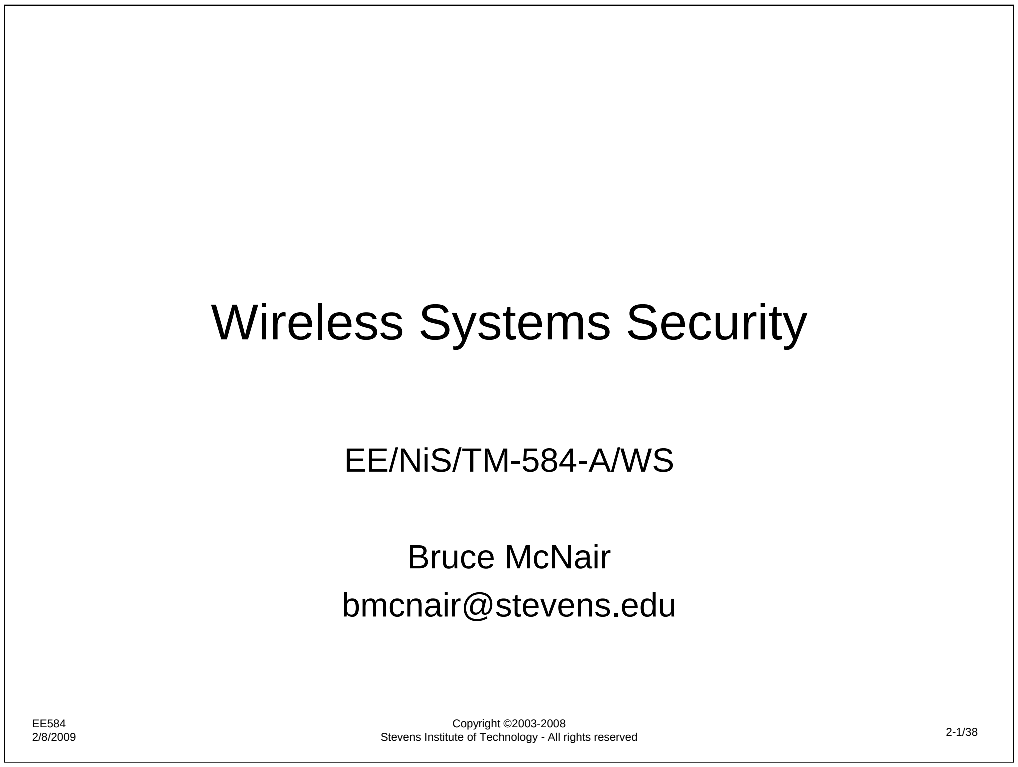
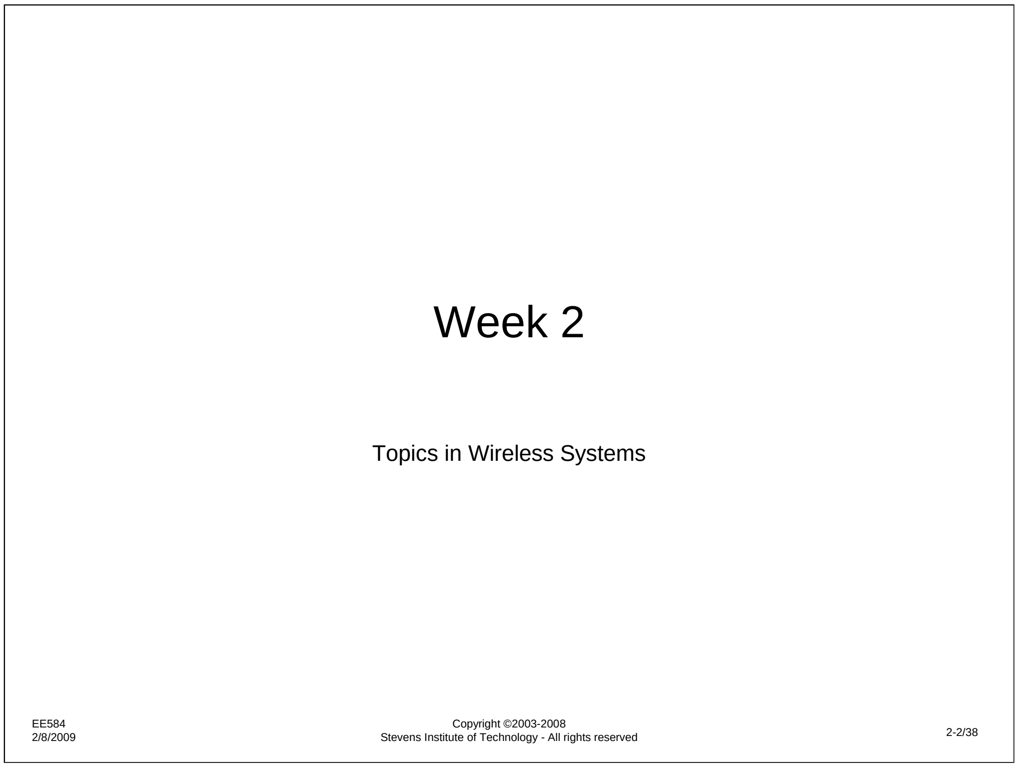


# Wireless Systems Security

EE/NiS/TM-584-A/WS

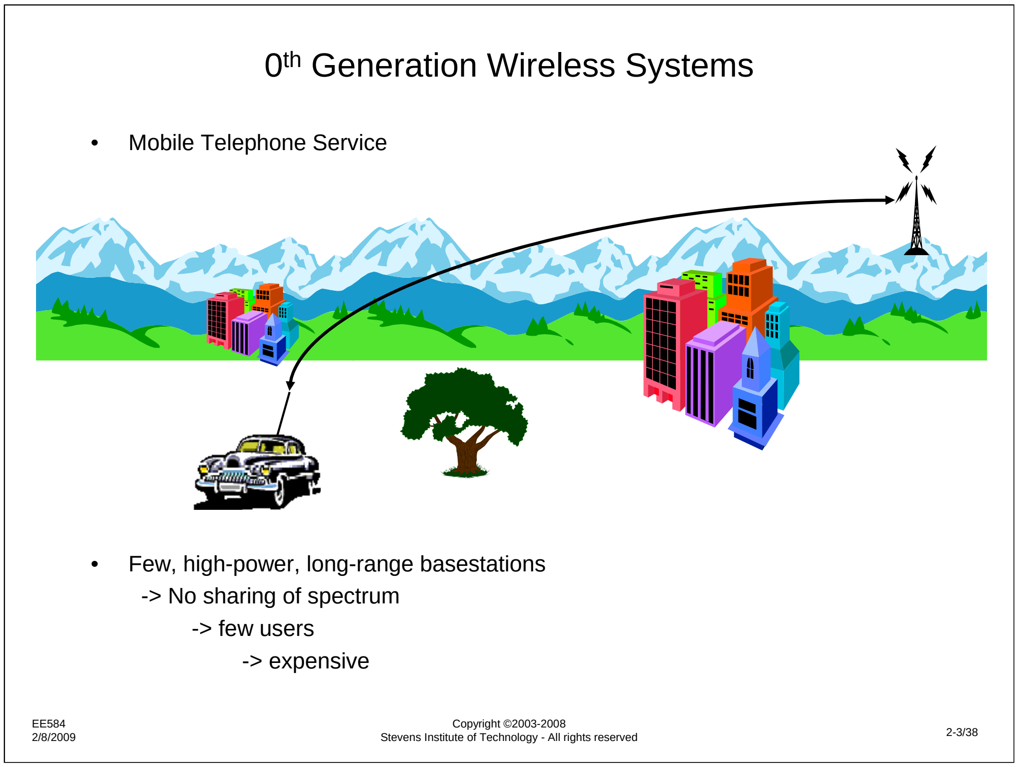
Bruce McNair
bmcnair@stevens.edu



# Week 2

Topics in Wireless Systems

We will continue the background material in wireless systems that was started last week.



# 0th Generation Wireless Systems

- Mobile Telephone Service

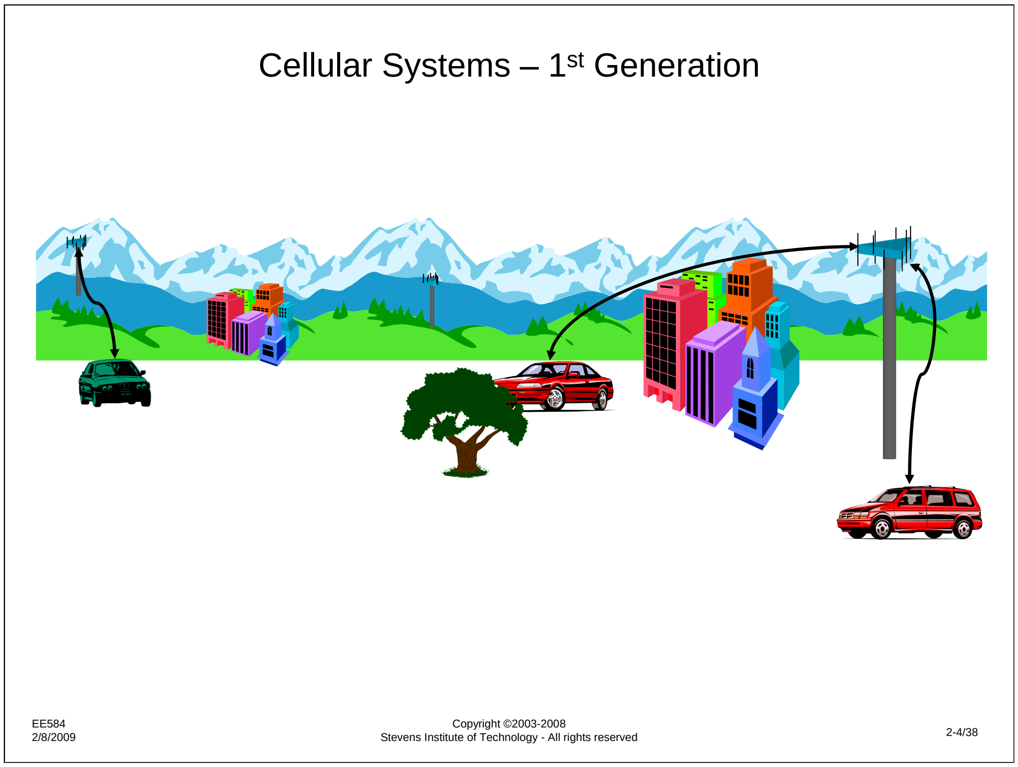
- Few, high-power, long-range basestations
  - -> No sharing of spectrum
    - -> few users
      - -> expensive

EE584
2/8/2009

2-3/38

Based on the same type of technology that was used by police since the early 1921s, the Mobile Telephone System (MTS) was the first “car telephone” system in the US, fielded in the 1940s.  Base station antennas were placed on top of high towers in the highest spots available to maximize the (generally line-of-sight) communications distance.  Doing so reduced the number of base stations needed to cover an area, but also meant that one user could not share the channel over the base station coverage area.  This lead to few users which, in turn, meant that the fixed service costs could not be shared, creating an expensive service.

While this is old technology personal communications systems, it is important to examine, since many of the current public service wireless systems are still using the same technology, for instance, law enforcement, emergency medical services, fire departments, etc.



## Cellular Systems – 1st Generation

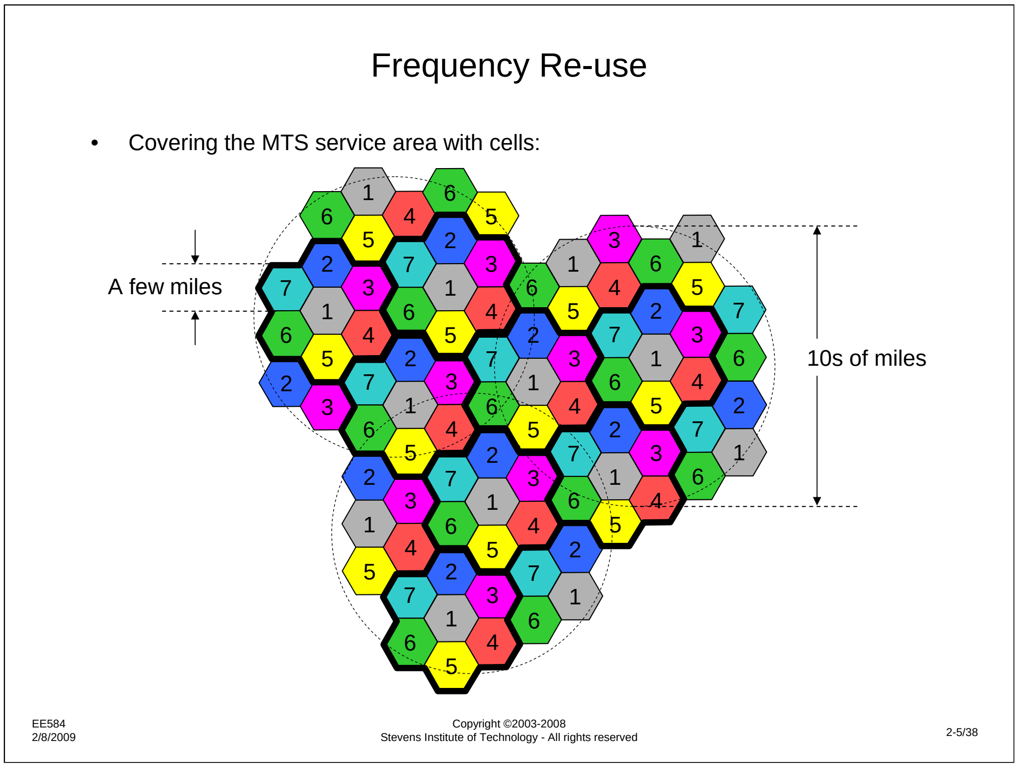
EE584
2/8/2009

2-4/38

The invention of cellular system drastically changed the environment for mobile wireless communications. Rather than having a single base station radiating over hundreds of square miles, the concept of cellular was to reduce the power, lower the antenna and thereby reduce the transmission range. Now, multiple base stations would provide service and would be able to reuse channels within a service area.

There are some obvious economic advantages to cellular service – since RF spectrum is a very valuable resource, being able to share it over different geographic areas drives down the cost of running a system. Lower spectrum costs translate into lower service costs, which make mobile communications affordable. The more affordable mobile communications has been a major driving factor in making cellular communications as popular as it has been. In turn, the deployment of affordable cellular services to large populations has driven down manufacturing costs and created a new wireless industry.

It is not unreasonable to assert that the development of cellular technology is what triggered the wireless industry as it exists today. Of course, the fact that electronics technology had evolved to the point to make these systems realizable was a key enabler, but the driver was the exploding cellular market. It is these forces that have created many of the security issues we will be addressing in this course.



## Frequency Re-use

- Covering the MTS service area with cells:

EE584
2/8/2009

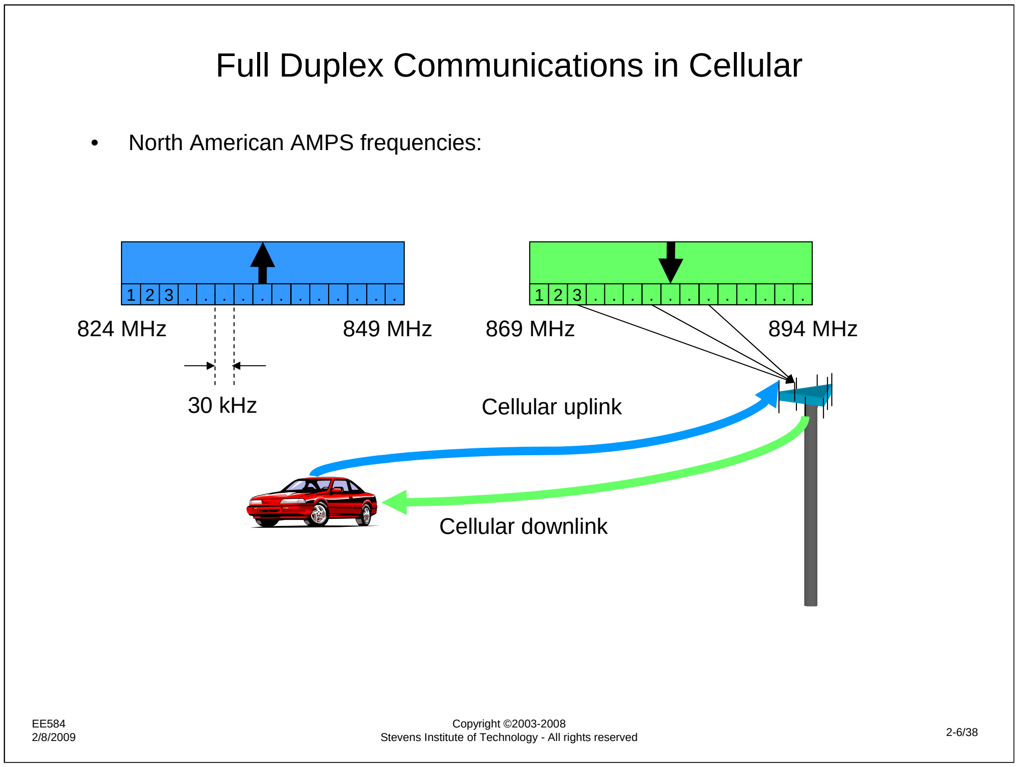
2-5/38

Let's assume that we want to provide essentially the same coverage area as the MTS system (shown as dotted circles), but we are doing so with smaller cells. By convention, the cells are drawn as hexagons, since that shape covers a plane with a regular structure. We could use square or triangular cells, just as well, but the hexagon is a better approximation to the nearly circular coverage pattern of an antenna.

How can we assign frequencies to the cells? It turns out that a cluster of 7 hexagons creates a shape that also covers a plane. If we number the hexagons within this cluster from 1 to 7, we have a frequency reuse plan – with 7 frequencies (or blocks of frequencies, or colors), we can cover an arbitrary size or shape plane, guaranteeing that the same frequency/block/color will not be closer than approximately 2 cell diameters (what is the exact spacing between the closest points in two cells using the same frequency in terms of the diameter of a circle that has the same area as the hexagon?)

This reuse of frequencies in different areas of the network is sometimes referred to as space division multiplexing, since the resource is shared (multiplexed) between users at different points in space.

There is a problem with this concept of cellular that may be apparent very quickly – every cell gets the same resources. Is it likely that usage within a geographic area is uniform? Probably not. A highway may run through the middle of this area where call traffic density may be higher than the suburban areas on the edges. This is easily remedied with cellular however – the cells can be split into smaller cells, just as the MTS "megacell" is broken into cells



## Full Duplex Communications in Cellular

- North American AMPS frequencies:

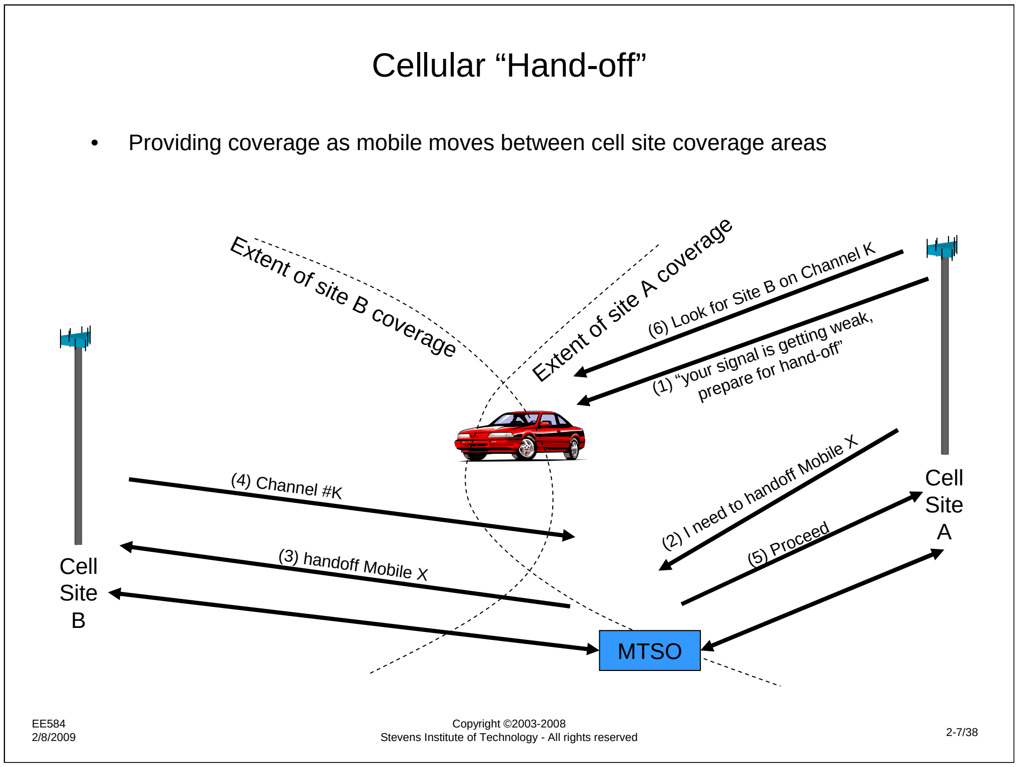
EE584
2/8/2009

2-6/38

In AMPS, each base station, according to the system reuse pattern, is assigned a group of (at least 15) channels to operate on.  The base station transmits beacon, control, and voice traffic on these downlink channels and, when a session is in progress with a mobile station, voice traffic is transmitted continuously to the mobile on one of the downlink channels.

During an active session, the mobile station is assigned a corresponding uplink channel to transmit voice and call signaling information.  Because of the 45 MHz frequency separation between each uplink and downlink channel, the mobile system is able to transmit and receive simultaneously.  Later in the course, we will discuss the “duplexer” that allows this to happen.

**Discussion topic**:  The Electronic Privacy Protection Act made it illegal to sell scanning radio receivers in the United States that were capable of monitoring the cellular channels, except to law enforcement and authorized communications companies.  How effective a deterrent do you suppose this law is?



## Cellular "Hand-off"

- Providing coverage as mobile moves between cell site coverage areas

Extent of site B coverage
Extent of site A coverage
(6) Look for Site B on Channel K
(1) "your signal is getting weak, prepare for hand-off"
Cell Site A
(2) I need to handoff Mobile X
(5) Proceed
(4) Channel #K
(3) handoff Mobile X
Cell Site B
MTSO

EE584
2/8/2009

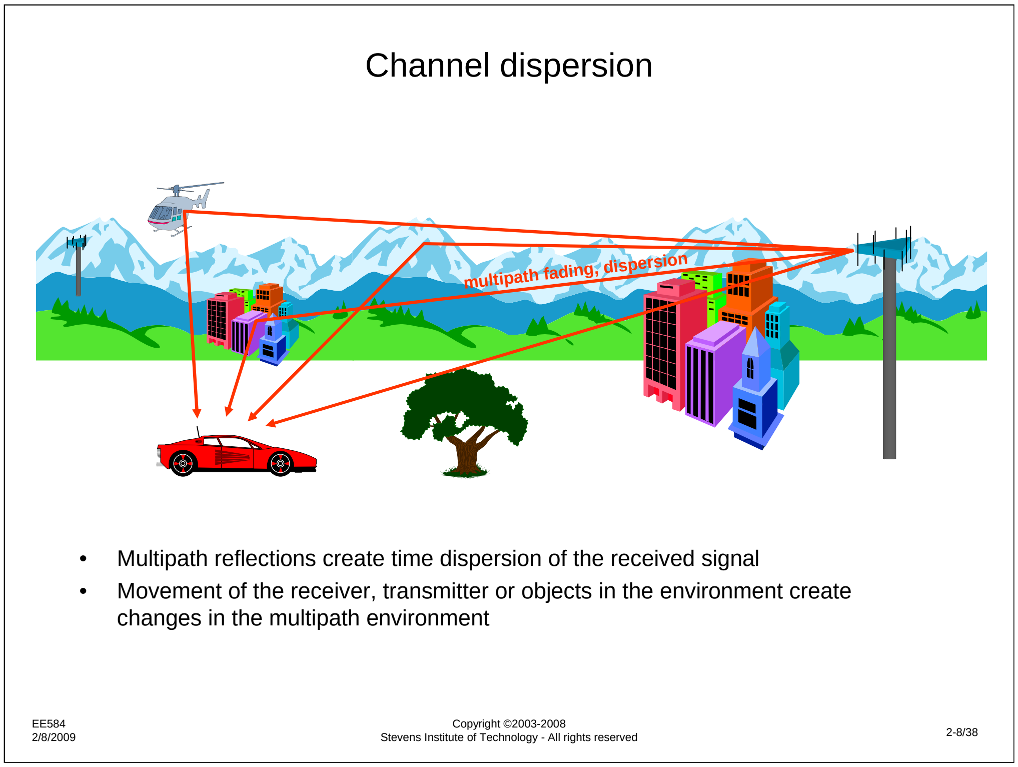
2-7/38

Because of the intentional limited range of a cell site, it is inevitable that a mobile station will sometime move out of the coverage area of a cell site. When this happens, it is necessary to "hand-off" the call to a new serving cell site.

The diagram above shows (conceptually, not exactly as the protocol operates) how a call can be handed off from one cell site to another.

The original serving base station is continually monitoring the signal strength of the mobile station. When the signal level drops below a threshold, the base station begins the hand-off process. Communicating through the Mobile Telephone Switching Office, the base station coordinates with the receiving site to transfer the call. When a suitable base station is found that has a channel available and can receive the mobile, a message is transmitted from the original base station to the mobile, telling to switch to a channel allocated to the new base station. At the same time, the voice path, which was originally connected via the MTSO to the original base station, is switched to the new base station, so the call can proceed.

**Discussion topic**: Is the hand-off process likely to make monitoring cellular calls difficult? Which circumstances would be easier and which would be harder?



## Channel dispersion

- Multipath reflections create time dispersion of the received signal
- Movement of the receiver, transmitter or objects in the environment create changes in the multipath environment

EE584
2/8/2009

2-8/38

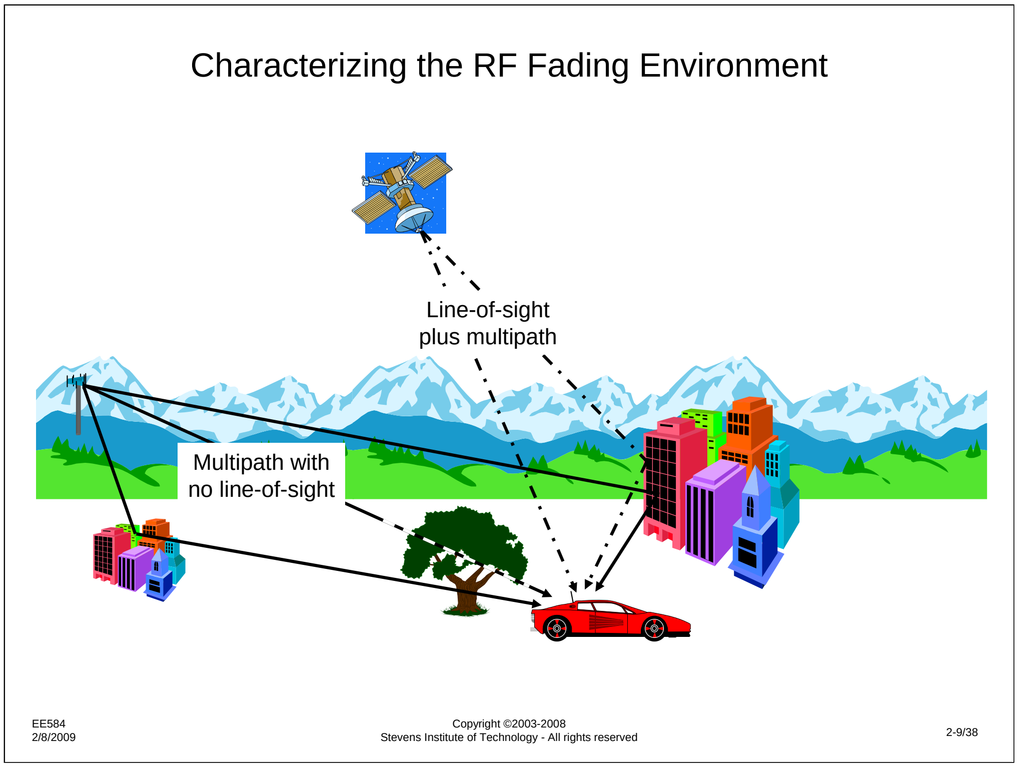
One major consideration in the design of wireless systems is the channel dispersion caused by multiple reflecting objects in the environment.

In the RF environment, especially, but also in the analog telephone plant and cable TV systems, there may be delayed copies of the transmitted signal presented to the receiver. In the RF environment, this is known as multipath, caused by reflections of the transmitted signal by objects in the environment.

Because the path length is different for the reflected replicas of the signal, they arrive at a slightly different time than the original signal. (Could they ever arrive *before* the original signal?)

This variation in signal arrival time leads to the same effect as an improperly designed filter – transmitted symbols, other than the intended one, interfere with the intended signal, creating ISI.

If you watch over-the-air television (less common today than it was 30 years ago!) multipath is immediately apparent – with a misaligned antenna or aircraft flying overhead, delayed copies of the TV signal are evident, shifted horizontally slightly from the main signal. In TV broadcasting, these delayed images are known as “ghosts.” Although not as prevalent, these “ghost” images can also exist in cable TV systems.



## Characterizing the RF Fading Environment

Line-of-sight
plus multipath

Multipath with
no line-of-sight

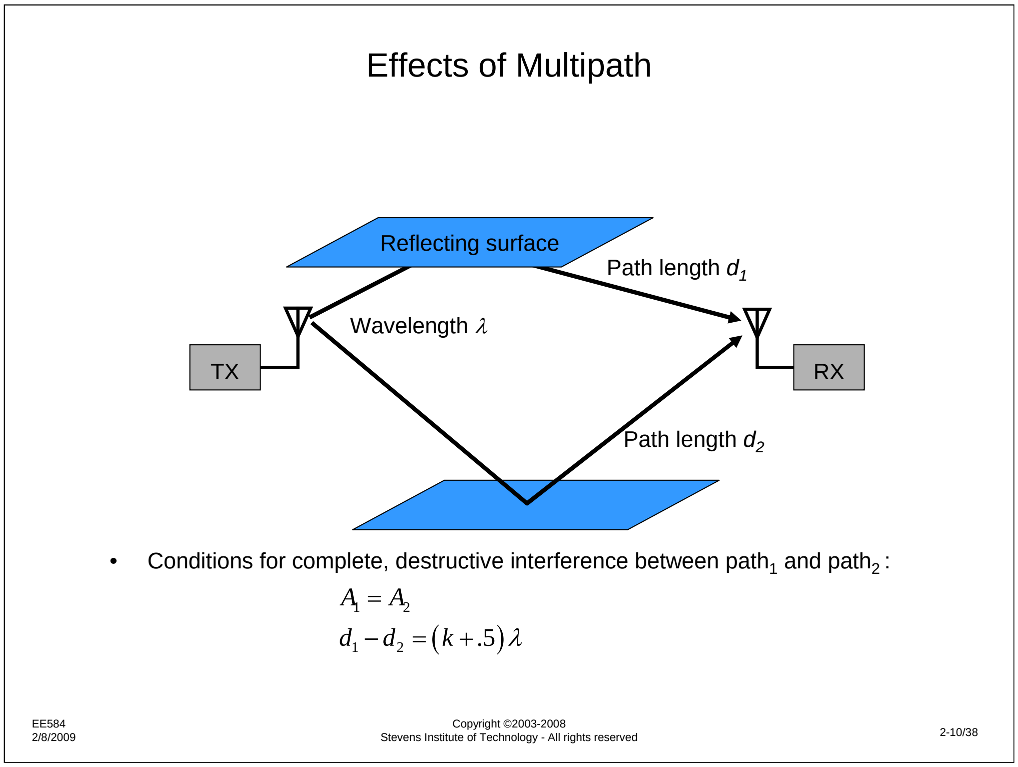
EE584
2/8/2009

2-9/38

To a high-frequency wireless signal, any metallic object that is relatively large, compared to the wavelength of the signal, looks like a reflector. Buildings, wires, vehicles, etc. can all provide reflections of the signal. This leads to “multipath” propagation, where the signal follows more than one path to the destination.

In some cases, there is a line-of-site path to the destination, as well as multipath. This might be the case if a signal is being received from a satellite that is high in the sky. This leads to “Rician” fading, referring to the Rician probability distribution of signal strengths at the receiver.

A more severe type of multipath propagation is “Rayleigh” fading, again named for the distribution of signal strengths. In Rayleigh fading, there is no clear line-of-sight path from the transmitter to the receiver. Rather, all the signals that are received are reflected signals. Rayleigh fading is characteristic of mobile wireless communications where the transmitter and receiver are close to the ground.



## Effects of Multipath

- Conditions for complete, destructive interference between path$_1$ and path$_2$ :

$$A_1 = A_2$$

$$d_1 - d_2 = (k + .5)\lambda$$

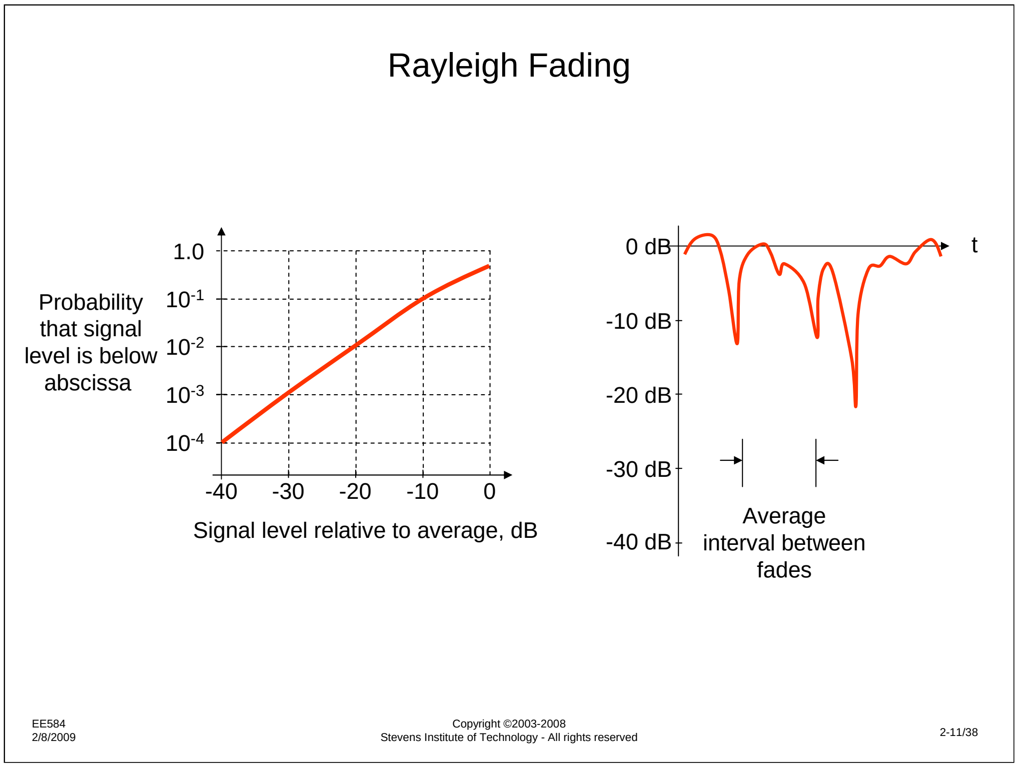
EE584
2/8/2009

2-10/38

If there are multiple paths that the signal can follow from the transmitter to the receiver, there is the possibility for the signals to cancel each other. In the simplest case, with two paths, the signals on the two paths will cancel each other if their amplitudes at the receive antenna are equal and if their path lengths differ by one-half wavelength (plus any integer multiple of wavelengths).

Because of this condition, deep multipath fades, with complete or near complete destructive interference, must be short term events. However, even if the amplitudes are nearly equal and the path lengths differ by nearly one-half wavelength, deep fades are possible.

At high frequencies, even a small movement of the transmitter, receiver, or environment can have a drastic effect. At 1 GHz, the wavelength is 30 centimeters (about 1 foot). This means that movement of 1 foot or less can change the relative path lengths by a wavelength or more, so a receiver can move from a deep null to a strong signal in this distance.



## Rayleigh Fading

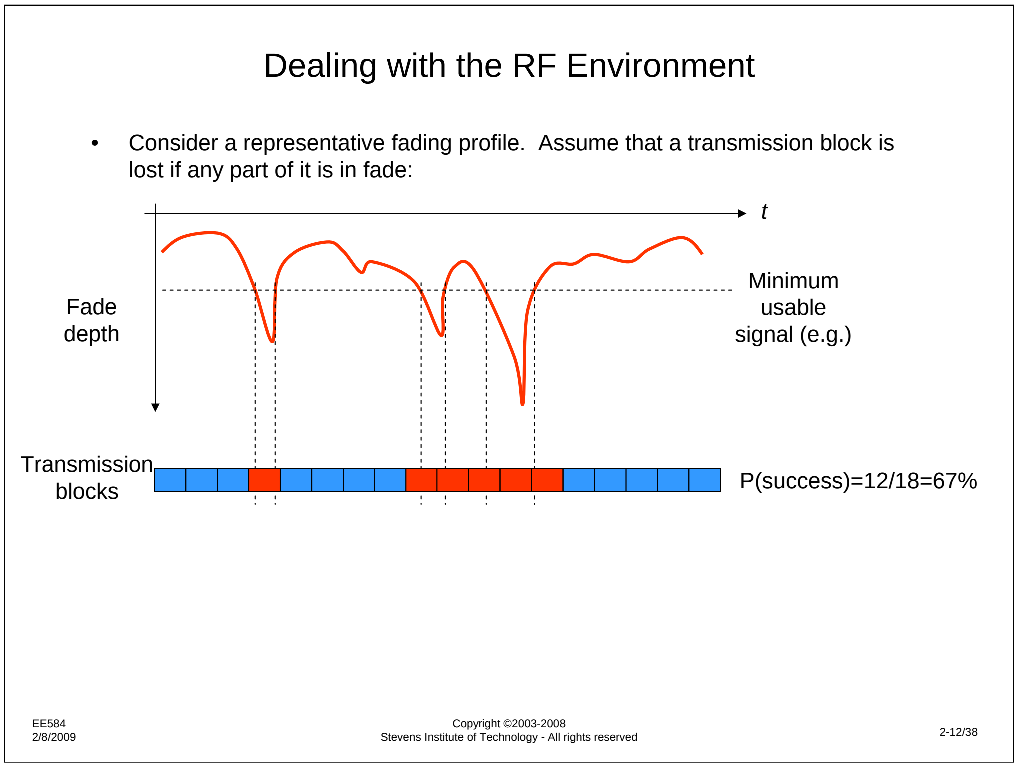
EE584
2/8/2009

2-11/38

In simple terms, this plot shows that 10% of the time, a received signal in a Rayleigh fading environment will be at least 10 dB below the average signal level. 1% of the time, the signal will be in a 20 dB fade, and .1% of the time the signal will be faded 30 dB. This is what makes the mobile wireless environment such a severe environment to design a communications system for. One can never design in enough margin (e.g., excess transmit power) to protect against the deepest fades. Other mechanisms are needed, and will be discussed later.

**One item worth noting**: the average duration between fades is related to the operating frequency and the velocity of the stations (why?)

On the positive side, there is a possibility that the multipath will cause the signal to be higher than the average signal level, improving the signal margin.



# Dealing with the RF Environment

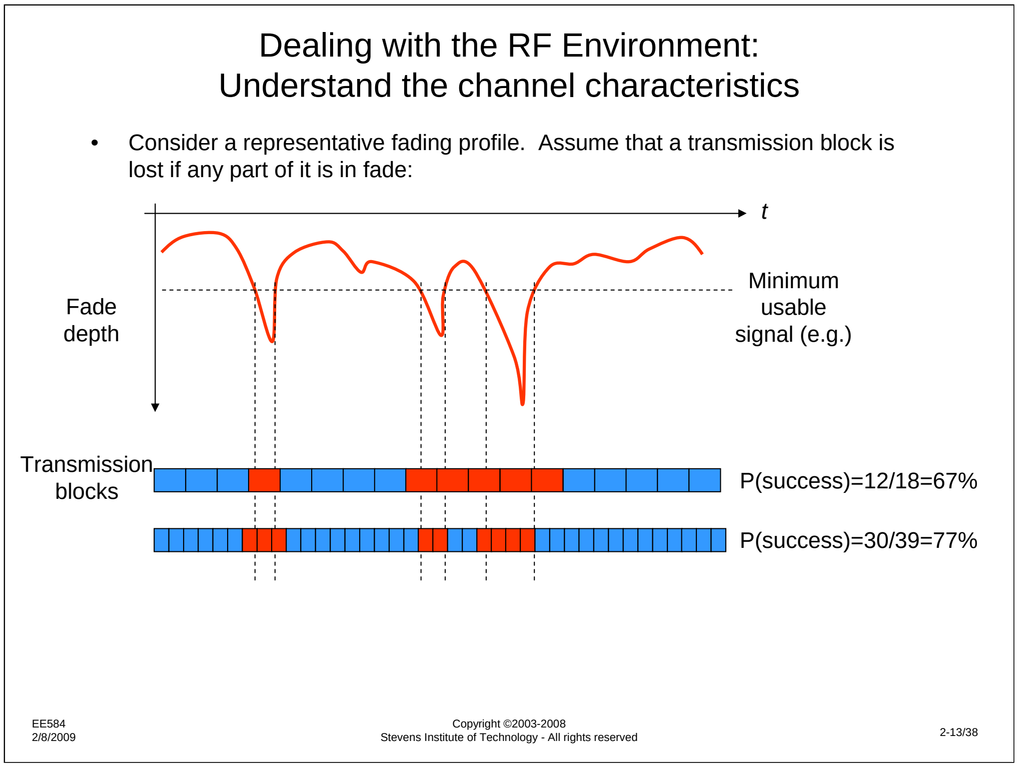
- Consider a representative fading profile. Assume that a transmission block is lost if any part of it is in fade:

EE584
2/8/2009

2-12/38

Since we are guaranteed that there will be variation in signal level in the RF environment and, with typical multipath, there will sometimes be deep fades, it is unreasonable to expect that we can transmit all of our data successfully. Here, I have illustrated how a fading channel might destroy a large number of transmission blocks. The next few slides will discuss techniques to deal with this issue.

At first glance, it might appear that this discussion of multipath and how to cope with it have no relationship to security. However, as we will see later, the same techniques that are used to combat these natural impairments can be used to deal with intentional disruption of wireless signals.



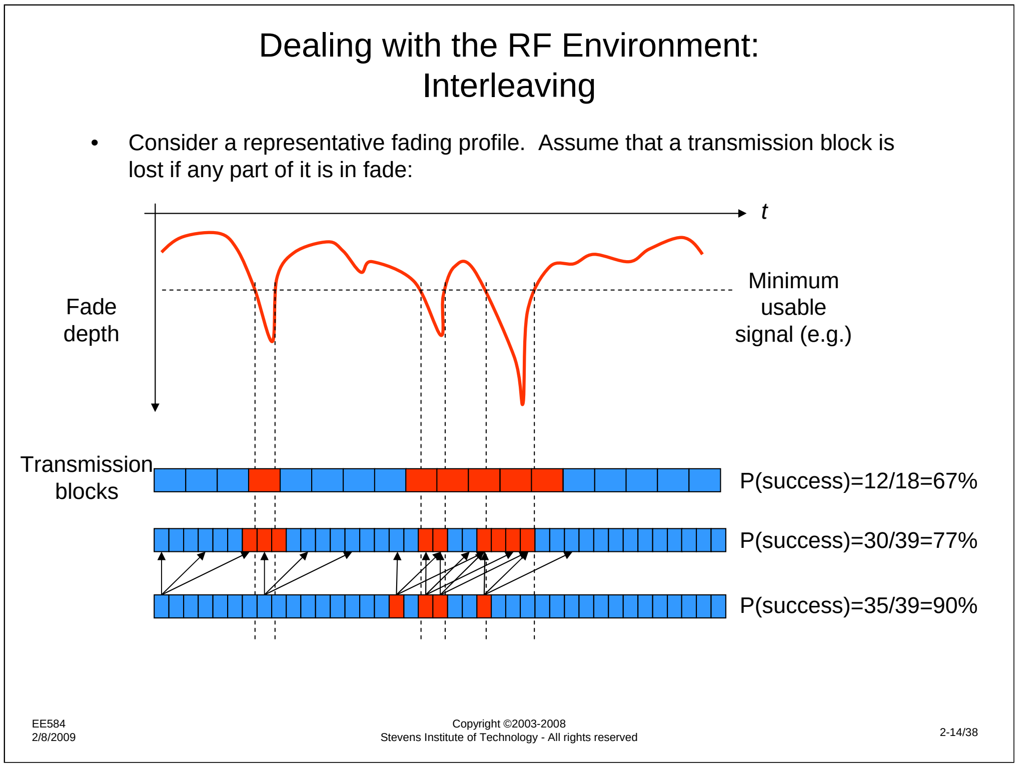
# Dealing with the RF Environment: Understand the channel characteristics

- Consider a representative fading profile. Assume that a transmission block is lost if any part of it is in fade:

EE584
2/8/2009

2-13/38

The simplest thing to do when faced with a fading channel is to insure that the system is matched to the environment. Here, by simply shortening the blocks to increase the probability that a block will make it through when the channel is “good” has increased the success rate by 10%.



## Dealing with the RF Environment: Interleaving

- Consider a representative fading profile. Assume that a transmission block is lost if any part of it is in fade:

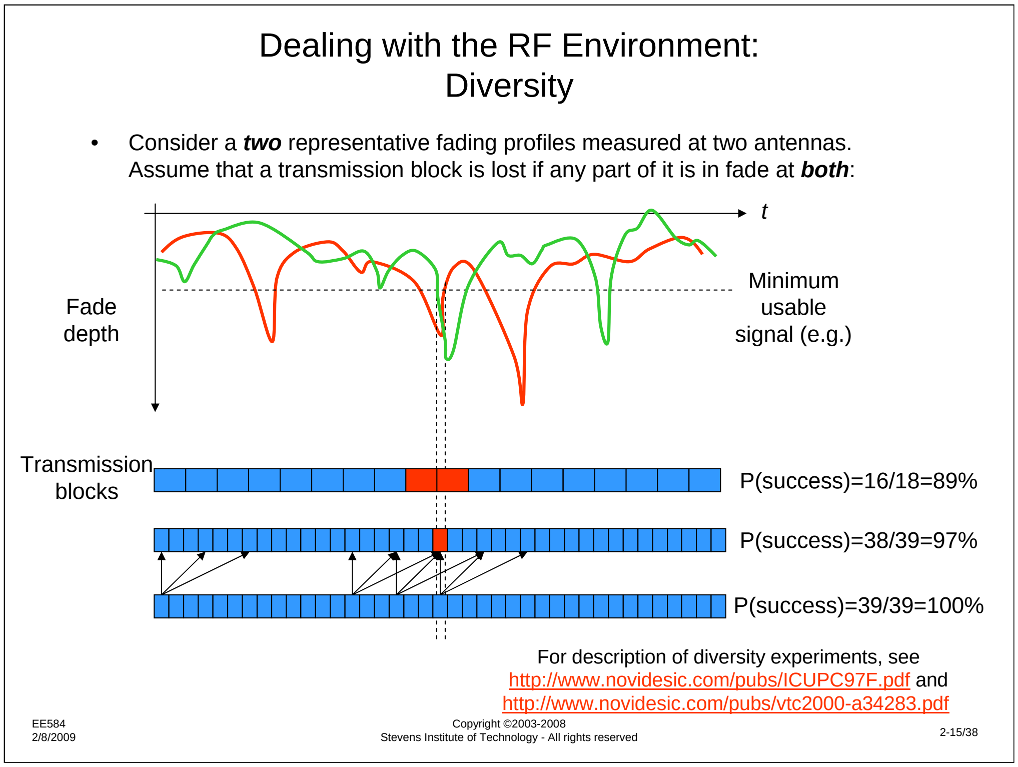
EE584
2/8/2009

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

2-14/38

Besides the fact that we can predict something about the channel fading, based on the frequency of operation and the vehicle speed, we know something else fundamental about fading – it is of short duration and constantly changing. If the probability of a 10 dB fade is 10%, two widely spaced independent samples of the channel only have a 1% chance of both being in a 10 dB fade. If we spread the transmission blocks around a bit, we can mitigate the effects of fading.

Here, I have illustrated a simple interleaver – each block is broken into three pieces, evenly spaced in time. We will assume that the transmission coding only breaks down if two out of the three pieces of the transmission are in blocks that would have been damaged. As you can see, this strategy, as simple as it is, works quite well, reducing the error rate from 23% to 10%.



## Dealing with the RF Environment: Diversity

- Consider a ***two*** representative fading profiles measured at two antennas. Assume that a transmission block is lost if any part of it is in fade at ***both***:

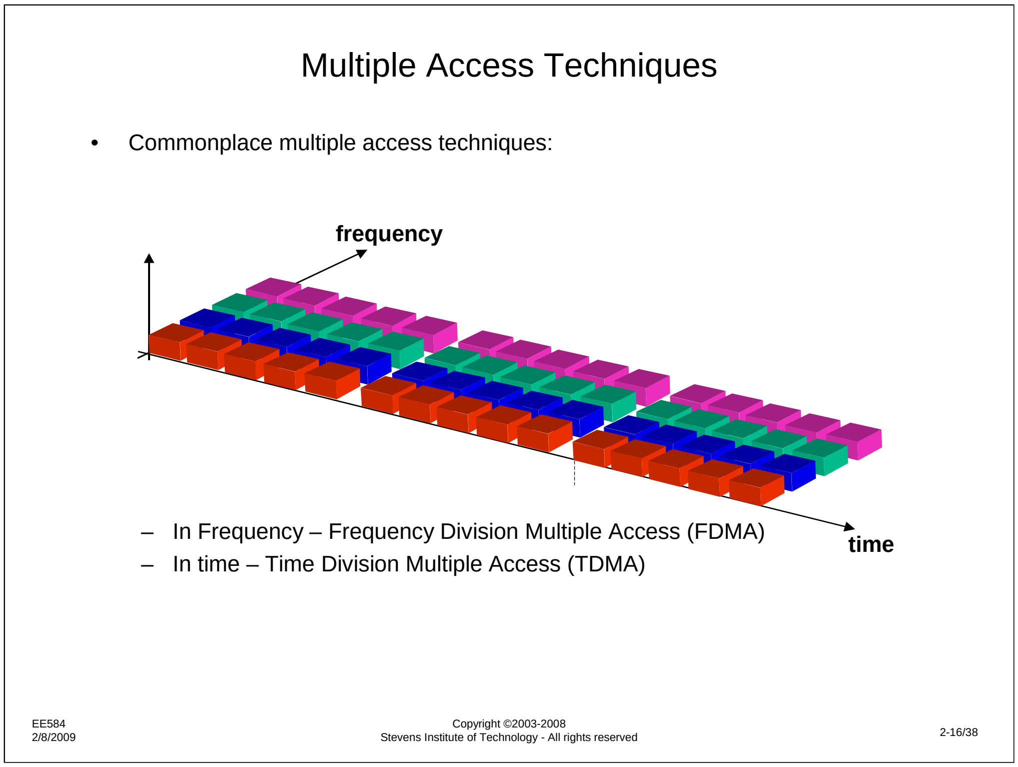
For description of diversity experiments, see http://www.novidesic.com/pubs/ICUPC97F.pdf and http://www.novidesic.com/pubs/vtc2000-a34283.pdf

Remember earlier, I pointed out that a deep fade is created by a unique set of events – nearly equal receive energy on two paths, plus a half-wavelength difference in path length. This has the effect that the fade is a very localized event in time and space. What happens if we sample the received signal one-half wavelength away? Perhaps we have moved in a direction to shorten one of the paths by one-half wavelength, while leaving other path length the same or changing it only slightly. This has the effect of changing the multipath environment drastically – perhaps from a deep fade to a situation where the two signal paths are reinforcing each other.

I have illustrated this by drawing two independent fading profiles. Just as before, we have a performance threshold that we must cross for the system to work properly. In this case, however, since there are two antennas available, we will select the signal on the stronger one (so-called selection diversity, the simplest and least effective means of diversity combining). Since it is unlikely that both antennas are in a deep fade at the same time, we can see the dramatic performance improvement in block error rate.

Antenna diversity is one of the most effective techniques to deal with the multipath environment.

This simple technique of picking the stronger signal can make a dramatic difference in system performance. However, once a system designer considers the potential to have more than one antenna on a transceiver, there are new sets of possibilities: it is possible to process the signals from two antennas in such a way to emphasize signals in one direction (where the desired signal is) and deemphasize signals in another direction (where the interferer is). These so-called “smart antenna systems” are the basis for ongoing research in wireless systems and dramatic performance gains.



## Multiple Access Techniques

- Commonplace multiple access techniques:

  - In Frequency – Frequency Division Multiple Access (FDMA)
  - In time – Time Division Multiple Access (TDMA)

EE584
2/8/2009

2-16/38

First Generation AMPS is an example of FDMA, one of the first multiple access techniques – separate users can simultaneously use the system because they are operating at distinct, separate frequencies. This channelization is the same technique used by broadcast radio and TV stations, each operating within their assigned channels.

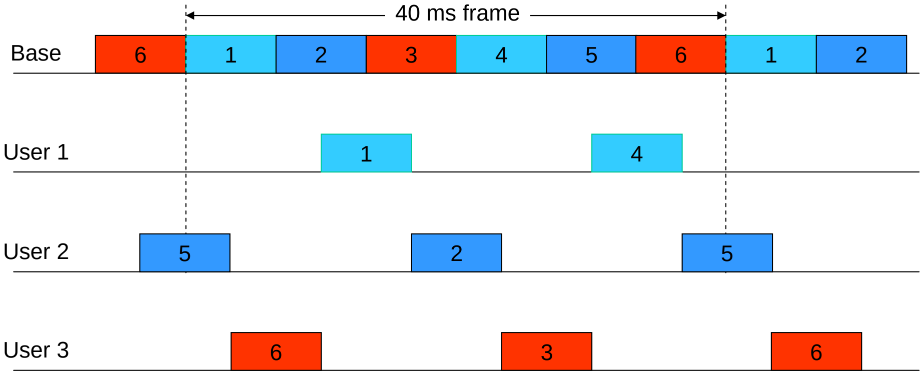
The RF medium can also be shared in ***time*** with TDMA. Users must transmit and receive within their assigned time periods. These time periods might be fixed or randomly assigned. Ethernet networks (802.3) use a random assignment TDMA system known as Carrier Sense Multiple Access with Collision Detection (CSMA-CD)

**Discussion topic**: what constraints might exist with the use of TDMA systems in an RF environment? Could CSMA-CD be used in a cellular environment?

The use of short range cells in a cellular system is an example of another multiple access technique – Space Division Multiple Access

## TDMA – 2nd Generation

- IS-54/IS-136:

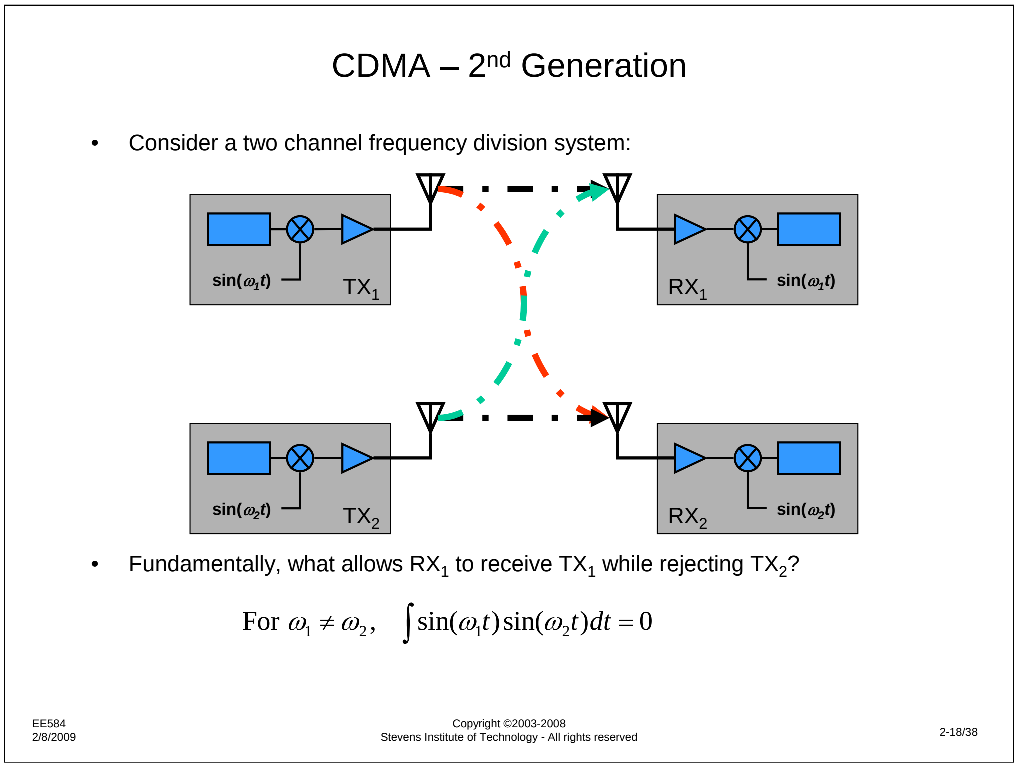


In North America, the TDMA cellular standard has been IS-54 and its refinement, IS-136. While the parameters are different in the GSM standard, used in many other countries and some 1800 MHz US PCS systems, the concepts are similar. I'll describe IS-136 here.

The base station transmits continuously on its assigned frequencies (the same frequencies that were used for AMPS at 800 MHz, as well as PCS frequencies at 1800 MHz) in the same 30 kHz bandwidth that AMPS uses. With the IS-136 system designed this way, the cellular operator can mix TDMA channels with AMPS channels, making the migration from 1st generation to 2nd generation easier. The transmission time is broken into 40 ms frames, with each frame divided into 6 slots. Conceivably, 6 simultaneous voice users could use the individual slots. Practically, for better speech quality, users are assigned two slots per frame.

User to base transmissions are short bursts so that individual users do not interfere with each other. In addition, the uplink transmission is timed to occur with an offset from the corresponding downlink. In this way, the mobile receiver is not operating at the same time the mobile transmitter is, simplifying the mobile transceiver design.

TDMA provides the potential for a significant power savings: the mobile TDMA receiver only needs to operate a fraction of the time – for IS-136, this is a 1/3rd duty cycle.



## CDMA – 2nd Generation

- Consider a two channel frequency division system:

- Fundamentally, what allows RX$_1$ to receive TX$_1$ while rejecting TX$_2$?

$$\text{For } \omega_1 \neq \omega_2, \quad \int \sin(\omega_1 t)\sin(\omega_2 t)dt = 0$$

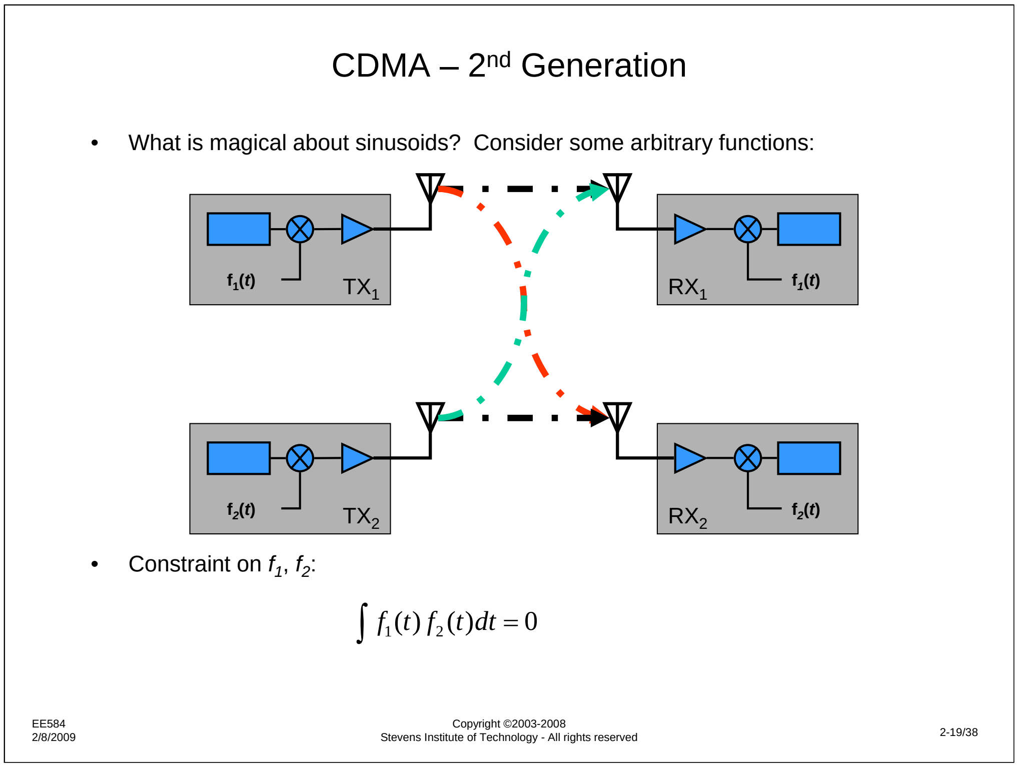
EE584
2/8/2009

2-18/38

There is another cellular multiple access technique that has direct implications in the design of secure systems. In fact, this Code Division Multiple Access (CDMA) technique actually has its roots in military systems that were designed to prevent signal detection and jamming, so-called Direct Sequence Spread Spectrum systems.

To understand how CDMA works, it is necessary to think about how it is possible to separate multiple signals all simultaneously transmitting in the same area.

In simplistic terms (only true for an unmodulated carrier), the orthogonality of sinusoids at different frequencies is what allows multiple users at different frequencies to share the same spectrum. Two sinusoids are orthogonal if the integral equation above applies. This equation is equivalent to an inner product or distance measure in a multidimensional vector space, so what the equation is really saying is that the sinusoids are orthogonal if the project of one sinusoid onto the other is zero, as the x and y axes in a cartesian plane are orthogonal.



## CDMA – 2$^{nd}$ Generation

- What is magical about sinusoids?  Consider some arbitrary functions:

$f_1(t)$
$TX_1$
$RX_1$
$f_1(t)$
$f_2(t)$
$TX_2$
$RX_2$
$f_2(t)$

- Constraint on $f_1$, $f_2$:

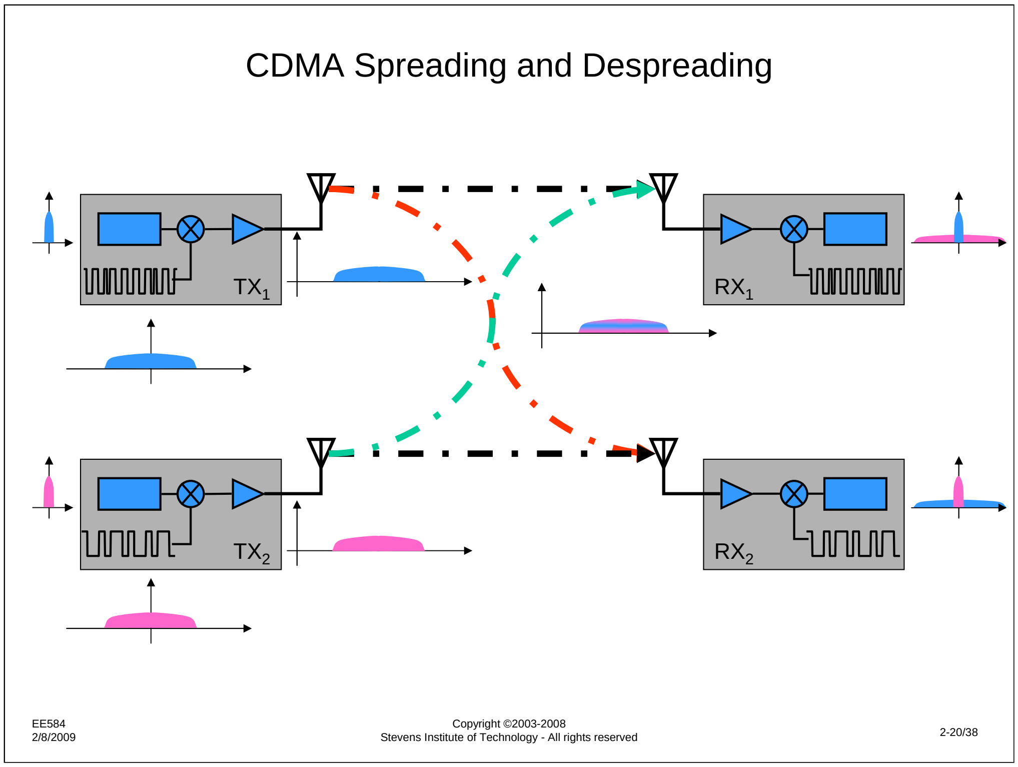
$$\int f_1(t) f_2(t) dt = 0$$

EE584
2/8/2009

2-19/38

If we had two or more arbitrary functions which were orthogonal to each other, we could "modulate" them with baseband information as we do for sinusoids and use them to transmit information over the RF channel.  Orthogonality of the functions would assure their separability at the receiver.  Other constraints on the functions that would be nice to have would include the ability to generate them easily, the existence of a large set of functions, and some uniformity between the different functions that would treat all users fairly, independent of which function they chose.

In CDMA, the functions used are sets of binary strings known as Walsh Codes.  They obey all of the constraints above.  The individual Walsh Codes, in combination with other pseudo-random sequences, generate a noise-like signal that spreads the transmitter energy over a wide band of frequencies.  To all but the user with the proper Walsh Code, pseudo-random sequence, and the precise state of the sequence, the transmitted signal looks like background noise.



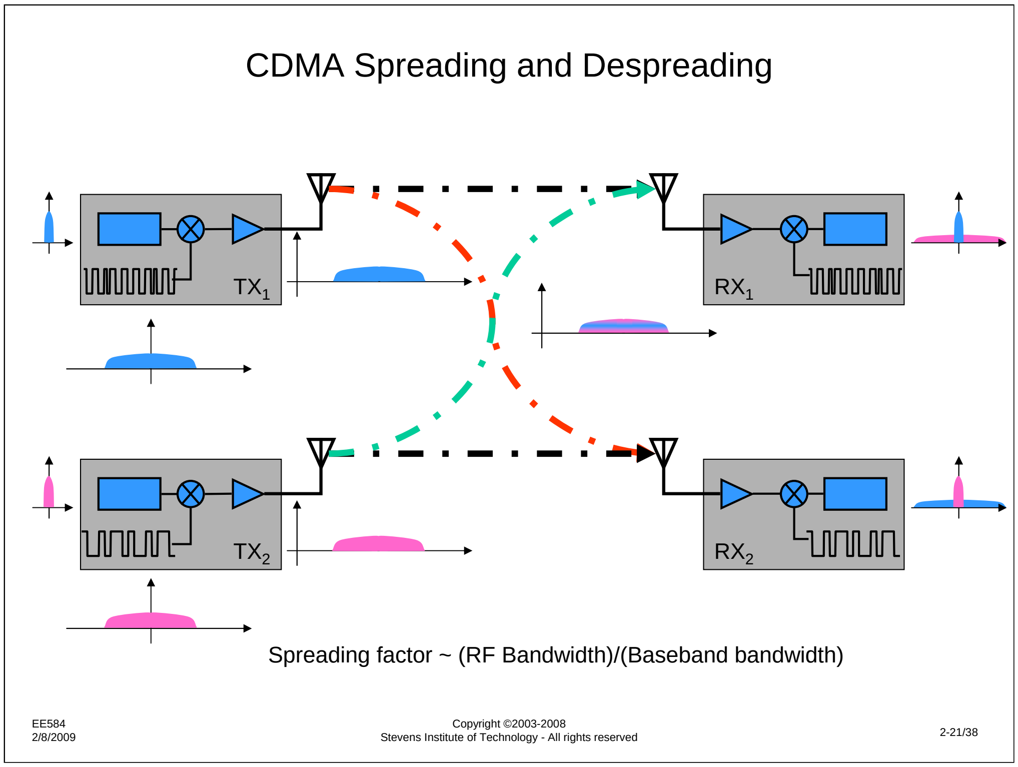
## CDMA Spreading and Despreading

EE584
2/8/2009

2-20/38

Assume that two users are operating in the same frequency band and spatial region with CDMA. Their baseband signals are shown at the left, relatively narrowband signals, perhaps speech. The spreading codes used by the two users are different and have a broadband spectrum, over 1 MHz wide for IS-95 CDMA. When the spreading codes are mixed with the baseband signals and translated to RF, the radiated spectrum is essential that of the spreading sequence. To an observer who does not know the spreading code, all users are indistinguishable.

Over the air, and at the two receivers on the right, the two signals are intermixed with each other. Each receiver uses the proper spreading code to despread the received signal. This has the effect of returning the desired baseband signal to its original shape. Meanwhile, since the two spreading codes are not correlated with each other, despreading the second signal leaves it unchanged. The broadly spread signal remains as it was and appears like low level noise to the other receiver.



## CDMA Spreading and Despreading

Spreading factor ~ (RF Bandwidth)/(Baseband bandwidth)

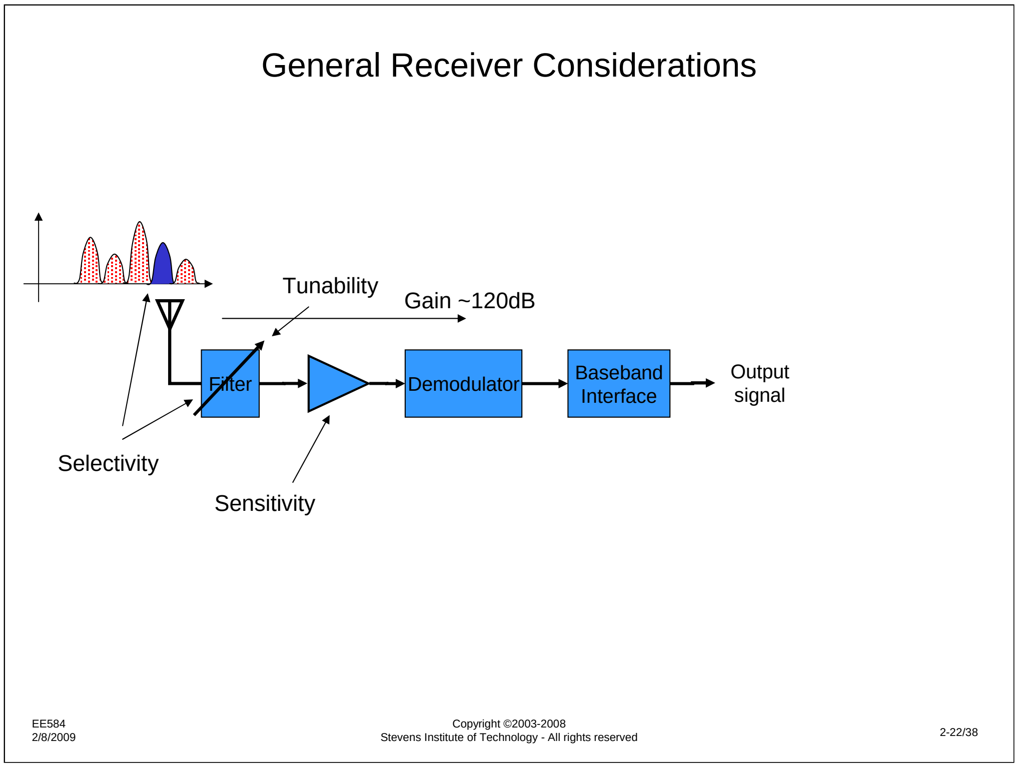
EE584
2/8/2009

2-21/38

Walsh codes are the current choice functions for CDMA, allowing multiple users to communicate on different Walsh codes in the same region. However, there is no secrecy in Walsh codes, since they are well known and easily replicated signals.

For military applications (EW – Electronic Warfare, ECM – Electronic Countermeasures, and ECCM – Electronic Counter-countermeasures), the codes uses are kept secret so that only an authorized user is capable of despreading a spread signal. This does not provide protection against the communications being monitored (**Discussion topic: Why?**), but it does make it difficult for the enemy to detect the presence of the signal or to jam it.

Consider this: a transmitter spreads a narrowband speech or data signal from some small baseband bandwidth to a wideband RF signal. The factor by which the signal bandwidth is increased is called the spreading factor. At the receiver, the same sequence is used to despread the wideband signal back to its baseband bandwidth. First imagine what happens to the jamming signal – it is completely unrelated to the spreading sequence. As a result, it does not benefit from the despreading. It remains the same wideband signal it was at RF. Meanwhile, the despread signal is a narrowband signal. The two can easily be separated with a low-pass filter, throwing away most of the energy of the jammer. This is the anti-jam (AJ) advantage of spread spectrum. Now consider what happens when the enemy tries to monitor the spread signal. The transmitter can use essentially the same energy for a spread spectrum signal as for a narrowband signal, since the despreading receiver will only be processing the baseband signal bandwidth. However, the interceptor does not know how to despread the signal. It is likely that the spread signal will be well below the noise floor at the interceptor. This is the low probability of intercept (LPI) advantage of spread spectrum.



## General Receiver Considerations

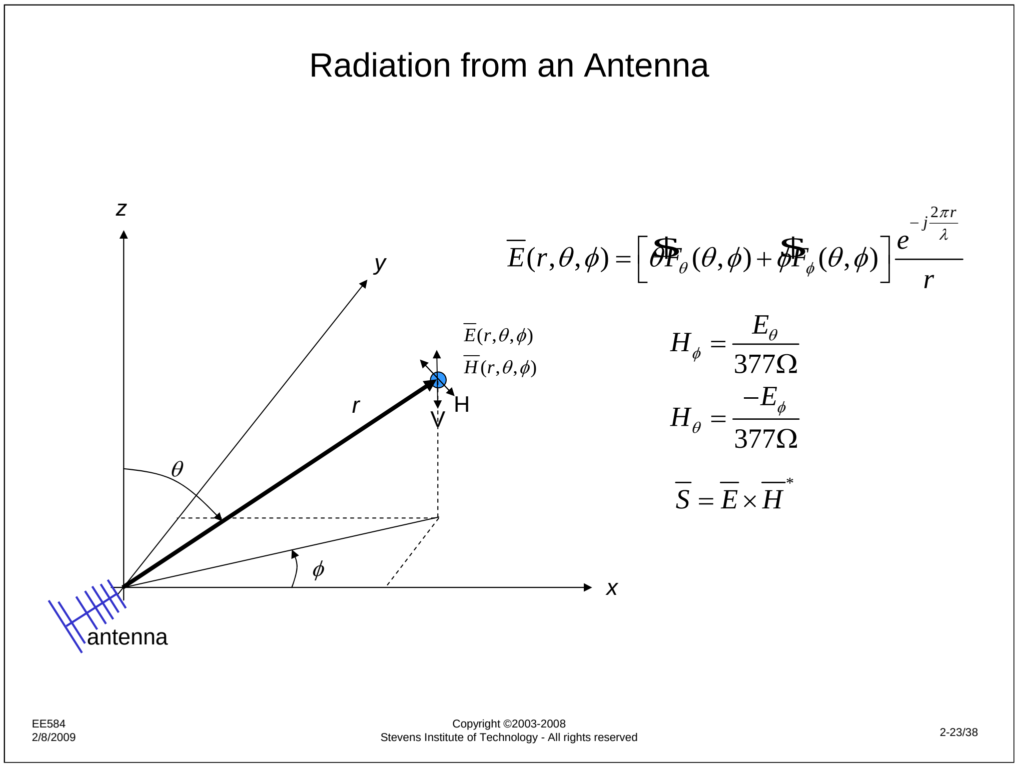
EE584
2/8/2009

2-22/38

Let’s put aside the high level system issues for now and examine the hardware that makes up wireless systems.  In particular, consider the receiver.

One hundred years ago, there were very few users of wireless communications.  Today, there are billions.  The crowed spectrum that has resulted creates one of the most important considerations for a receiver design – one desired signal has to be selected from among the hundreds to thousands of signals that are present at the antenna.  In addition, the receiver is often required to tune to one of many possible desired signals.  Finally, to make practical use of the spectrum, the receiver must be sensitive to very low level signals that are transmitted over a long distance or have been transmitted at a low power level.

While the diagram above depicts one of the simplest forms of a receiver, it is generally not practical for real communications applications.



## Radiation from an Antenna

$$\overline{E}(r,\theta,\phi)=\left[\hat{\theta}F_{\theta}(\theta,\phi)+\hat{\phi}F_{\phi}(\theta,\phi)\right]\frac{e^{-j\frac{2\pi r}{\lambda}}}{r}$$

$$H_{\phi}=\frac{E_{\theta}}{377\Omega}$$

$$H_{\theta}=\frac{-E_{\phi}}{377\Omega}$$

$$\overline{S}=\overline{E}\times\overline{H}^{*}$$

EE584
2/8/2009

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

2-23/38

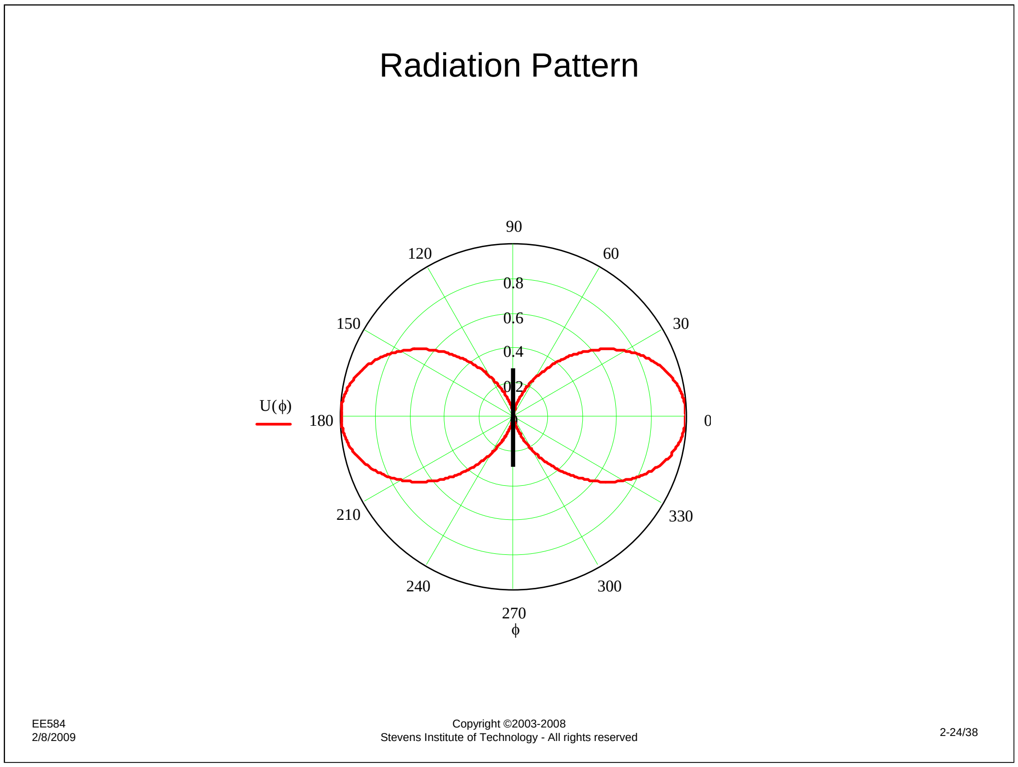
Next, consider how signals radiate from transmit antenna to receive antenna.

In describing the radiation from an antenna, we need to consider how things behave near the antenna differently than far from the antenna. We might be concerned about the near field if we are investigating the antenna radiation into a user's head, for example. When considering propagation over long distances, we are concerned with the far field, which is portrayed on this slide.

We use a polar coordinate system when describing antennas since the electric field drops off with the distance and is function of the azimuth (horizontal angle) and elevation (vertical angle). The equation at the top shows that the electric field has two distance relationships – first, the amplitude falls as the inverse of the distance and second, there is a periodic oscillation in the real and imaginary part of the electric field every wavelength. In addition, the electric field has so-called pattern components related to the polarization of the wave, either horizontal (in the phi-hat direction) or vertical (in the theta-hat direction), expressed by the F(.) functions.

As the electric field propagates radially outward from the source, there is a magnetic field at right angles to the electric field. The lower two equations express the horizontal and vertical components of the magnetic field, as they are related to the opposite components of the electric field. The 377 ohm constant is the impedance of free space. The bottom equation defines the Poynting vector, S, expressing the transfer of power as the vector cross product of the electric field with the complex conjugate of the magnetic field. Recognize that the units of the electric field are volts/meter, due to the fact that the electric field falls off as 1/r. Therefore, the magnetic field also falls off as 1/r and the power must fall off as 1/r^2.

This last point is important for defining communications range and has a very simple physical interpretation. Imagine two concentric spheres surrounding the origin, one R times the radius of the other. Assuming that no power is lost in the medium, all the power leaving the antenna passes through both spheres. The bigger sphere's surface area is R^2 times that of the smaller sphere –the power per unit area is 1/R^2 times less on the larger sphere. Thus, power per unit area falls as 1/r^2, as the Poynting vector suggests.



## Radiation Pattern

EE584
2/8/2009

2-24/38

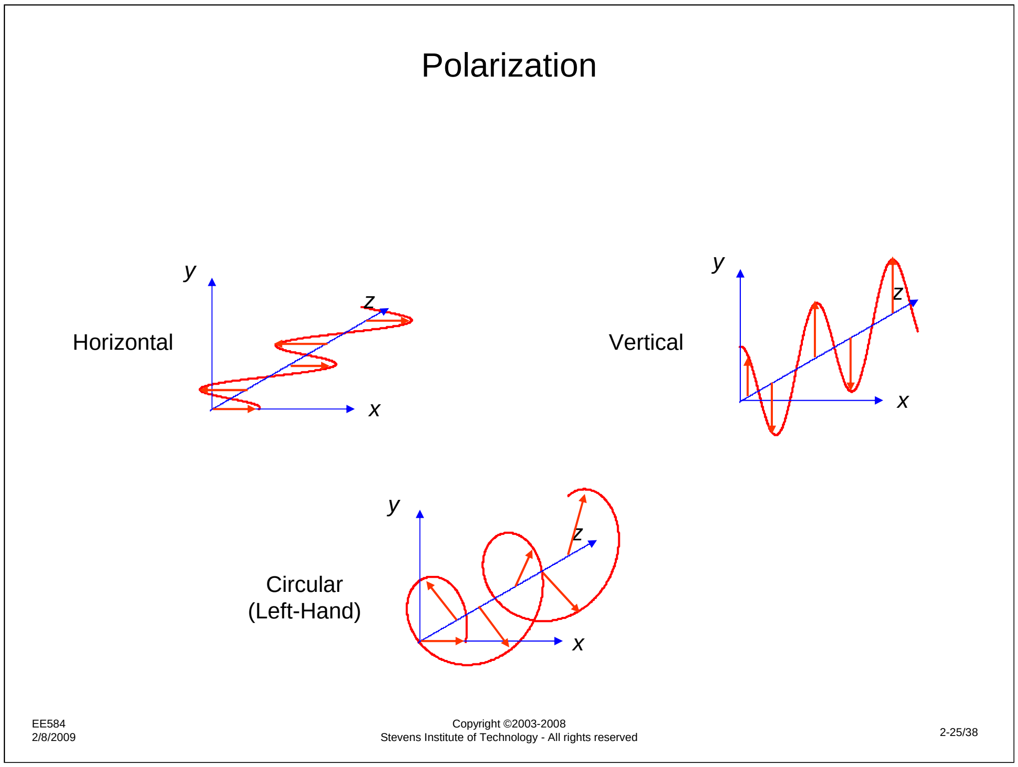
When designing an antenna for a communications system, we will be concerned about how the antenna radiates energy in different directions. By measuring in the field or calculating analytically, we can find the far field strength at a particular distance from the antenna. Depending on whether the antenna is horizontally or vertically polarized, we would study F(sub)phi or F(sub)theta, or, perhaps both. We would then plot the antenna pattern on a polar graph, as shown above.

The radiation pattern shown here is representative or what we might see for a half wave horizontally polarized antenna in free space. Imagine that the antenna is the black vertical line on the page and we are looking at it from above. The radiation off the ends of the antenna are minimal, so the field strength is minimal. The radiation pattern is strongest broadside to the antenna, but it varies as we change the azimuth angle.

If we intended to use this antenna to communicate, it would obviously be optimum if this antenna were oriented broadside to the intended station. On the other hand, if there were an interferer to contend with, it might be best to orient the antenna so the interferer were at the end of the antenna, where the response is weakest.

From a security perspective, the susceptibility of the system to monitoring or jamming will obviously be greatest at angles where U(phi) is greatest and least where U(phi) is least. While this pattern illustrates the simplest antenna, a dipole, other antenna designs will have more complex radiation patterns.

By antenna orientation or combination of multiple antennas, this pattern can be controlled mechanically or electrically.



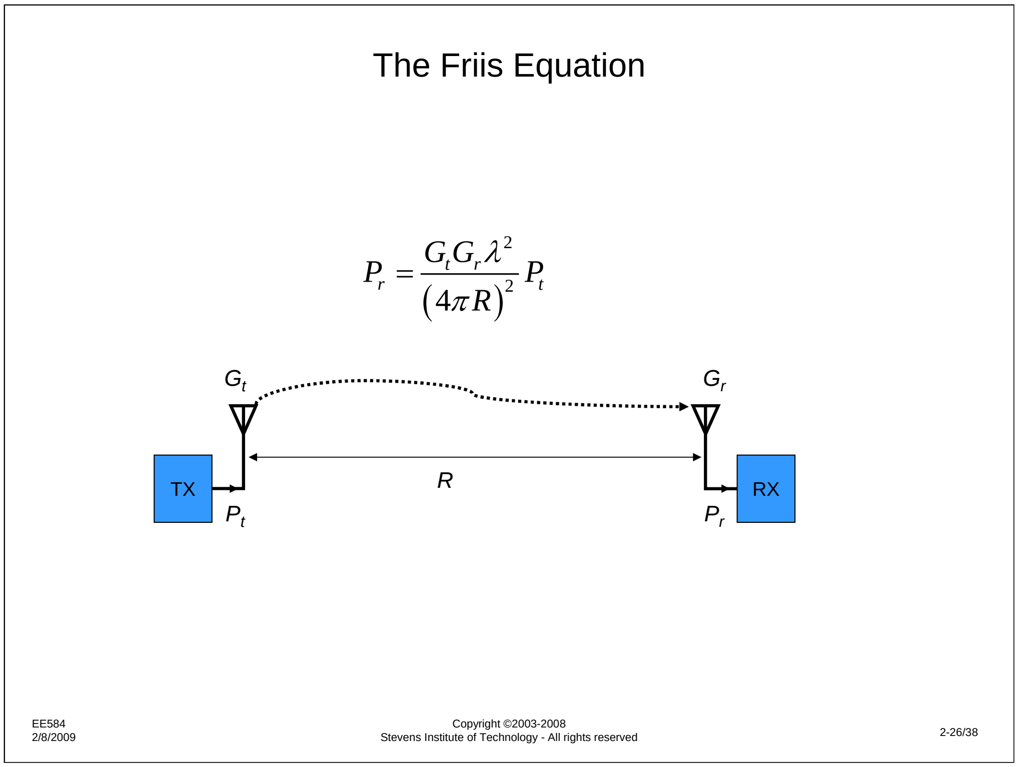
## Polarization

EE584
2/8/2009

2-25/38

The electromagnetic field radiated from an antenna is expressed in a polar coordinate system for convenience in analyzing parameters that are related to the radial distance from the antenna or are functions of the angle with respect to the antenna orientation.  For a minute, consider that we are in the far field of an antenna, looking at the electric field as it propagates along the z axis.  We can define the polarization of the electric field in terms of how the field changes as it travels in the z direction.  For antennas with predominately linear elements, the polarization will often align with the elements, so a vertical whip antenna has an electric field that changes in a vertical direction as it propagates, as shown in the upper right diagram.  Likewise, a horizontally polarized wave's electric field oscillates in the horizontal plane.  Horizontally and vertically polarized signals are special cases of "linearly" polarized waves, meaning the electric field varies in a plane.  In-phase x and y field components cause linear polarization typically used for most terrestrial systems.  For terrestrial systems that do not have line of sight conditions, scattering may change the signal's linear polarization, but not the phase of the components.

The x and y components may not be in phase – often they are 90 degrees out of phase. Remember the e^(jx) component of the electric field.  With a 90 degree phase difference, one will be real while the other is imaginary, and as one's imaginary part grows, the other's imaginary part decays.  Circular polarization describes the case where x and y are equal in magnitude and 90 degrees out of phase, shown in the bottom graph. To maximize the received energy the receiver and transmitter must use the same polarization for a line-of-sight system. In satellite communications systems, it is difficult to predict what the satellite antenna orientation will be as the satellite orbits so these systems typically use circular polarization. Right-hand (clockwise) or left-hand (counter-clockwise) circular polarization depend on which axis (x or y) leads or lags the other.



## The Friis Equation

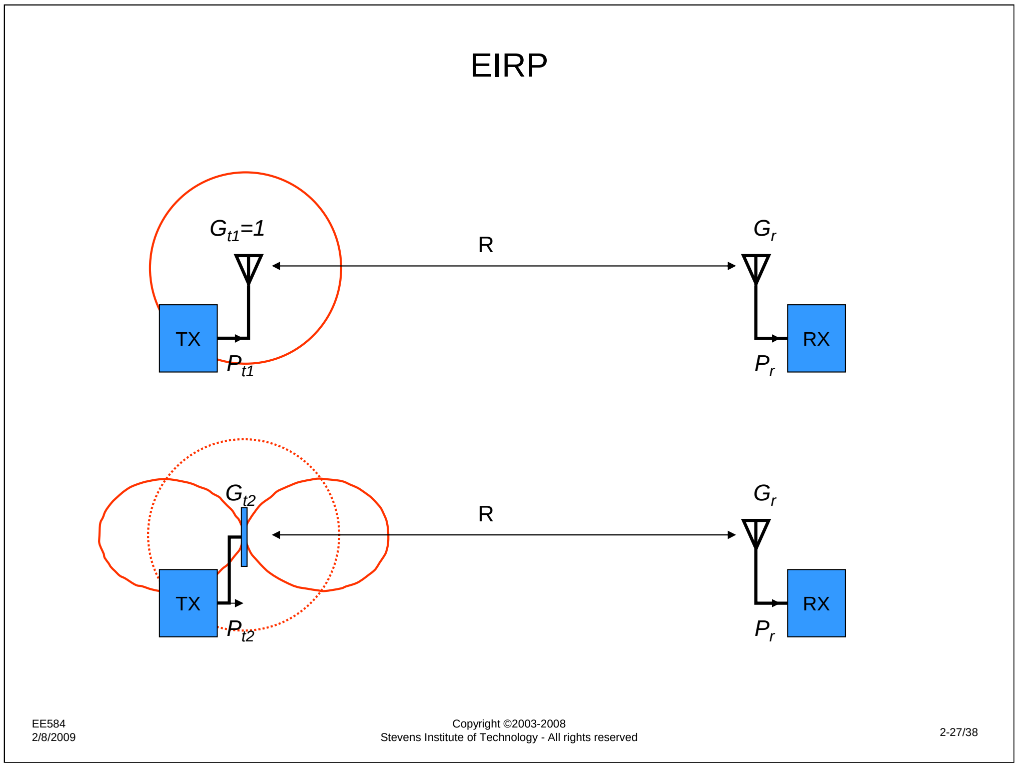
$$P_r = \frac{G_t G_r \lambda^2}{(4\pi R)^2} P_t$$

Now, putting the pieces together:

Does a usable communication path exist between point A and B? If A is the transmitter and B is the intended receiver, this condition is desirable. If B is the interceptor or A is a jammer, we would like to make sure the condition is not the case.

The Friis equation is central to understanding a wireless communications link on end-to-end basis. It predicts the received antenna power over a free space link as a function of the transmit power, the distance and the gains of the transmit and receive antennas. It does not include issues like loss in transmission lines to and from the antennas, receiver noise, or fading, but should be used as a starting place in any wireless range calculation.

A well designed antenna does not turn transmit power into heat, but couples it into the environment. Likewise, it is a passive device, so it cannot create energy. Where does the gain come from? If the antenna is NOT radiating power in one direction, the power must radiated elsewhere, so antenna gain is really a measure of the directivity of the antenna. Likewise, we can think of the gain of a receiver antenna in terms of its increased sensitivity in one direction versus another. These are the Gr and Gt terms. As shown in the first slide on propagation, the RF energy in free space falls off as 1/R^2. Received power is also proportional to the square of the wavelength, and is directly dependent on the transmitted power, so we can estimate the link performance, at least in free space with the Friis equation.

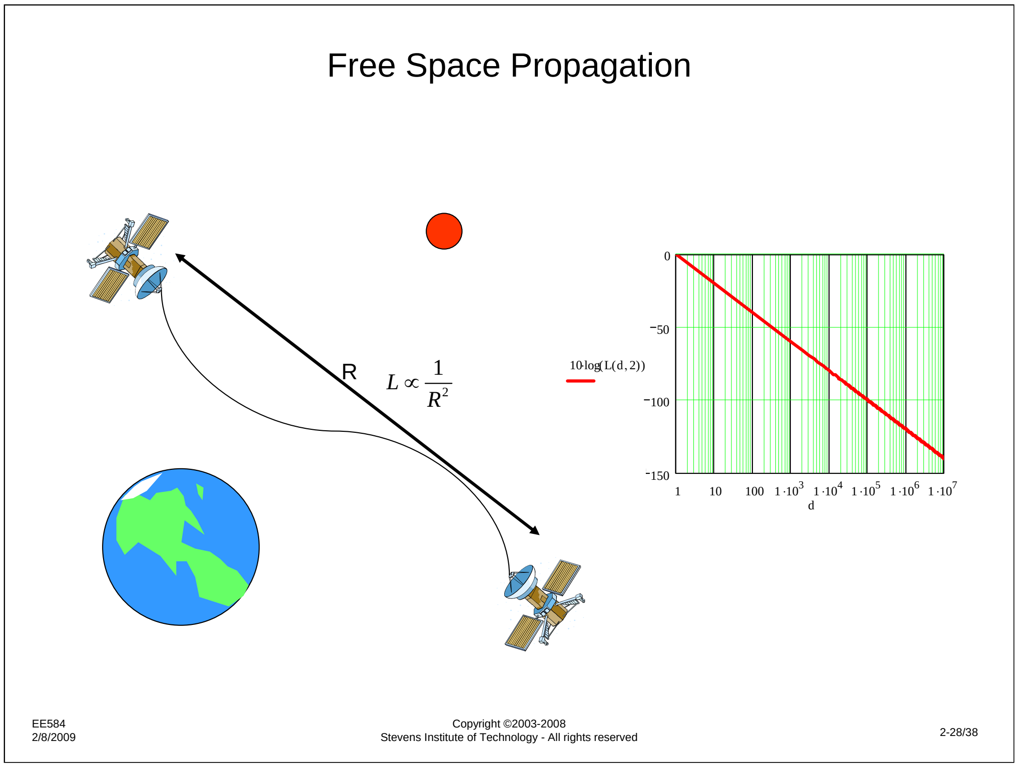


## EIRP

Consider two wireless links as shown above. The path length and the receiver gains for both are the same, so we can ignore them for comparison purposes. Let’s assume that the received power is the same for both links, as well.

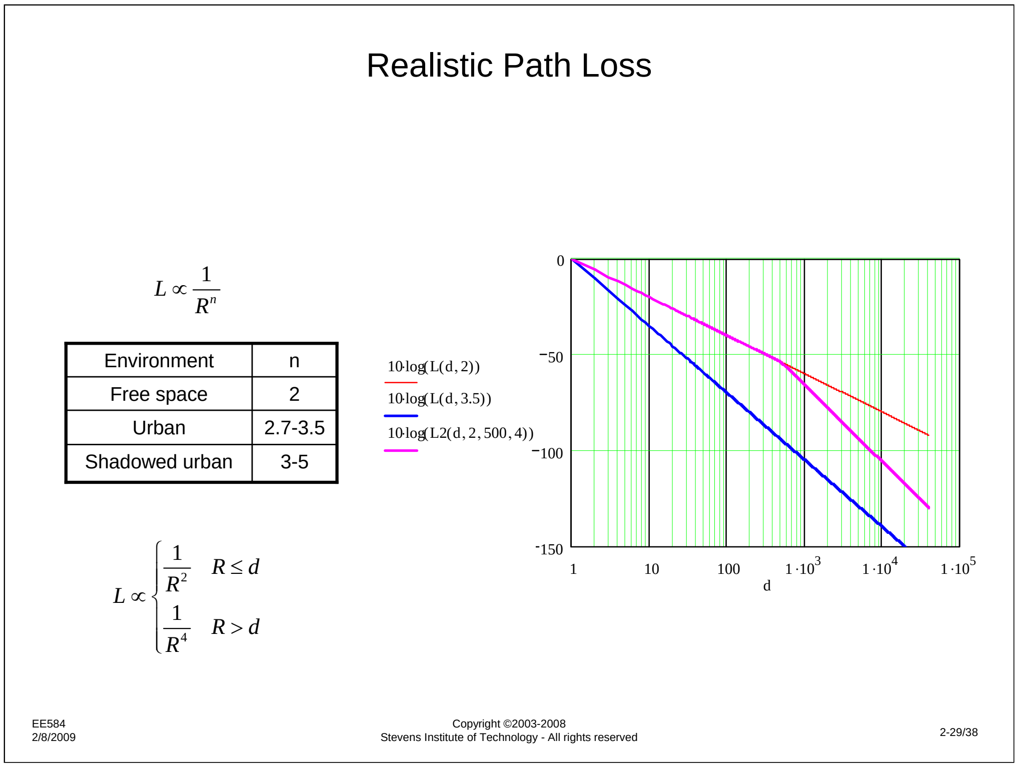
The upper link is transmitting with an ideal isotropic antenna, so the antenna gain is 1, while the bottom link has an antenna with some directivity, but also, potentially some inefficiency. When we compute the received power on the top link, we include the transmit power. Since the lower link is producing the same receiver power, it is behaving like an isotropic radiator with a higher transmit power. Thus, the term Effective Isotropic Radiated Power (EIRP) is a normalized measure that combines the transmitter power and antenna gain, while expressing this independently of any receiving conditions or path.

Since transmit power and antenna gain can always be traded against each other, frequently transmitter radiated power is specified in terms of EIRP. Another term that is frequently used is ERP – Effective Radiated Power. ERP uses a dipole antenna as a reference, the same as EIRP uses an isotropic radiator. The difference is that one could actually construct a reference dipole, while an isotropic radiator is a theoretical device. The gain of a dipole is 2.16 dBi, so ERP power levels are 2.16 dB above EIRP levels.



## Free Space Propagation

From the Friis equation, we can see that path loss is proportional to the inverse square of the distance. Strictly speaking, this relationship is only for signals in free space, where there is nothing nearby to reflect, refract, or shadow the signal. The satellite-to-satellite link at the left illustrates this situation. The inverse square approximation is reasonable for short paths (but not too short) or for paths where there are no objects near the direct path. For the most part, the free space path loss is a lower bound on the path loss - in a realistic environment, the path loss will generally be more.



# Realistic Path Loss

$$L \propto \frac{1}{R^n}$$

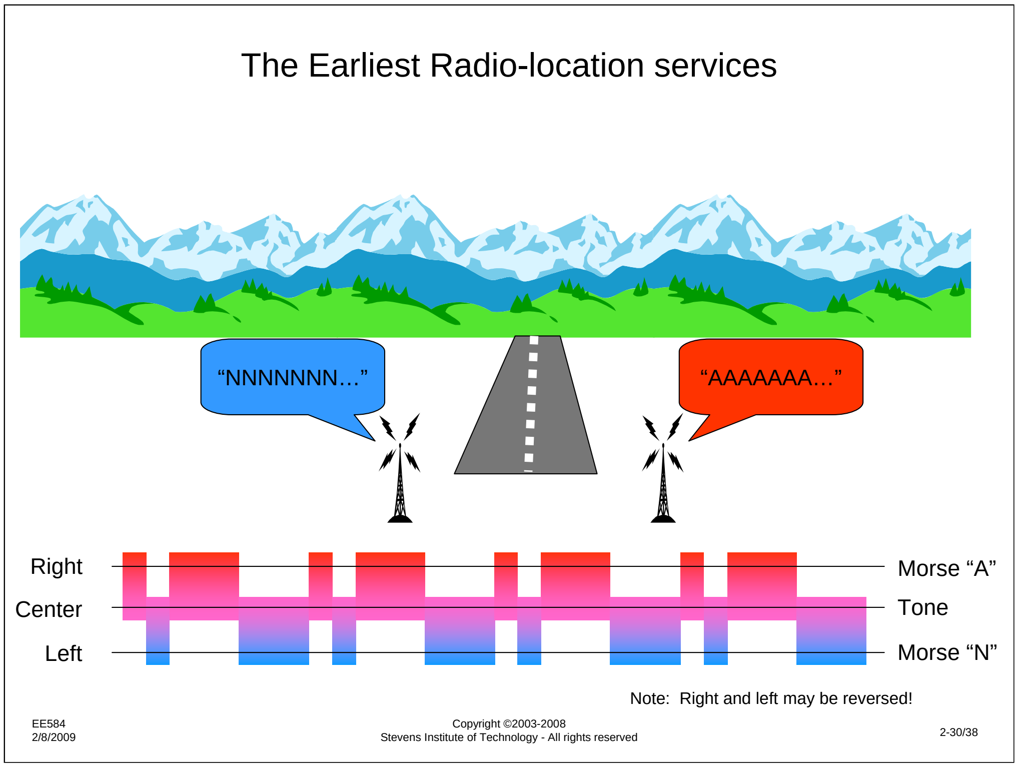
| Environment | n |
|---|---|
| Free space | 2 |
| Urban | 2.7-3.5 |
| Shadowed urban | 3-5 |

$$L \propto \begin{cases} \frac{1}{R^2} & R \le d \\ \frac{1}{R^4} & R > d \end{cases}$$

How can we develop a better model for path loss that allow us to use something as convenient as the Friis equation, but still produce something that has some meaning? One model changes the exponent of the path length. Instead of computing a loss based on R^2, a larger exponent causes the signal strength to fall off more quickly. As shown in the table at the left, exponents of 2.7 to 3.5 model an urban environment and perhaps 3-5 for an urban environment with a lot of shadowing (e.g., large buildings). Actually, as Pozar mentions, for indoor line-of-sight environments, the path loss exponent could be ***less than*** 2. How can this be? Free space is supposed to be the best case? Remember that free space assumes that the signal power is dropping off as the sphere over which the signal is spreading gets bigger. With an indoor LOS environment, the metal walls of the building can act like waveguides, guiding the signal down a straight hall without allowing the power to be distributed over a growing sphere.

Realistically, with furniture and walls indoors, with objects in the outdoor environment, the path loss exponent will be greater than 2 for most typical cases. But rather than modeling the environment with a fixed path loss exponent, several propagation researchers have suggested a model with two path loss exponents and a breakpoint. For short paths, the path loss exponent is 2 or something close. When the path gets beyond a certain distance, the path loss exponent gets bigger, due to the likelihood that there is more clutter in a long path than a short one.

In the graph at the right, there are 3 plots of path loss in dB as a function of distance. The red line represents free space path loss. The blue line represents an exponent of 3.5, while the magenta line represents nverse square up to a d=500, then inverse 4th power. One could dream up models with multiple breakpoints and several path loss exponents. Any path loss model must be consistent with the real world and convenient to use in simulation or analysis. In the end, models must be validated with real world measurements.



## The Earliest Radio-location services

Note: Right and left may be reversed!

EE584
2/8/2009

2-30/38

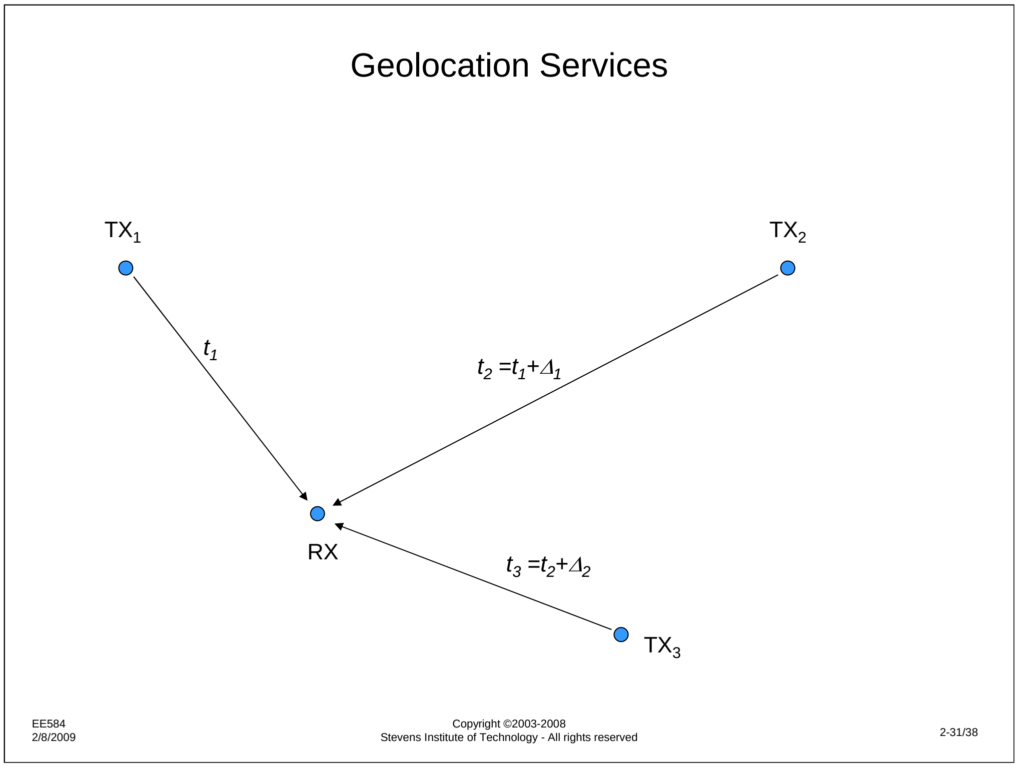
Now let's turn to discussion of some of the applications of wireless communications to set the stage for discussions of the security issues. First, let's examine a simple radio location service, the aircraft landing service that has been used for several years.

[Note: It has been many, many years since I took the exam for my 1st Class Radiotelephone operators license, and I couldn't find definitive references on this, so my explanation of right and left may be reversed]

The Morse code symbol for A is dot-dash, while the Morse code symbol for N is dash-dot. With the proper timing and spacing between dots and dashes, the two symbols fill in the blank periods of the other.

The simplest aircraft radiolocation system merely transmits an A on one side of the runway and an N on the other. If a plane is too far to the right or left, the pilot will hear the A-A-A message or the N-N-N message. By steering the plane in the proper direction, when the plane is inline with the runway, a continuous tone will be heard. Thus, even if the pilot is too far away to see the runway or is flying in clouds or fog, it is possible to get properly oriented.

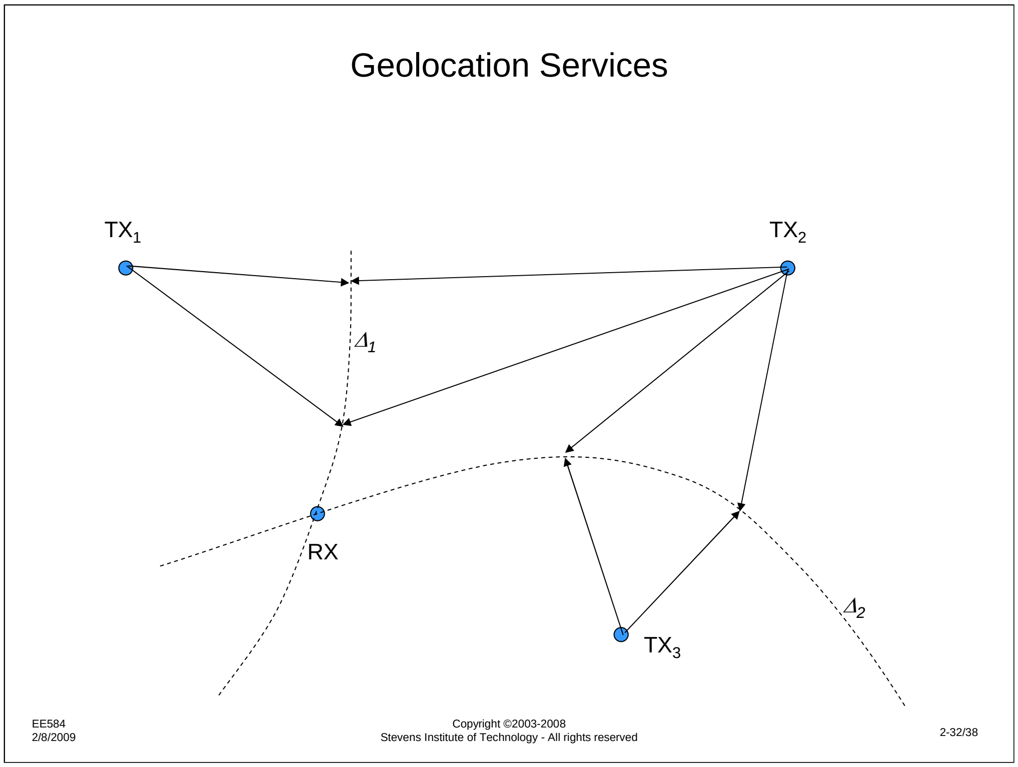
What might the security considerations of such a system be? If a jamming message is sent or if one or both of the transmitters are disabled, the pilot will be denied use of a system needed to navigate safely to the airport.



## Geolocation Services

Let's consider a more sophisticated geolocation service. Imagine that there are three base stations at known locations, transmitter 1, 2 and 3. Now consider that there is a receiver near these three transmitters, capable of determining the relative time delays of signals received from each of the transmitters. It is not necessary for the receiver to measure the individual path delays, it is sufficient to know that t2 differs from t1 by delta1 and t3 differs from t2 by delta2.

How can we use this information to determine the position of the receiver? First realize that the propagation of electromagnetic signals is a constant in air. The speed of propagation of wireless signal is the same as the speed of light (3 x 10^8 meters/second). As a rule of thumb, this is 1 foot per nanosecond.



## Geolocation Services

EE584
2/8/2009

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

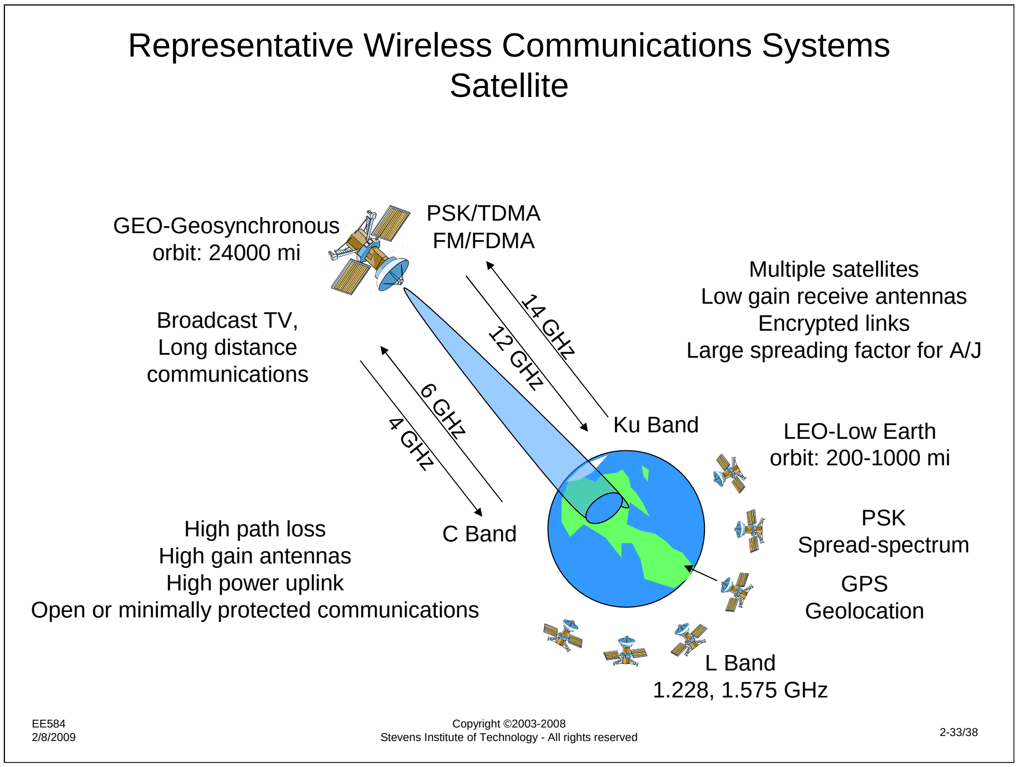
2-32/38

Knowing the relative path delays, we can draw the locus of points that have path length differences of delta1 between transmitter 1 and 2. It turns out that this locus of points is a hyperbola that lies between the two transmitters. Similarly, we can draw the locus of points for delta2, which is a hyperbola between transmitter 2 and 3. Since we are doing 2 dimensional navigation here, we only need three transmitters to uniquely find the position of the receiver at the intersection of the two hyperbolas.

If we want to do 3 dimensional navigation, we need four transmitters. Here, the loci for any given pair of transmitters are hyperbolic surfaces, but the 3 resulting surfaces still intersect in a point, where the receiver is located.

The Global Positioning Satellite (GPS) system uses orbiting satellites to provide accurate 3 dimensional navigation. You might question how the receiver is able to measure time differences. Partially for security reasons but also for ease of implementation, GPS uses a spread spectrum-like code to transmit information from the satellite. By noting how it must adjust the pseudo-noise (PN) sequence to synchronize to each of the transmitters, the receiver can measure time differences to within a few tens of nanoseconds, providing position accuracy to within tens of feet.

The security issues in this system are multidimensional – how do you use the system to provide the intended user high accuracy navigation while denying the enemy the ability to use the system effectively? How do you prevent the enemy from jamming the system, depriving you of accurate navigation?



## Representative Wireless Communications Systems Satellite

GEO-Geosynchronous
orbit: 24000 mi

PSK/TDMA
FM/FDMA

Broadcast TV,
Long distance
communications

14 GHz

12 GHz

6 GHz

4 GHz

Multiple satellites
Low gain receive antennas
Encrypted links
Large spreading factor for A/J

Ku Band

LEO-Low Earth
orbit: 200-1000 mi

High path loss
High gain antennas
High power uplink
Open or minimally protected communications

C Band

PSK
Spread-spectrum

GPS
Geolocation

L Band
1.228, 1.575 GHz

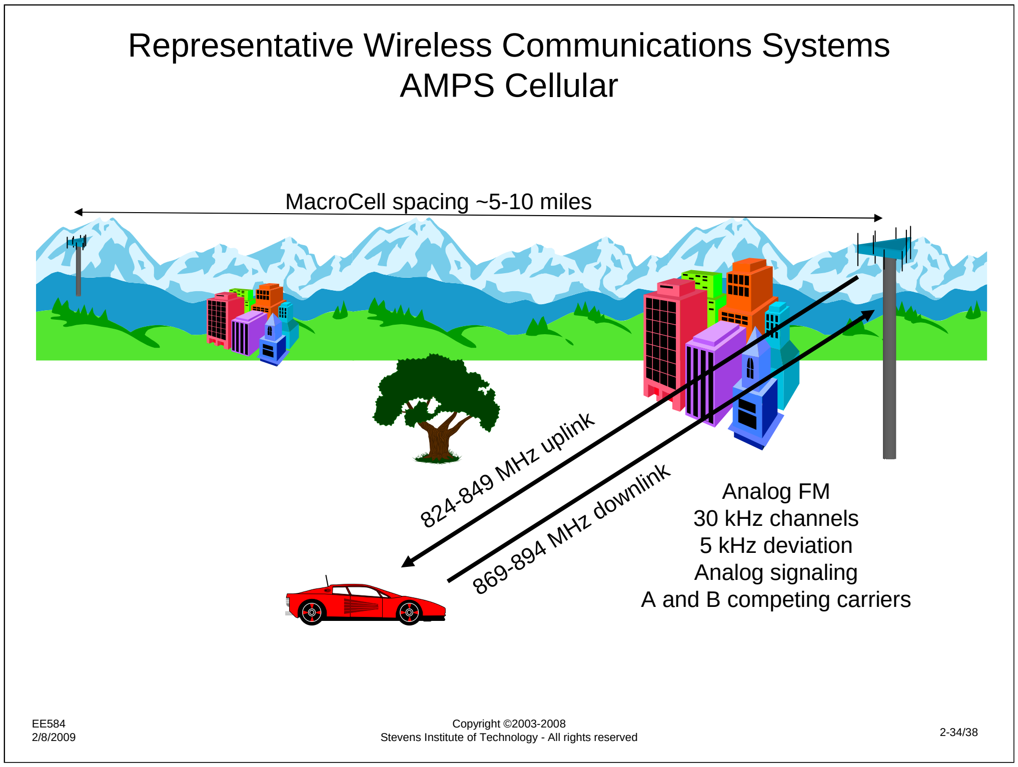
EE584
2/8/2009

2-33/38

While we are on the topic of space-based communications, let’s examine some wireless satellite communications systems.

I have already mentioned GPS, which uses frequencies around 1200 and 1600 MHz.  There are so-called Low Earth Orbit (LEO) systems that orbit a few hundred miles above the Earth, with orbital times that are measured in minutes or hours.  There are also Geosynchronous and Geostationary Earth Orbit (GEO) systems that orbit at about 24000 miles. Geosynchronous satellites orbit every 24 hours, the rotational period of the earth, so they do not seem to move east or west as the Earth rotates below them at the same angular speed. However, they may move to the north and south during their orbit.  Geostationary satellites, on the other hand, are in an orbit that is aligned with the rotation of the Earth.  As a result, these satellites always appear to be directly above the same point on Earth, a fixed position east or west and directly above the Equator.

Of necessity, the greater distance from a GEO satellite to the Earth means that the signal will be attenuated as it travels over the 24000 path distance.  This requires high power transmitters and high gain antennas.  We will examine this type of wireless communications in much greater detail during the second half of this course.



## Representative Wireless Communications Systems
## AMPS Cellular

MacroCell spacing ~5-10 miles

824-849 MHz uplink

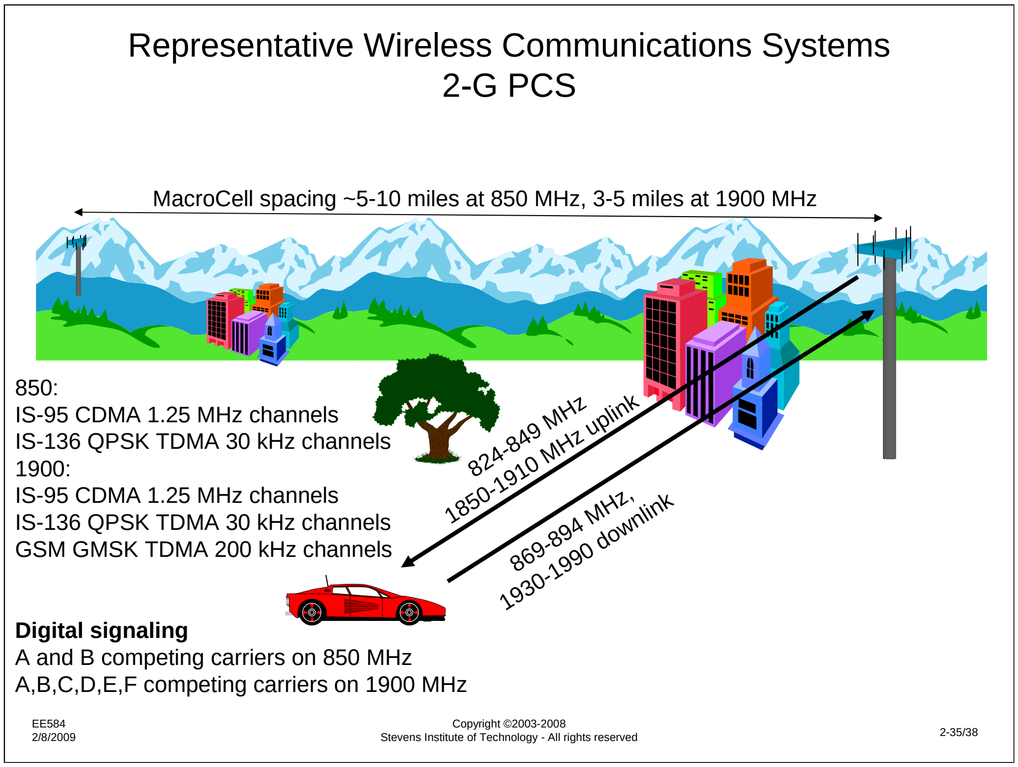
869-894 MHz downlink

Analog FM
30 kHz channels
5 kHz deviation
Analog signaling
A and B competing carriers

EE584
2/8/2009

2-34/38

Another wireless communications system that we will be examining in detail is the analog cellular system. While this is relatively old technology, being replaced by digital cellular for increased efficiency and features, it is still in widespread use and is likely to continue to be used for quite some time. Monitoring of analog cellular is relatively straightforward with simple receiving equipment, but the biggest issue has traditionally been theft of service. We will discuss why this is so and the implications of this issue later.



## Representative Wireless Communications Systems
## 2-G PCS

MacroCell spacing ~5-10 miles at 850 MHz, 3-5 miles at 1900 MHz

850:
IS-95 CDMA 1.25 MHz channels
IS-136 QPSK TDMA 30 kHz channels
1900:
IS-95 CDMA 1.25 MHz channels
IS-136 QPSK TDMA 30 kHz channels
GSM GMSK TDMA 200 kHz channels

824-849 MHz
1850-1910 MHz uplink

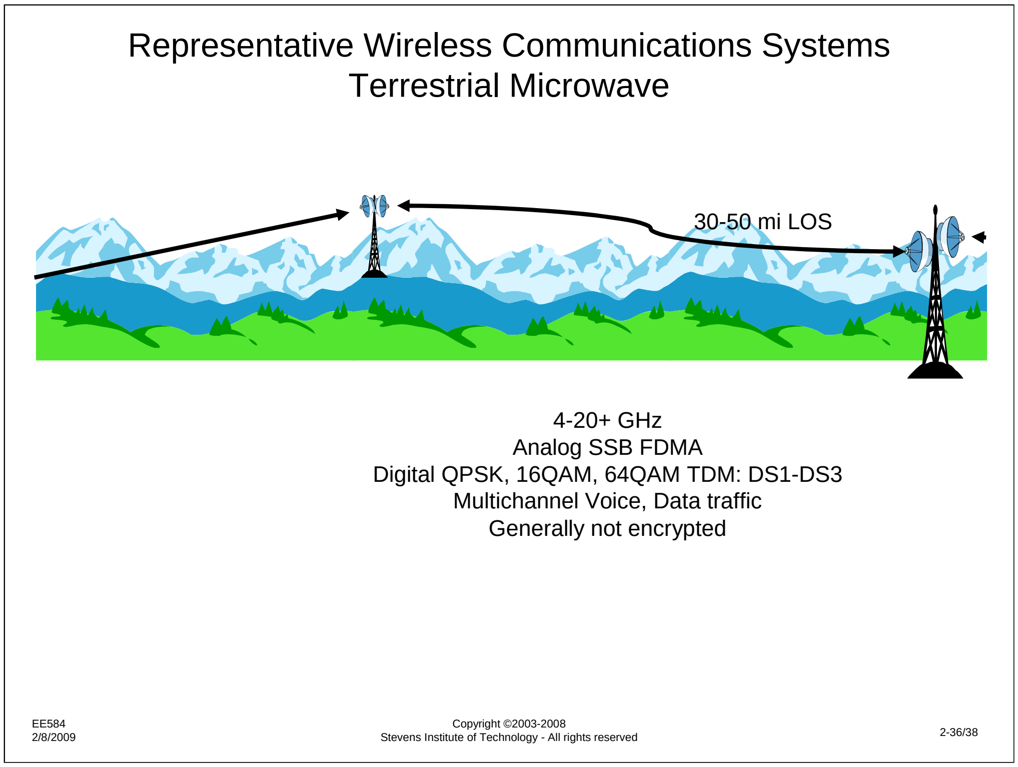
869-894 MHz,
1930-1990 downlink

**Digital signaling**
A and B competing carriers on 850 MHz
A,B,C,D,E,F competing carriers on 1900 MHz

EE584
2/8/2009

2-35/38

As mentioned, 1st generation analog AMPS has been replaced by 2nd generation digital cellular systems for economics (3 IS-136 users occupy the bandwidth of one analog AMPS user) and to provide enhanced features, such as caller ID and messaging services.  We will discuss security improvements that were introduced in digital cellular service, but this does not mean that there are no other security issues to discuss.



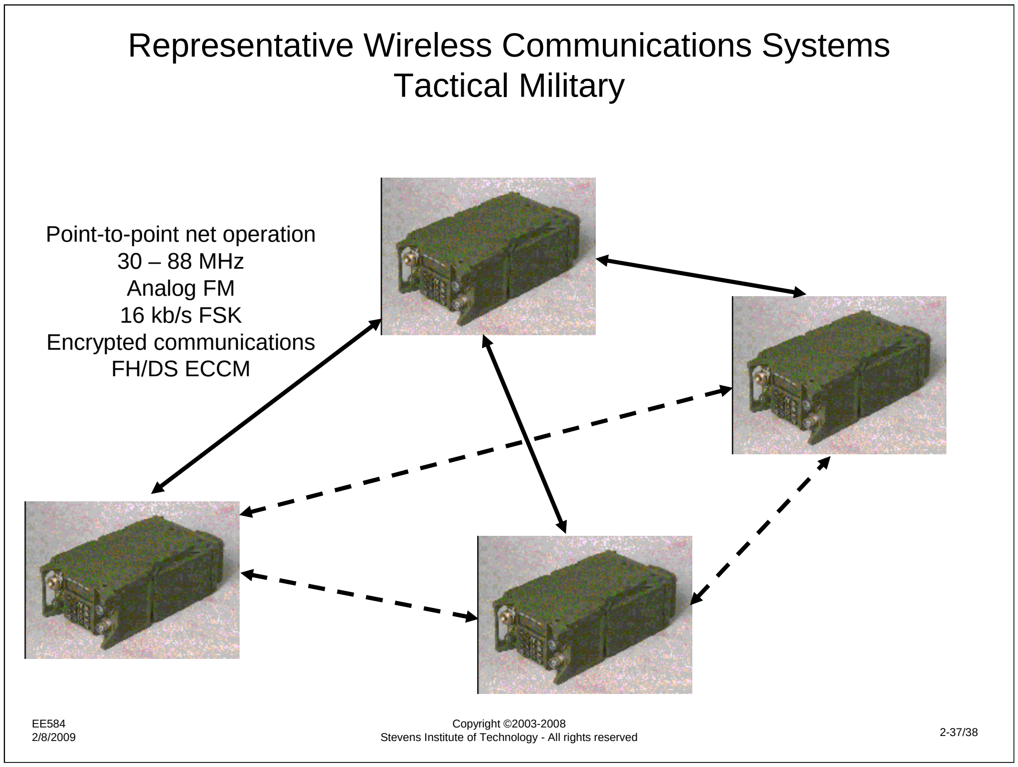
## Representative Wireless Communications Systems
## Terrestrial Microwave

4-20+ GHz
Analog SSB FDMA
Digital QPSK, 16QAM, 64QAM TDM: DS1-DS3
Multichannel Voice, Data traffic
Generally not encrypted

EE584
2/8/2009

2-36/38

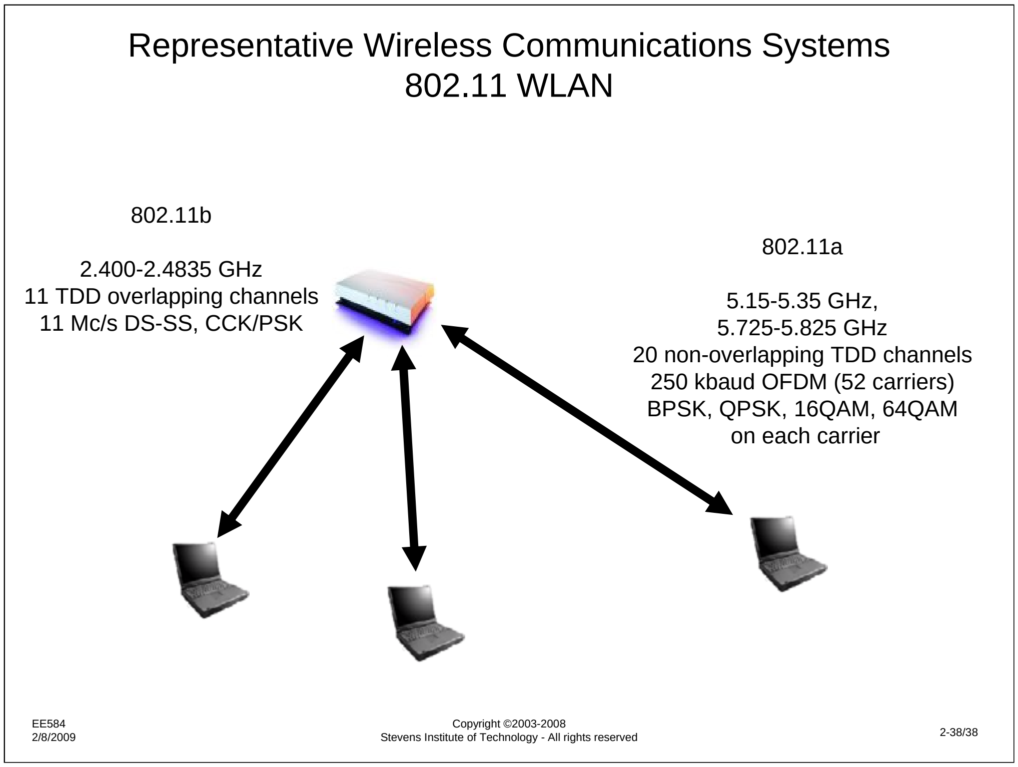
Before fiber communications, microwave radio was the mainstay of long distance voice telephone relay. Although fiber has replaced many microwave routes, there are still some systems in place today. I will be using a terrestrial microwave as the first case study in the class to illustrate how systems may be attacked in ways the designers never considered.



## Representative Wireless Communications Systems
## Tactical Military

Point-to-point net operation
30 – 88 MHz
Analog FM
16 kb/s FSK
Encrypted communications
FH/DS ECCM

I had to include military tactical radio systems for two reasons. First, I spent an important part of my career working on the SINCGARS (Single Channel Ground Airborne Radio System) system. But more importantly, second, the military has been concerned about the security of their wireless communications before most other users were even aware of wireless communications. There are many important lessons to be learned from how these military communications systems are designed and used that we can apply to many other systems. We will perform an assessment of the security of these systems to see that there can still be issues that are difficult to deal with.



## Representative Wireless Communications Systems
## 802.11 WLAN

802.11b

2.400-2.4835 GHz
11 TDD overlapping channels
11 Mc/s DS-SS, CCK/PSK

802.11a

5.15-5.35 GHz,
5.725-5.825 GHz
20 non-overlapping TDD channels
250 kbaud OFDM (52 carriers)
BPSK, QPSK, 16QAM, 64QAM
on each carrier

EE584
2/8/2009

2-38/38

Finally, I have illustrated the increasingly popular 802.11 WLAN. Like cellular, the economy of scale has rapidly brought down the price of 802.11 networks from thousands of dollars to tens of dollars. However, we will see how inattention to potential attacks created a massive weakness in these networks that limit their utility for many applications.