2004

Vulnerability of Wireless Networks in Indoor and Urban Environments

Jenn, David C.; Sumagaysay, Paul

Vulnerability of Wireless Networks in Indoor and Urban Environments

Associate Professor David C. Jenn and LT Paul Sumagaysay, USN

Department of Electrical & Computer Engineering
Naval Postgraduate School
Monterey, CA

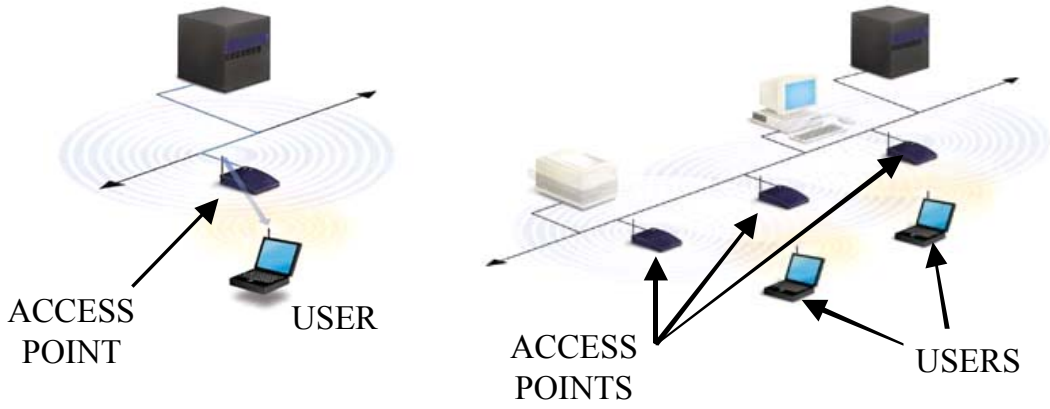
(831) 656-2254
jenn@nps.navy.mil
http://web.nps.navy.mil/~jenn

Wireless Systems and the Terrorist Threat

- Wireless systems are in common use in both the civilian and military sectors
- Examples include wireless local area networks (LANs) and mobile communications systems
- The signals from wireless systems radiate in free space and therefore can be intercepted by terrorist operatives
- Hidden receivers (or transmitters) can be placed in public areas such as lobbies and parking lots outside of buildings
- Small businesses may be particularly susceptible (unaware of the problem and do not have resources to spend on security)
- Methods of exploitation:
    1. Signals can be intercepted and data collected (e.g. meeting times, locations, and attendees)
    2. High power signals injected into the systems to jam or incapacitate
    3. Signals injected to deceive

Wireless Local Area Network (WLAN)

- WLANs allow roaming users access to a network



- WLANs are based on the IEEE 802.11 standard[1] (802.11b operates in the 2.45 GHz band; 802.11a operates in the 5 GHz band)
- Number of access points is determined by coverage requirements (usually by trial and error)
- The maximum range of coverage depends on the antenna parameters, transmit power, receiver sensitivity, and propagation environment

---

[1]K. Pahlavan, et al, "Trends in Local Wireless Networks," *IEEE Communications Magazine*, March 1995, pp. 88-95

WLAN Security

- Media Access Control (MAC): address-based access lists on access points are used to register and recognize MAC addresses that are allowed to join the network

- Radius server based authentication: users are authenticated against a centralized radius server that is based on the MAC address or the username and password

- Encryption between the wireless adapter and access points: Wired Equivalent Privacy (WEP) is an algorithm that is designed to provide privacy for data transmitted between the wireless client and the access point

  > Data encryption based on 40-bit or 128-bit keys that are hidden from users
  > WEP has been defeated by knowledgeable hackers
  > See S. Singhal, "The Seven Deadly Sins of Wireless LANS" for more on the misconceptions with regard to WEP security and its weakness[1]

[1] See www.reefedge.com

Link Equation

- Consider the access point antenna to be transmitting
- The received power at the user's receiver is given by the Friis transmission equation

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

P_r = received power, W

P_t = access point transmit power, W

G_t = gain of the access point antenna in the direction of the user

R = range (distance) between the user and access point antenna, m

G_r = gain of the user antenna

λ = wavelength = 0.1224 m at 2.45 GHz

L = loss factor to account for the many losses that occur in the operating environment and system (cables, connectors, antenna variations, multipath fading, etc.)

Detection Range

- The minimum power required for normal operating conditions at maximum range is $P_{r_{\min}}$
- Re-arrange the link equation and solve for the maximum range

$$R_{\max} = \sqrt{\frac{P_t G_t G_r \lambda^2 L}{(4\pi)^2 P_{r_{\min}}}}$$

- In practice, there is a link margin (safety factor) built into the system that is on the order of 10 to 100 (i.e., under normal operating conditions, at range $R_{\max}$, the received power $P_{r_{\min}}$ is higher than required)
- This equation is oversimplified but gives insight into system tradeoffs
- The intercept receiver only has control R, G_r $P_{r_{\min}}$ and to some extent L
- The antenna gain cannot be increased without limit
  - > physical size constraints
  - > limited by the coherence distance of the field

Decibel Unit

- In general, a dimensionless quantity Q in decibels (denoted Q_{dB}) is defined by

$$Q_{\text{dB}} = 10\log_{10}(Q)$$

- Q usually represents a power ratio, where the denominator is the reference
- Characters are added to the "dB" to denote the reference quantity. Examples:

$10\log_{10}\left(\frac{P}{1\text{W}}\right) = P_{\text{dBW}}$ (if just dB then 1W reference assumed)

$10\log_{10}\left(\frac{P}{1\text{mW}}\right) = 10\log_{10}\left(\frac{P}{0.001\text{W}}\right) = P_{\text{dBm}} (= P_{\text{dBW}} + 30)$

$10\log_{10}\left(\frac{G}{1}\right) = G_{\text{dBi}}$ (by definition antenna gain is referenced to an isotropic source so the “i” is typically not used)

- Note: 1. 10 dB represents an order magnitude change in the quantity Q
  2. the dB unit does not depend on the reference that is used to define it
  3. when quantities are multiplied their dB values add

WLAN System Parameters

- Typical transmitter power settings: 100 mW to 1 mW
- Receiver sensitivity (P_o, absolute minimum power to establish and maintain the link):

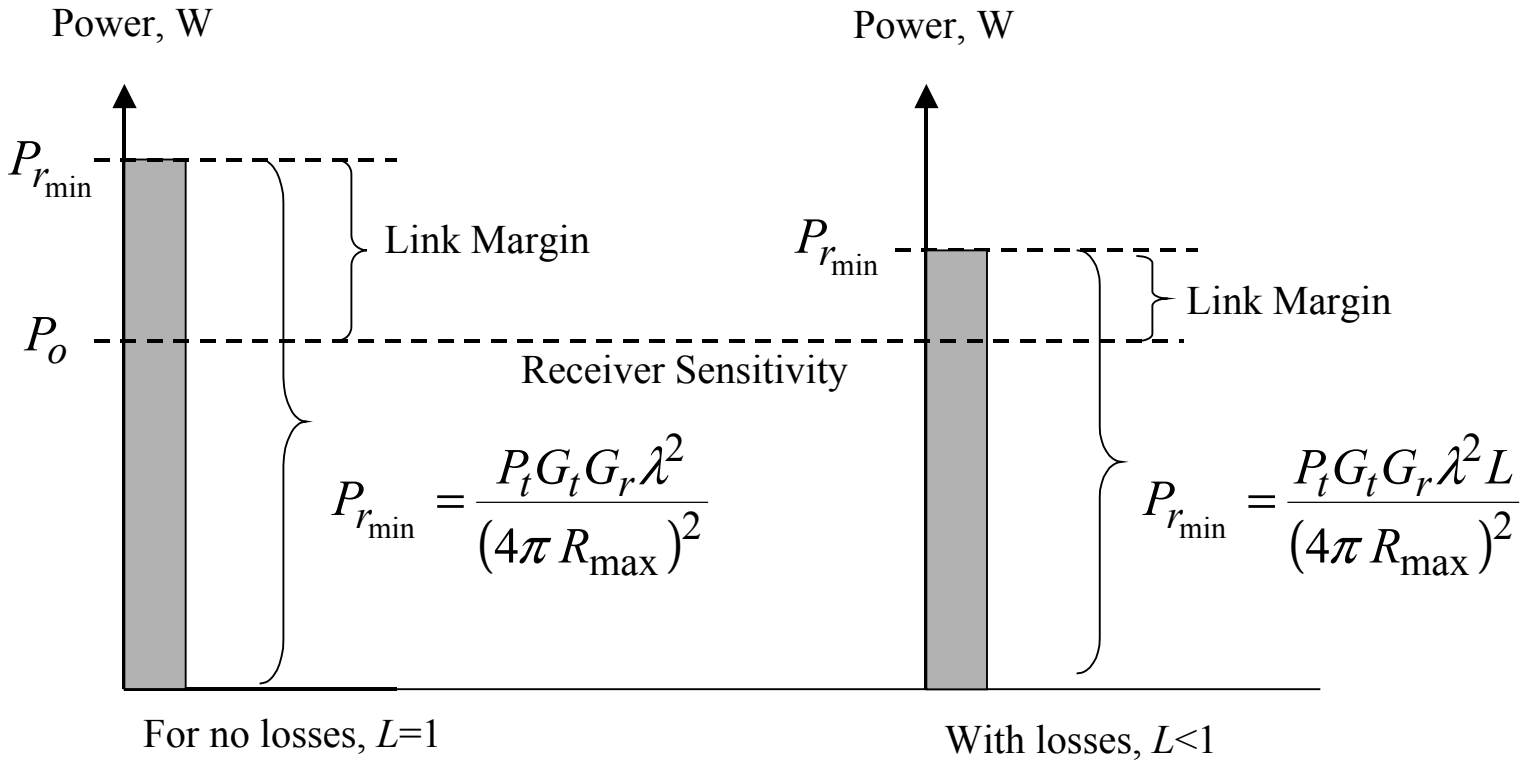
BIT RATE	MINIMUM SENSITIVITY LEVEL
1 Mbps	-94 dBm
2 Mbps	-91 dBm
5.5 Mbps	-89 dBm
11 Mbps	-85 dBm

- Advertised range:

INDOOR	OUTDOOR
130 ft (39.6m) at 11 Mbps	800 ft (244m) at 11 Mbps
350 ft (107m) at 1 Mbps	2000 ft (610m) at 1 Mbps

Illustration of the Friis Equation

- The loss can be as high as the link margin, and the link will still operate



Note: to accurately model the link, receiver noise should be considered, and the concept of signal-to-noise ratio (SNR) and probability of bit error introduced. To avoid this complication, the notion of link margin is used.

Sample Calculation of Detection Range

- Receiver sensitivity, $P_o = -94 \text{ dBm} = 10^{[(-94-30)/10]} = 3.98 \times 10^{-13}$ W
- Low transmit power uses more of the link margin than high transmit power[1]
  Assume: 20 dB link margin for high power: $L = -20$ dB = 0.01
  8 dB link margin for low power: $L = -8$ dB = 0.1585
- Gain of the access point antenna, $G_t = 2 \text{ dB} = 10^{2/10} = 1.6$ (typical dipole)
- Gain of the user antenna, $G_r = 0 \text{ dB} = 10^{0/10} = 1$ (isotropic element)
- For 100 mW = 0.1 W of transmit power

$$R_{\max} = \sqrt{\frac{P_t G_t G_r \lambda^2 L}{(4\pi)^2 P_o}} = \sqrt{\frac{(0.1)(1.6)(1)(0.1224)^2(.01)}{(4\pi)^2 (3.98 \times 10^{-13})}} = 617 \text{ m}$$

- For 1 mW of transmit power, $R_{\max} = 246$ m

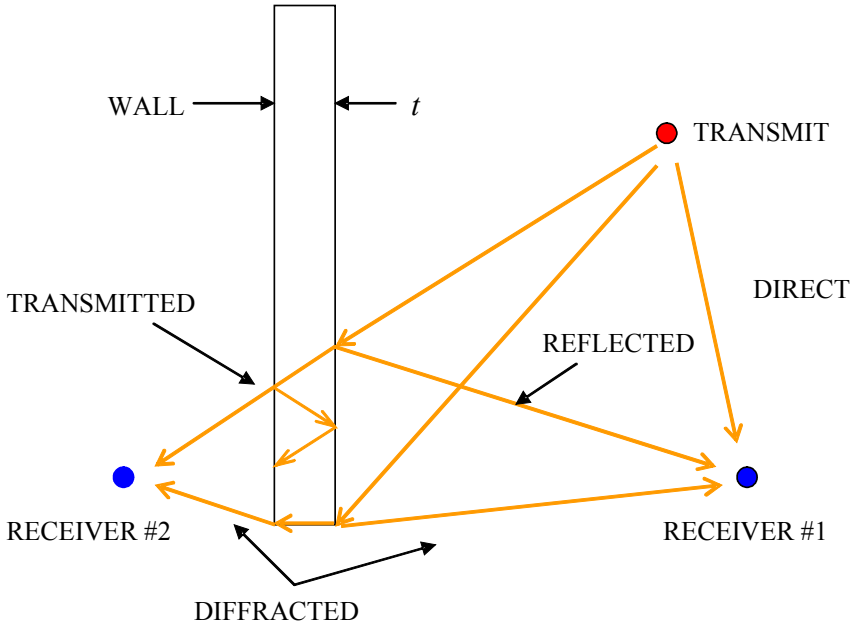
[1]This is related to the fact that because the signal is higher for high transmit powers, less of the link margin is needed to boost the signal to noise ratio

Electromagnetic Propagation Issues

- Electromagnetic wave propagation modeling of complex environments is a mature science driven by problems like radar cross section and mobile communications
- Exact formulations are possible, but they require a numerical solution of Maxwell's equations in integral or differential form (i.e., computationally demanding in memory and CPU time)
- Approximate methods reduce memory requirements and solution time, but neglect higher order effects
- Approximate methods are sufficient for wireless problems because the geometry models are generally of "low fidelity"
- High frequency approximations are valid at 2.45 GHz (assumption is that primary scattering objects like walls and furniture are large compared to the wavelength)

Propagation Issues

- Computational electromagnetics (CEM) codes were used to predict the propagation of electromagnetic (EM) waves indoors and in urban environments
- These codes are capable of modeling higher-order propagation mechanisms such as multipath and diffraction (which allow signals to be received behind walls, through windows, and behind buildings even when there is no line of sight path)
- Propagation and interaction with materials is decomposed into
  1. transmission
  2. reflection
  3. diffraction from discontinuities
- High frequency approximations are commonly referred to a "ray tracing"

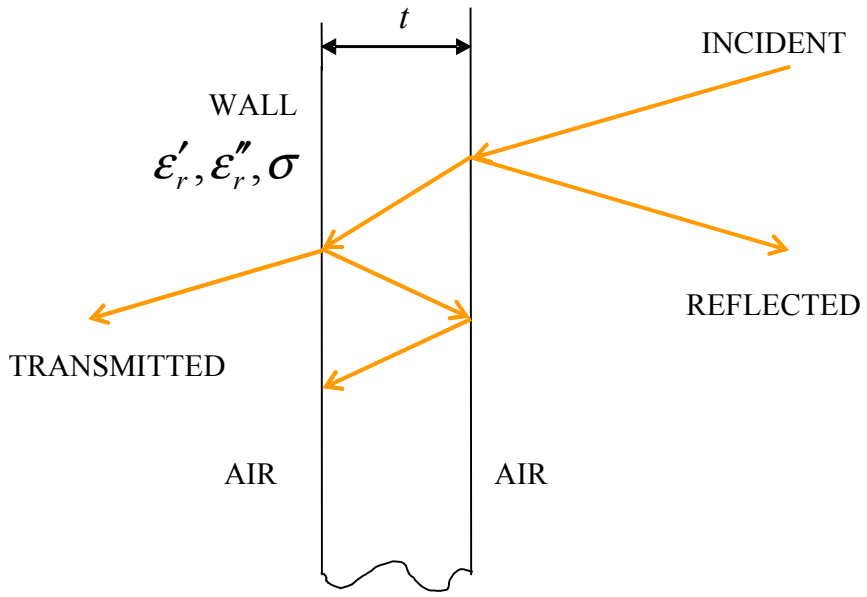


Propagation Issues

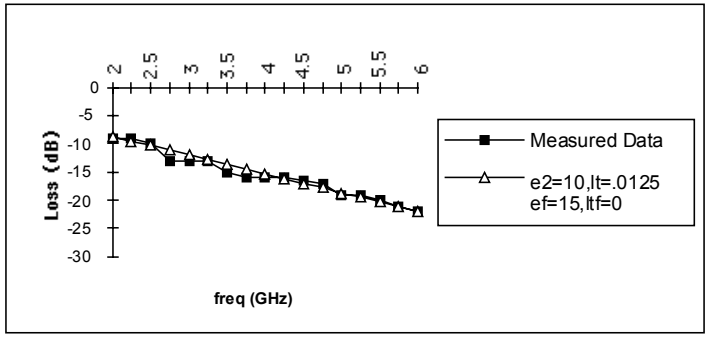
- Scattering properties of common building materials are determined by its permittivity and conductivity
- Sources of loss inside of walls (attenuation):
  1. absorption (energy dissipated inside of material)
  2. cancellation of reflections
- Decibel unit is used:

$$\text{Loss, dB} = 10\log_{10}\left(\frac{P_{transmitted}}{P_{incident}}\right)$$

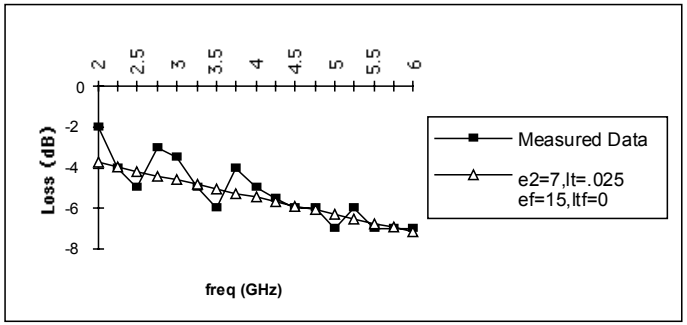
- Usually do not know exactly what is inside of a wall



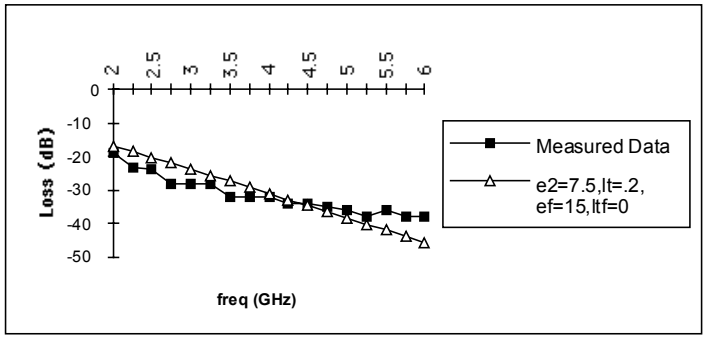
Propagation Loss Through Walls



Loss through a 10 inch concrete wall



Loss through a 1.75 inch wood doors



Loss through 1.75 inch metal doors

Measurement of propagation through building walls

Propagation Loss Through Windows

Closed blinds

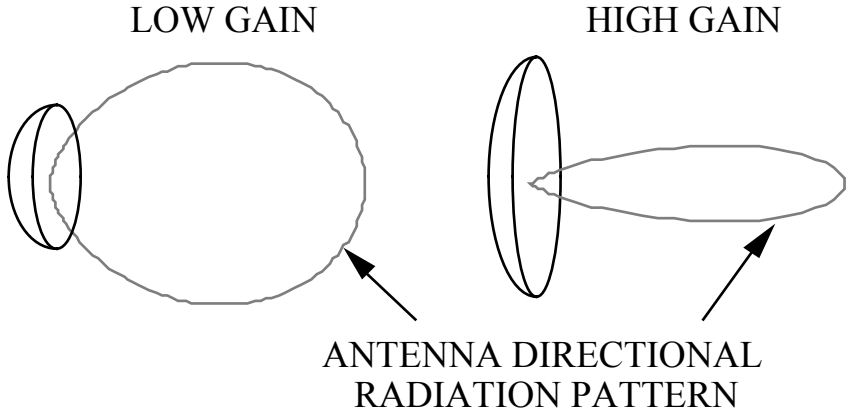
Insertion loss about 10 dB

Window tinting film

Insertion loss about 20 dB

Antenna Patterns and Gain

- The antenna pattern is a directional plot of the received or transmitted) signal
- From a systems point of view, two important antenna parameters are gain and beamwidth
- Both gain and beamwidth are measures of the antenna's capability to focus radiation
- In general, an increase in gain is accompanied by a decrease in beamwidth, and is achieved by increasing the antenna size relative to the wavelength
- With regard to WLANS, high gain is desirable for increased range, but low gain for wide area coverage with a single antenna

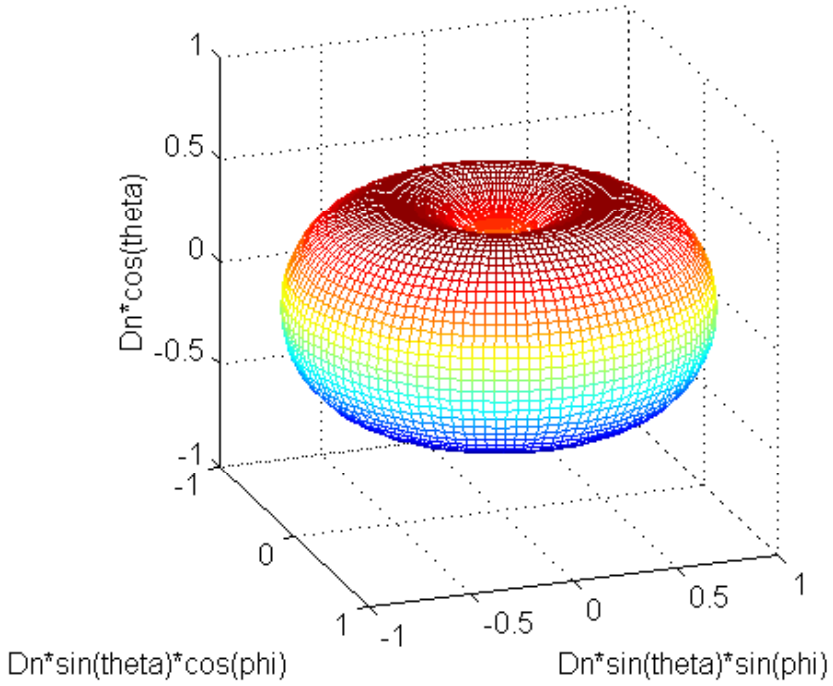


Dipole Antenna (Omnidirectional)

- Ceiling mount

- Desktop mount diversity anten

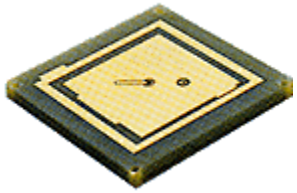
Spatial radiation distribution of a vertical dipole antenna



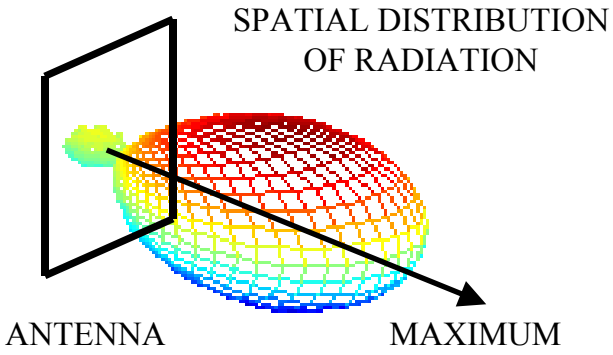
Directional Antennas

Microstrip patch antenna
(typically mounted on a wall)

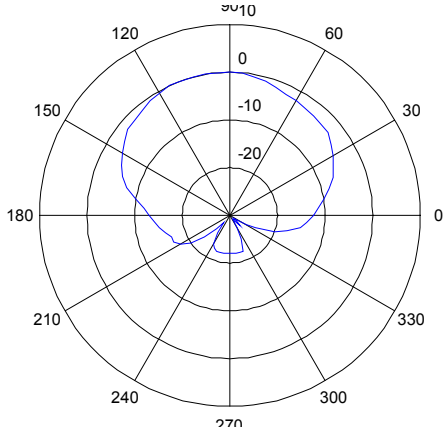
Radome cover removed



Radiation pattern (power measured as a function of angle at constant radius)



Typical antenna pattern
(top view)



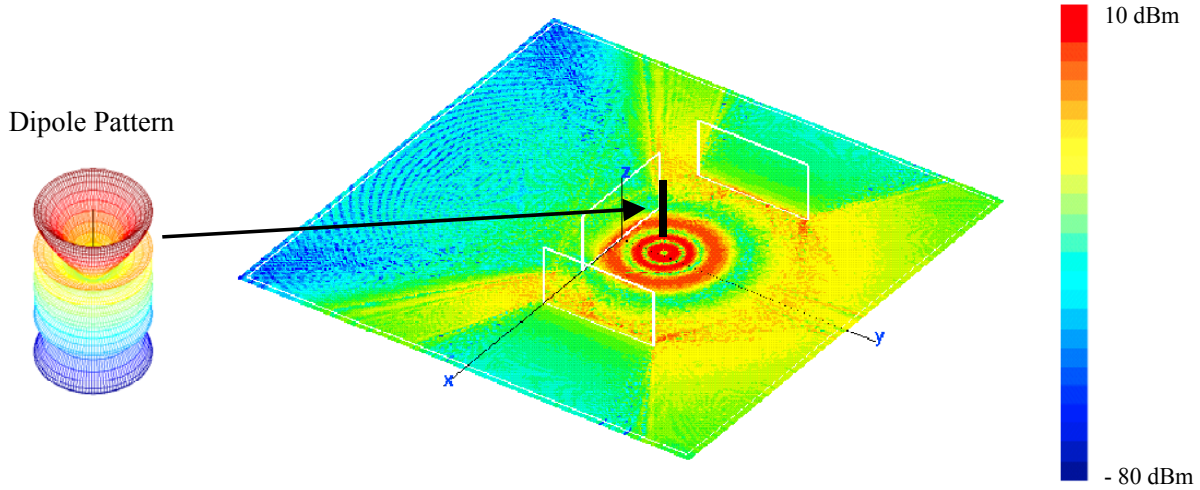
Urbana Wireless Toolset

- Components
  1. *XCell*: geometry builder and visualizer; antenna placement; observation point definition
  2. *Cifer*: utilities, translators, geometry manipulation
  3. *Urbana*: electromagnetic solvers

- Features
  1. Interfaces with computer aided design (CAD) software
  2. Reflections by geometrical optics (GO) or "shooting and bouncing rays" (SBR)
  3. Diffraction by geometrical theory of diffraction (GTD) or physical theory of diffraction (PTD)
  4. Surface and edge curvature can be modeled
  5. Complex materials (dielectrics, conductors, magnetic material)

Simple Three Wall Example

- Dipole behind walls (1 watt transmit power; plastic walls are 25m by 50m; 8 wavelength dipole antenna)

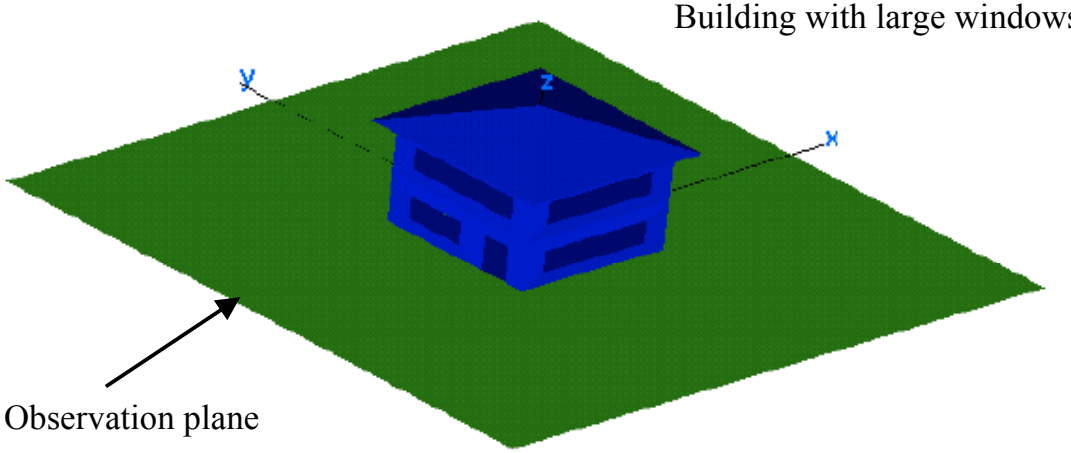


- Propagation features:
  - > dipole radiation rings (red)
  - > multipath from ground and wall surfaces (red speckle)
  - > propagation through gaps
  - > "shadows" behind walls (shadow boundaries from wall edges
  - > diffraction from wall edges (blue arcs)

Two Story Building

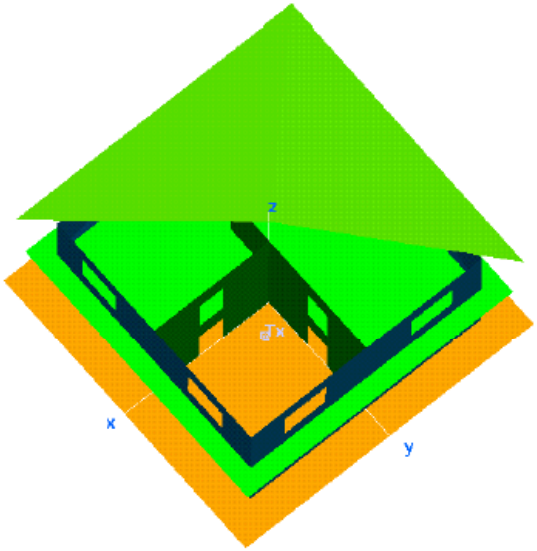
- Two story building: 40 feet on a side

Building with large windows

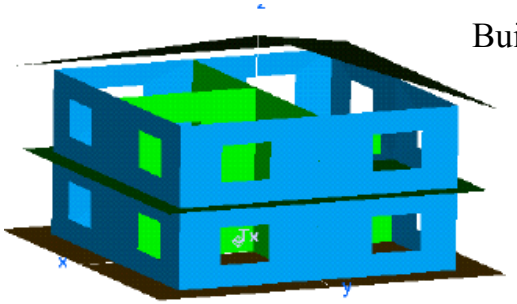


Observation plane

Partial cut away showing ground floor



Building with small windows

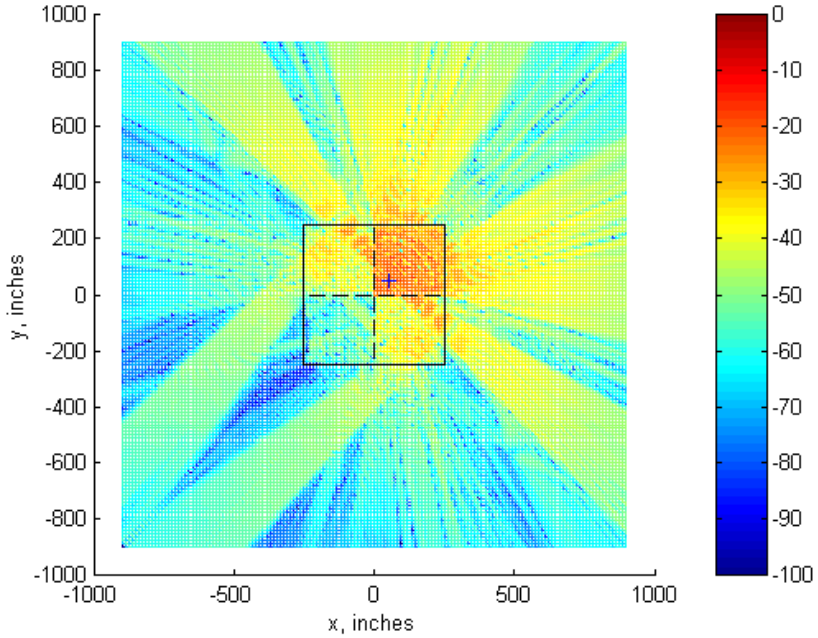


Two Story Building Details

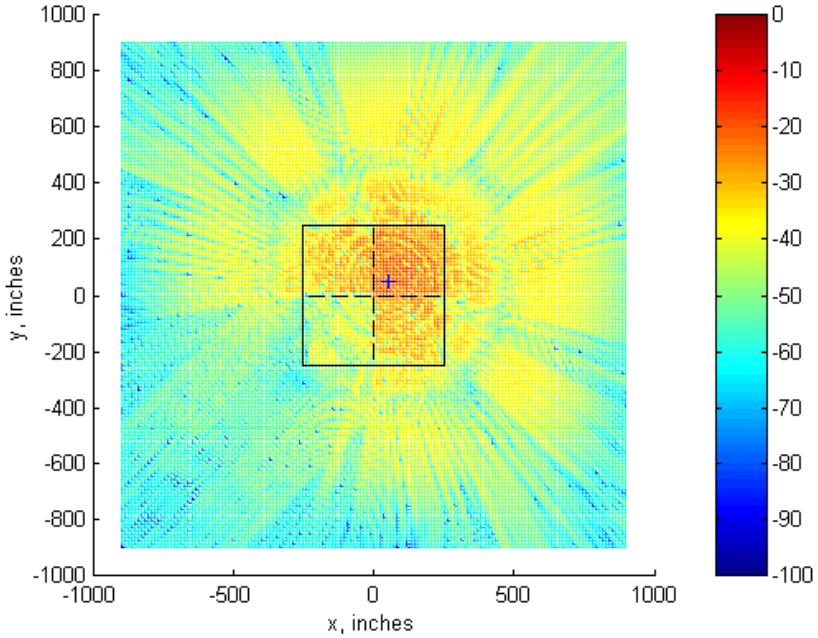
- Two story building: 40 feet on a side
  Rooms square, 20 feet on a side
- Exterior materials: Wood
  Concrete
  Metal/composite
- Windows: Open
  Standard glass
  Tinted
  Various opening sizes
- Interior walls coated with foam sound attenuating material
- Ground material: Perfect electric conductor
  Imperfect conductor
- Observation plane: 150 feet on a side
  Various heights above ground
- Various transmit power levels, dipoles on transmit and receive

Wall Materials

Metal composite walls



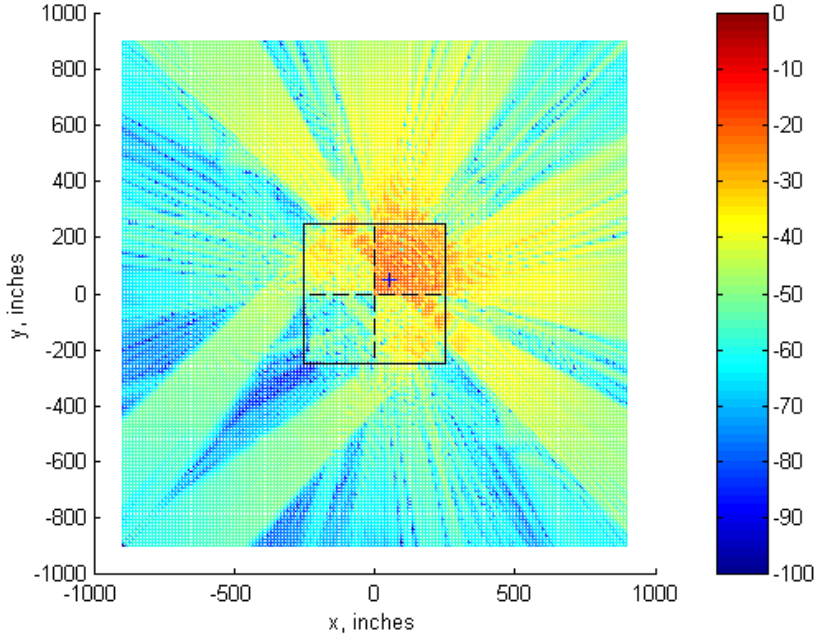
Wood walls



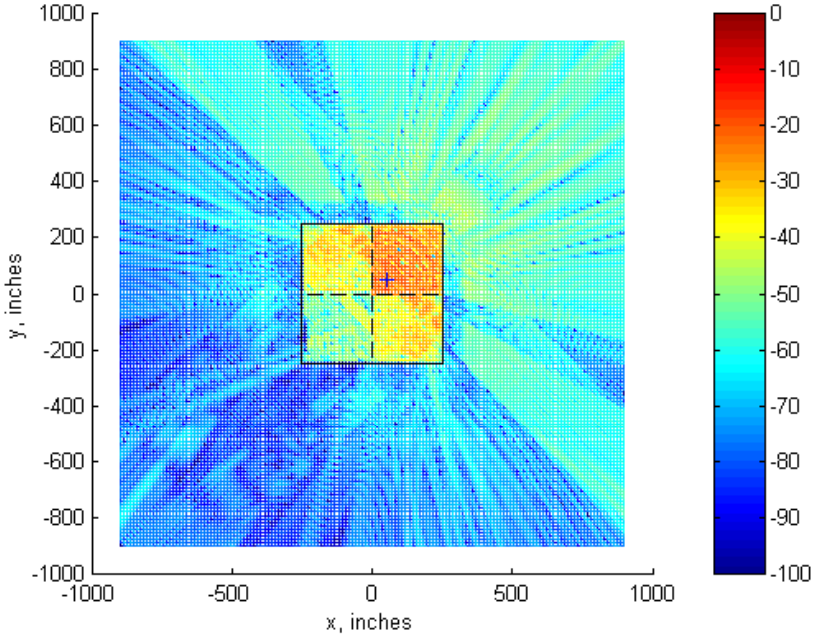
- Propagation through windows dominates for metal buildings
- Many transmissions and reflections diffuse the signal for the wood building
- Receive antenna is 5 feet above ground

Window Materials

Standard glass windows



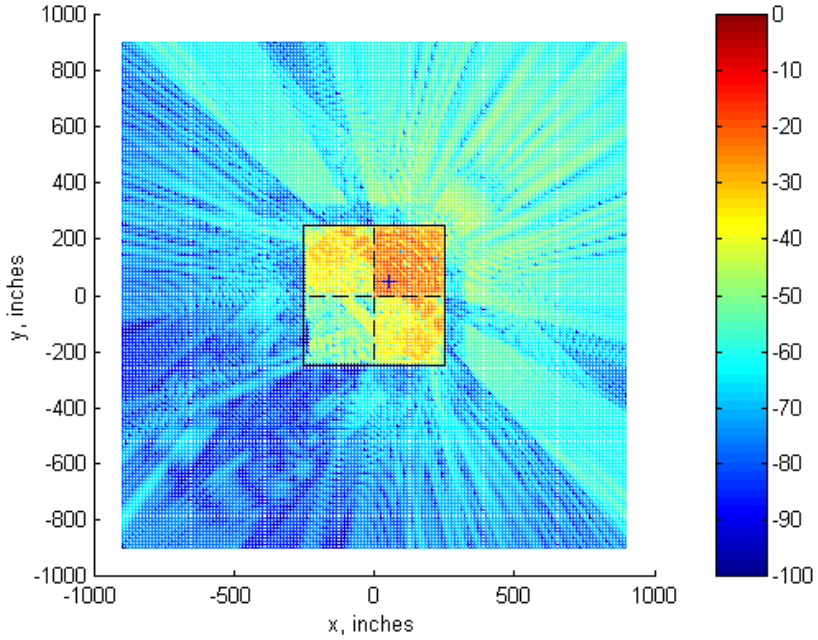
Tinted windows



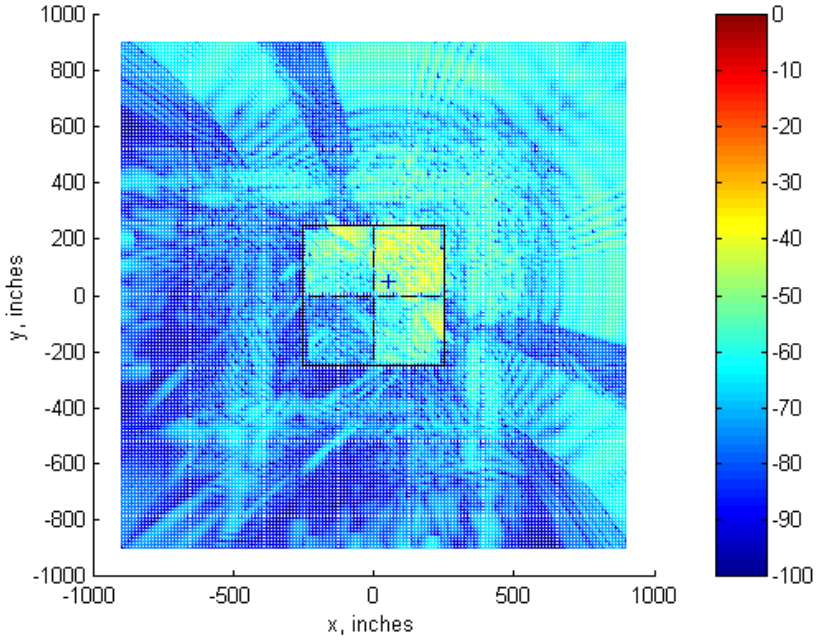
- There is a direct line of sight above the window sill from inside the building
- Receive antenna is 5 feet above ground

Antenna Location

Access point on 1st floor



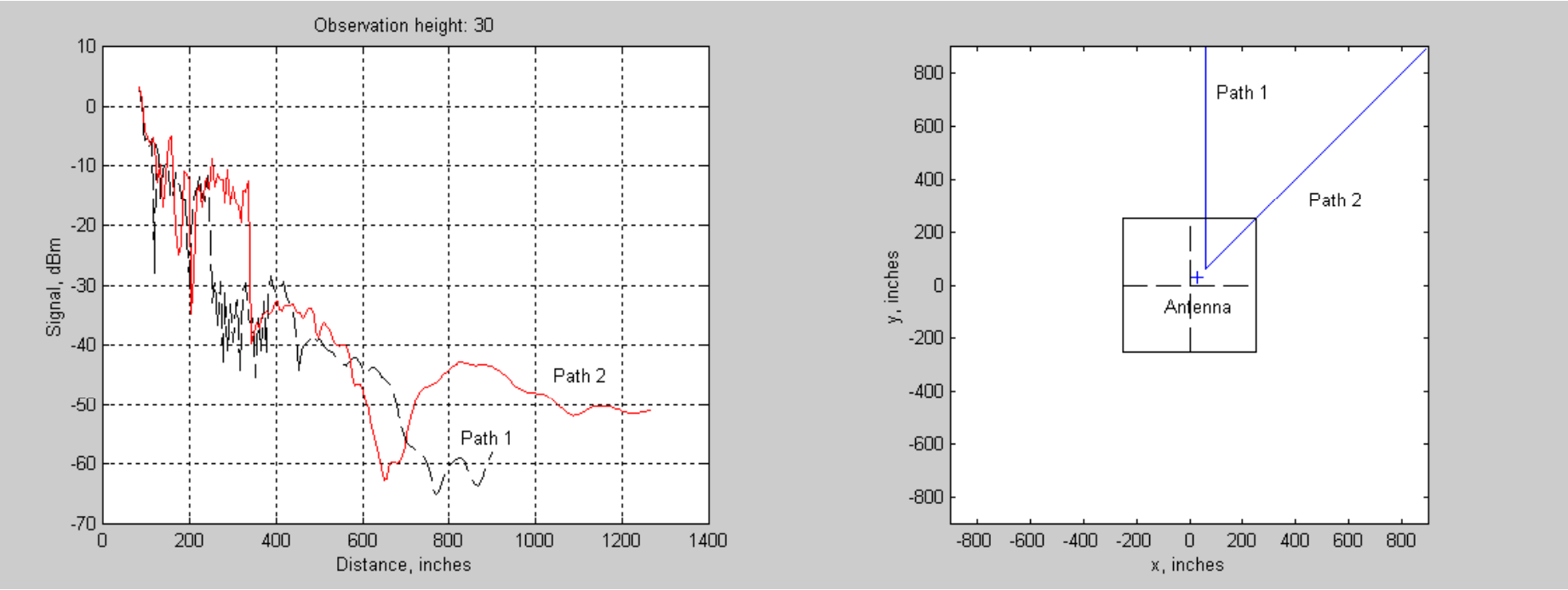
Access point on 2nd floor



- Detection is reduced by moving the access point to second floor
- Results in reduced signal levels inside on first floor
- Receive antenna is 5 feet above ground

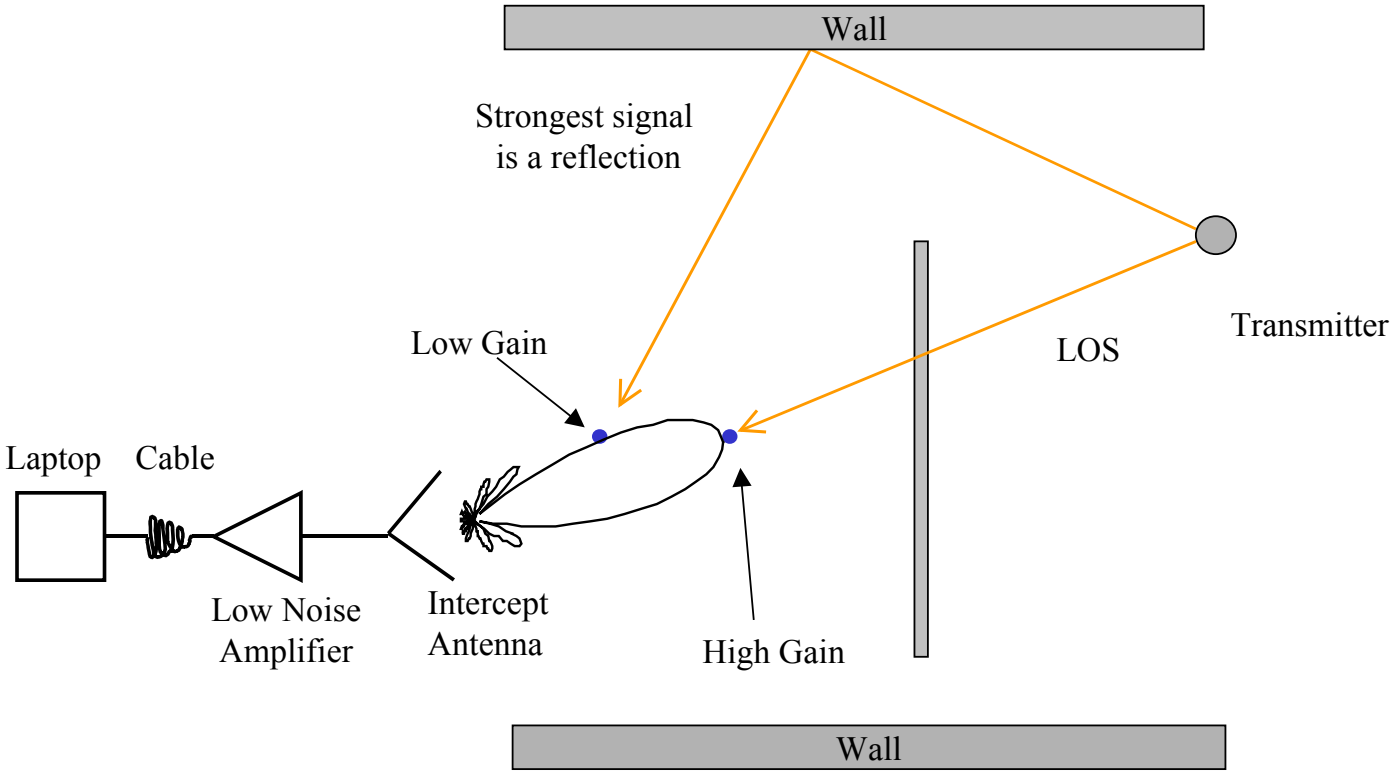
Line Path

- Metal composite walls, standard glass
- 10 to 20 dB drop through the wall



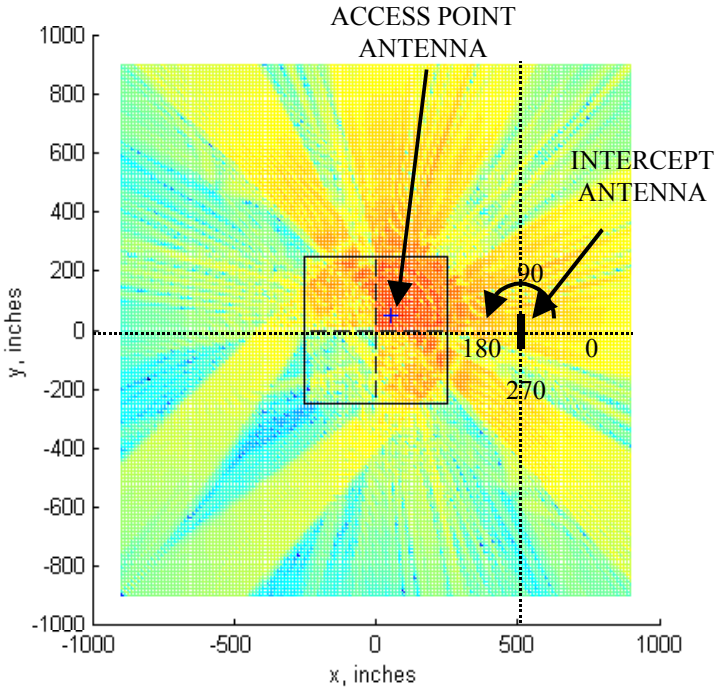
Intercept Antenna

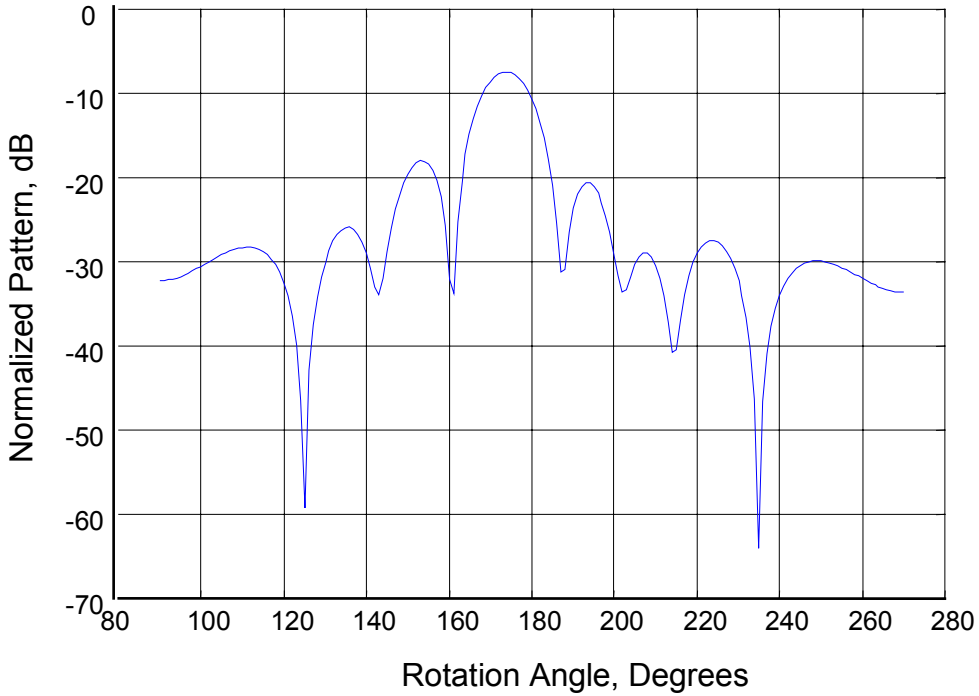
- High gain intercept antenna increases the detection range
- High gain is accompanied by narrow beamwidth.
- Antenna pointing becomes important, but the direction of the strongest signal is not always obvious



Intercept Antenna Pointing

- Antenna rotates around its vertical axis (18 by 18 square antenna centered 50 inches above the ground)
- Plot of antenna output as it is rotated
- The 0 dB reference is the power that would be received if the antenna is pointed directly at the access point (30 inches above the ground)





Summary and Conclusions

- WLAN transmission levels vary greatly depending on
  - > Exterior wall composition
  - > Location of access points
  - > Location of intercept receiver
  - > Sophistication of intercept antenna and receiver
  - > WLAN system parameters
- General guidelines for reducing probability of interception:
  - > Locate access points in the most interior building spaces
  - > Close all doors
  - > Close blinds on exterior windows (metal blinds provide about 10dB of attenuation)
  - > Use directive or sectored access point antennas to limit the spatial radiation distribution
  - > Use minimum power for coverage (“power management”)
  - > Coverings on the inside of exterior walls can be used to attenuate signals

Future Work

- Examine the vulnerability of point-to-point wireless networks
- Point-to-point links are used to network widely separated areas, such as several buildings on a business campus
- Generally, the antennas in these links are more directional than those used indoors, thereby making it more difficult to intercept signals
- However, it is possible to get into the link's field of view in some cases. For a rooftop link, the perpetrator could be on one of the top floors of the building making interception of the signal possible