Chip" is the most recent innovation in digital phone security. A telephone security device created by AT&T makes modern encryption technology accessible to mobile devices. A telephone security device that is now accessible for mobile devices. A telephone security device that is easy to attach to a portable phone decrypts the digital signal of the transmitting phone using a method of encryption that has been certified by the government. Data sent over the radio is encrypted using "Clipper Chip" technology to prevent unauthorized access. Federal, state, and local government officials have the freedom to decrypt data whenever they want, which gives them the power to listen in on shady phone calls. Many people hesitate to use the device because the government can listen to private discussions.

Conclusion

The "Clipper Chip" is the most recent innovation in digital phone security. Thanks to a telephone security device created by AT&T, modern encryption technology is now accessible for mobile devices. A telephone security device that is easy to attach to a portable phone decrypts the digital signal of the transmitting phone using a method of encryption that has been certified by the government. Data sent over the radio is encrypted using "Clipper Chip" technology to prevent unauthorized access. Federal, state, and local government officials have the freedom to decrypt data whenever they want, which gives them the power to listen in on shady phone calls. Many people hesitate to use the device because the government can listen to private discussions.

Definitions

- 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 found in each

cell.

- CDMA – Code Division Multiple Access - is a low-powered spread spectrum technology with greater channel capacity than analog AMPS, TDMA, and GSM. It assigns a code to each signal using bits and then spreads the signal over a wide spectrum, allowing several users to be transported simultaneously.
- Cell – A geographical area served by a single receiver/transmitter
- Channel – The bandwidth of the radio frequency spectrum occupied by information measured in Hertz.
- ESN – ESN Stands for Electronic Serial Number. it is the number that a mobile phone sends to base stations to identify itself
- FCC stands for Federal Communications Commission. They are the agency of the United States government in charge of allocating radio spectrum to the communications industry.
- FDMA –stands for Frequency Division Multiple Access. The same as TDMA technology.
- GSM – Is an abbreviation for Global System for Mobile Communications. It is the digital standard in Europe.
- Hand-off – The procedure of transferring the home base station of a mobile unit.
- ISI – It stands for Inter-Symbol Interference. Signals travel various paths from the transmitter to the receiver, and occasionally, the signals arrive at the receiver out of phase with each other, making it difficult for the receiver to make the correct judgment on what to accept.
- Spectrum – The spectrum is the total range of electromagnetic waves produced and transmitted by sources such as the sun and cellular phones. EM waves have varying wavelengths that correspond to different frequencies across the spectrum. High frequencies are visible as light, while lower frequencies are employees for communication.
- Spread Spectrum – A military-developed device that spreads radio transmissions throughout a spectrum to make signal jamming and interference more difficult.
- TDMA – Time Division Multiple Access - expands the capacity of a channel by serving signals and assembling each component into a separate time slot. Allows a single channel to carry numerous users at the same time.

References

Baker, R. H. (1995). Network security: How to plan for it and achieve it. McGraw-Hill.

British Airways. (1996, February 29). Cell fraud. Retrieved from http://www.ba.com//nr/96/feb/2-29 cellfraud.html

Brodsky, I. (1995). Wireless: The revolution in personal telecommunications. Artech House Publishers.

AT&T. (1994, October 10). Press release. Retrieved from http://www.att.com/PRESS/1094/941010.nsa.html

GTE Wireless. (n.d.). Home page. Retrieved from http://www.wireless-gte.com

Holtzman, J. M., & Goodman, D. J. (1993). Wireless communications (Future directions). Kluwer Academic Publishers.

Marchuk, C. (1997, June 7). Interview. Access Fraud Division, Telus Mobility Canada.

Schneiderman, R. (1994). Wireless personal communications: The future of talk. IEEE Press.

Simonds, F. (1996). Network security (Data and voice communications). McGraw-Hill.

Sussman, V. (1993, December 6). Policing the digital world. U.S. News and World Report.