



NAVAL  
POSTGRADUATE  
SCHOOL

MONTEREY, CALIFORNIA

**THESIS**

**VULNERABILITY OF WIRELESS POINT-TO-POINT  
SYSTEMS TO INTERCEPTION**

by

Wee Pin Melvin Lim

December 2003

Thesis Advisor:  
Second Reader:

David C. Jenn  
Jeffrey B. Knorr

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> December 2003	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE:</b> Title (Mix case letters) Vulnerability of wireless point-to-point systems to interception			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Melvin Lim Wee Pin				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public Release; distribution is unlimited			<b>12b. DISTRIBUTION CODE</b>  A	
<b>13. ABSTRACT (maximum 200 words)</b> Wireless systems have always been susceptible to interception in both urban outdoor and indoor environments. In point-to-point communication links, the placement of base station antennas is usually determined by an experimental or analytical assessment of the propagation path. Since point-to-point links are typically used to network widely separated areas, antennas used in such situations are likely to be directional, but may still be susceptible to interception by covert entities. In this thesis research, issues pertaining to vulnerability will be identified and preventive measures will be suggested. The generation of received signal contours as a function of location and frequency for different propagation models will also be investigated. This thesis thus examines the vulnerabilities of wireless point-to-point communication to interception by propagation simulations using computational electromagnetic codes available in the Naval Postgraduate ECE Department's Microwave and Antenna Laboratory. The software was used to examine the vulnerability of these wireless systems and identify simple measures that can be taken to increase the system's security.				
<b>14. SUBJECT TERMS</b> Wireless Point-to-Point Vulnerability, Antenna Propagation, Indoor-Outdoor Propagation.			<b>15. NUMBER OF PAGES</b> 93	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b>  Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b>  Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b>  Unclassified	<b>20. LIMITATION OF ABSTRACT</b>  UL	

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**VULNERABILITY OF WIRELESS POINT-TO-POINT SYSTEMS TO  
INTERCEPTION**

Melvin Lim Wee Pin  
Civilian, Singapore DOD  
B.Eng. (Electrical & Computer) Queensland University of Technology, 1999  
M.S. (Engineering Management) Queensland University of Technology, 2000

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN ENGINEERING SCIENCE  
(ELECTRICAL ENGINEERING)**

from the

**NAVAL POSTGRADUATE SCHOOL  
December 2003**

Author: Melvin Lim Wee Pin

Approved by: Professor David C. Jenn  
Thesis Advisor

Professor Jeffrey B. Knorr  
Second Reader

Professor John Powers  
Chairman  
Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

## ABSTRACT

Wireless systems have always been susceptible to interception in both urban outdoor and indoor environments. In point-to-point communication links, the placement of base station antennas is usually determined by an experimental or analytical assessment of the propagation path. Since point-to-point links are typically used to network widely separated areas, antennas used in such situations are likely to be directional, but may still be susceptible to interception by covert entities. In this thesis research, issues pertaining to vulnerability will be identified and preventive measures will be suggested. The generation of received signal contours as a function of location and frequency for different propagation models will also be investigated.

This thesis thus examines the vulnerabilities of wireless point-to-point communication to interception by propagation simulations using computational electromagnetic codes available in the Naval Postgraduate ECE Department's Microwave and Antenna Laboratory. The software was used to examine the vulnerability of these wireless systems and identify simple measures that can be taken to increase the system's security.

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>WIRELESS POINT-TO-POINT NETWORKS .....</b>	<b>1</b>
<b>B.</b>	<b>WIRELESS NETWORK RISKS .....</b>	<b>1</b>
<b>C.</b>	<b>OUT OF HARM'S WAY .....</b>	<b>2</b>
<b>D.</b>	<b>OBJECTIVE AND TECHNICAL APPROACH.....</b>	<b>2</b>
<b>E.</b>	<b>THESIS OUTLINE.....</b>	<b>3</b>
<b>II.</b>	<b>BACKGROUND .....</b>	<b>5</b>
<b>A.</b>	<b>WIRELESS POINT-TO-POINT NETWORKS .....</b>	<b>5</b>
<b>B.</b>	<b>TOOLS FOR PROPAGATION MODELING.....</b>	<b>7</b>
<b>1.</b>	<b>Geometric Optics .....</b>	<b>7</b>
<b>2.</b>	<b>Geometrical Theory of Diffraction.....</b>	<b>7</b>
<b>3.</b>	<b>Urbana Wireless Toolset .....</b>	<b>8</b>
<b>III.</b>	<b>ASPECTS OF THE ELECTROMAGNETIC MODEL .....</b>	<b>11</b>
<b>A.</b>	<b>RADIATION PATTERNS.....</b>	<b>11</b>
<b>1.</b>	<b>Simulation of a PTP Antenna Using a Uniform Circular Aperture.....</b>	<b>12</b>
<b>2.</b>	<b>Antenna Rotation .....</b>	<b>13</b>
<b>B.</b>	<b>FRESNEL ZONES.....</b>	<b>15</b>
<b>C.</b>	<b>PATH LOSS .....</b>	<b>17</b>
<b>1.</b>	<b>Effective Isotropic Radiated Power.....</b>	<b>19</b>
<b>D.</b>	<b>MULTIPATH DISTORTION .....</b>	<b>19</b>
<b>E.</b>	<b>VSWR AND RETURN LOSS.....</b>	<b>20</b>
<b>F.</b>	<b>OTHER THEORETICAL CONSIDERATIONS.....</b>	<b>22</b>
<b>IV.</b>	<b>URBANA TEST SIMULATIONS.....</b>	<b>23</b>
<b>A.</b>	<b>INPUT DATA GENERATION .....</b>	<b>23</b>
<b>1.</b>	<b>Creation of a Directional Antenna Pattern .....</b>	<b>23</b>
<b>2.</b>	<b>Creating the Geometry Facets .....</b>	<b>25</b>
<b>3.</b>	<b>Creating Observation Points.....</b>	<b>25</b>
<b>B.</b>	<b>INPUT FILE GENERATION AND EXECUTING URBANA .....</b>	<b>27</b>
<b>C.</b>	<b>DISPLAYING RESULTS .....</b>	<b>27</b>
<b>D.</b>	<b>VARIATIONS OF THE GROUND PLANE TEST CASE.....</b>	<b>30</b>
<b>E.</b>	<b>SUMMARY OF TEST CASE RESULTS.....</b>	<b>34</b>
<b>V.</b>	<b>AIRBASE MODEL.....</b>	<b>35</b>
<b>A.</b>	<b>AIRBASE BUILDING MODEL .....</b>	<b>35</b>
<b>1.</b>	<b>Building the Model.....</b>	<b>35</b>
<b>2.</b>	<b>Creating Observation Points.....</b>	<b>36</b>
<b>B.</b>	<b>INITIAL URBANA SIMULATIONS .....</b>	<b>37</b>
<b>1.</b>	<b>Summary of Initial Simulation Results.....</b>	<b>43</b>
<b>C.</b>	<b>INVESTIGATION INTO LOCALIZED SCATTERING EFFECTS .....</b>	<b>43</b>
<b>1.</b>	<b>Building Orientation and Multipath .....</b>	<b>43</b>
<b>2.</b>	<b>Zooming in on the Hotspot.....</b>	<b>45</b>

3.	Absorbing Walls.....	46
4.	Doped (Tinted) Glass .....	47
5.	Urbana Simulation Summary .....	49
D.	OTHER SCENARIOS.....	49
1.	Antenna Position .....	49
2.	Parked Cars.....	51
3.	HPBW and Frequency.....	53
4.	Summary.....	54
E.	SUMMARY .....	54
VI.	SUMMARY AND CONCLUSIONS .....	55
A.	SUMMARY .....	55
B.	CONCLUSIONS .....	55
C.	FUTURE WORK.....	56
	APPENDIX.....	59
A.	WIRELESS POINT-TO-POINT PERIPHERALS .....	59
1.	RF spectrum allocation.....	59
2.	Antennas .....	59
3.	Bridges .....	61
B.	MATLAB CODES .....	62
C.	URBANA INPUT SCRIPT FILE .....	66
	LIST OF REFERENCES.....	73
	INITIAL DISTRIBUTION LIST .....	75

## LIST OF FIGURES

Figure 1.	(a) Point-to-point (b) Point-to-multiple points (From Ref. [7].).....	6
Figure 2.	Illustration of the direct, reflected, transmitted and diffracted wave components .....	8
Figure 3.	<b>Urbana</b> flow diagram.....	10
Figure 4.	Radiation pattern of a 7.5°-HPBW, 2.4-GHz antenna .....	13
Figure 5.	Antenna coordinates system .....	14
Figure 6.	Fresnel zones.....	16
Figure 7.	Approximate Fresnel zone clearance (From Ref. [9].) .....	16
Figure 8.	Distance versus path loss for frequency of 2.4 GHz.....	18
Figure 9.	Distortion of signal caused by multipath inside a building (From Ref. [2].).....	20
Figure 10.	Transmitting antenna height reduced to avoid reflections (From Ref. [11].).....	20
Figure 11.	VSWR versus Return Loss .....	21
Figure 12.	Main GUI interface page .....	24
Figure 13.	Antenna pattern generation GUI.....	24
Figure 14.	Ground plane facet.....	25
Figure 15.	Observation point generation.....	26
Figure 16.	Ground plane with transmitting antenna signal contour for input data shown in Table 4.....	29
Figure 17.	Radiation pattern at 7 m.....	30
Figure 18.	Radiation pattern at 16 m offset and 7.5° HPBW .....	31
Figure 19.	Antenna radiation pattern in the presence of a building with absorbing facets .....	32
Figure 20.	Two antennas with input data shown in Table 10.....	33
Figure 21.	Hypothetical airbase model.....	36
Figure 22.	Antenna rotation GUI .....	38
Figure 23.	Signal contour of case 1 in Table 12.....	41
Figure 24.	Signal contour of case 2 in Table 12.....	41
Figure 25.	Signal contour of case 3 in Table 12.....	41
Figure 26.	Signal contour of case 4 in Table 12.....	42
Figure 27.	Signal contour of case 5 in Table 12.....	42
Figure 28.	Signal contour of case 6 in Table 12.....	43
Figure 29.	Signal contours when buildings are translated.....	44
Figure 30.	Signal contour at 2 m with one ray bounce.....	44
Figure 31.	Signal contour at 2 m with two ray bounces.....	45
Figure 32.	Signal contour at 2 m with four ray bounces .....	45
Figure 33.	Signal contour at 2 m .....	46
Figure 34.	Signal contour at 68 m .....	46
Figure 35.	Signal contour with a 2-m absorbing wall in front of the affected building.....	47
Figure 36.	Tinted glass on single side of building .....	47
Figure 37.	Signal contours showing doped glass coatings on wall .....	49
Figure 38.	Signal contour at 2-m height.....	51
Figure 39.	Signal contour at 62-m height.....	51

Figure 40.	Signal contour at 2 m offset with parked cars.....	53
Figure 41.	Signal contour at 2 m offset with a broader beamwidth .....	54
Figure 42.	FSO product overview (From Ref. [15].) .....	57
Figure 43.	An operational FSO equipment setup (From Ref. [15].) .....	57
Figure 44.	RF spectrum allocation (From Ref. [15].) .....	59
Figure 45.	A commercial off the shelf (COTS) Yagi antenna (From Ref. [17].).....	60

## LIST OF TABLES

Table 1.	WLAN Receiver sensitivity (From Ref. [2].).....	6
Table 2.	Distance versus path loss (dB) for typical wireless frequencies (Ref. [10].)...	17
Table 3.	Typical wireless PTP system EIRP (From Ref. [2].).....	19
Table 4.	Important <b>Urbana</b> Input Parameters .....	27
Table 5.	Inputs For Running <i>f2f.x</i> .....	28
Table 6.	Data for the antenna pattern test case results of Figure 16 .....	29
Table 7.	Data for the antenna pattern test case results of Figure 17 .....	30
Table 8.	Data for the antenna pattern test case results of Figure 18 .....	31
Table 9.	Data for the results of Figure 19 .....	32
Table 10.	Data for the results of Figure 20 .....	33
Table 11.	Observation plane size .....	37
Table 12.	Summary of initial test cases .....	37
Table 13.	<b>Urbana</b> input parameters for airbase building model .....	39
Table 14.	Inputs for running <i>f2f.x</i> .....	40
Table 15.	Observation plane size .....	46
Table 16.	Observation plane size .....	48
Table 17.	<b>Urbana</b> input parameters for the airbase building model with tinted glass ....	48
Table 18.	<b>Urbana</b> input parameters for the airbase building model with tinted glass ....	50
Table 19.	<b>Urbana</b> input parameters for the airbase building model with parked cars ....	52
Table 20.	Typical client adapter antennas (From Ref. [6].).....	60
Table 21.	Typical COTS bridges (From Ref. [2, 17].).....	61

THIS PAGE INTENTIONALLY LEFT BLANK

## ACKNOWLEDGMENTS

The author would like to gratefully thank Professor David Jenn for his patience, support, and generosity with time and instructions. The author would also like to thank Professor Jeffrey Knorr for his instruction and support with this thesis. Thanks also to the author's wife, Grace, for being a wonderful wife and being understanding. The author thanks the Lord and all of his classmates who helped him to achieve success at the Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

## EXECUTIVE SUMMARY

As information bandwidth increases, the push for wireless communications will escalate. The benefits of using a wireless topology include real-time information availability, achievable high bandwidths, resilience to failures, and simple and rapid installation.

The susceptibility of wireless systems has always been a topic of interest. The drawback of an omni-directional antenna commonly found in most local wireless systems is fairly apparent. However, in the case of a directional antenna in a point-to-point wireless communication scenario, it is commonly believed that interception is not a major concern. However, this research has shown that there is most likely ample opportunity for uninvited intruders to hack into the network.

This possibility is even more threatening in a military environment as critical data may be compromised. The purpose of this research is to examine the vulnerability of wireless point-to-point communication to interception and to determine what simple steps can be taken to improve security. The **Urbana** wireless toolset provides the means for computer simulation to predict multipath signals of wireless networks in complex environments such as point-to-point propagation between buildings.

Several scenarios were modeled to investigate the signal strength of transmitted electromagnetic waves at a grid of observation points. Initial simulations include testing of the antenna pattern, effects of various observation plane levels on reception and the effects of diffraction. This was achieved using an antenna pattern that was generated in Matlab.

Subsequent simulations were executed using a replica of an airbase model. The different simulation results clearly show the various effects of scattering from the surrounding buildings, parked cars, and antenna placements. All simulations include the effects of polarization, material properties, diffraction, and antenna patterns. The simulation results have shown that sporadic hotspots may appear due to the building layouts. According to the results of the experiments, some precautions are suggested to

reduce the chances of interception, including adjustment of the locations of the antennas, tinting of windows, exercising of physical security measures in regions of hotspots and selective frequency hopping.

The thesis concludes with the suggestion that a free space optics (FSO) system serve as a primary wireless link along with a radio frequency wireless system in a dual redundancy system. A simulation of urban optical propagation behavior should be performed so that a comparison of FSO and RF can be made.

## **I. INTRODUCTION**

A company or a military installation typically sets up a wireless local access network (WLANs) in early phases of its existence. Most industry estimates suggest that more than 50% of all enterprises will have at least one WLAN installation by 2003 [1]. As the organization grows, it may acquire new buildings several tens of meters away or even up to hundreds of meters apart. This chapter looks at the motivation and objectives for the thesis research and outlines the approach.

### **A. WIRELESS POINT-TO-POINT NETWORKS**

Many radio frequency (RF) systems, like cellular phones, police radios, and WLANs intentionally radiate signals in all directions making the signal accessible to anyone with a receiver. Instead of radiating in all directions, point-to-point (PTP) microwave systems transmit a highly directional, cone-shaped beam that minimizes off-axis radiation, thereby reducing the potential for security breaches. However, the divergent transmit beam is still vulnerable to interception and jamming within a fairly wide footprint. This may vary from the side of a building to an entire city block. As a result, an unauthorized receiver can be located well off-axis of the main beam and remain fairly discreet.

### **B. WIRELESS NETWORK RISKS**

Wireless networks may be put at risk by someone trying to get unauthorized access to the internal network. Some of the more common risks include stealing and disclosing sensitive information transmitted unencrypted over the air, an adversary launching a denial of service (DoS) attack against wireless connections or devices, and stealing the identity of network users.

Often, emphasis is placed on software-level protection. However, in the case of PTP wireless transmission, signals could be picked up from areas least expected and adversaries will be able to attack ad-hoc transmissions.

### **C. OUT OF HARM'S WAY**

Security is always a major concern with wireless systems, but since most well-designed point-to-point links are highly directional, intercepting signals is difficult. Nonetheless, most vendors include hardware-based encryption features that do not impair system performance. An example of one such methodology in securing a single point-to-point link is to employ simple shared keys.

In order to retain robust received signal strength, directional antennas used to communicate between two buildings must be properly aligned, as directional antennas have greatly reduced radiation angles. In doing so, sporadic hotspots may emerge and security may be compromised. The *Wall Street Journal* (April 27, 2001) described two hackers with a laptop and a boom antenna driving around Silicon Valley listening to network after network [2]. It was revealed that the highest signal strength areas were outside of many *Fortune 500* enterprises. This shows that the larger organizations are the most vulnerable. One solution is for companies to embrace WLAN security standards such as 802.1X authentication standards, Wireless Equivalency Privacy (WEP) key management, and user and session authentication. Of course, the ideal situation is to prevent a perpetrator from tapping into a wireless signal in the first place.

### **D. OBJECTIVE AND TECHNICAL APPROACH**

The purpose of this research was to examine the vulnerability of wireless point-to-point communication to interception, and to determine the steps that can be taken to improve security.

The **Urbana** Toolset used a method of predicting wireless antenna propagation in typical environments such as the surroundings of buildings. The propagation model

utilizes a three-dimensional (3-D) ray tracing process that predicts the local mean power received at any given point. For each point, the vector sum of the multipath power is computed. Using the model, the effects of polarization, material properties, and antenna patterns can be changed to observe the signal levels. The toolset also accounts for edge diffraction that may contribute significantly due to numerous building edges around a typical city block.

The simulations provide contours of power levels that can be used to predict the maximum detection range of the wireless signals. The effect of several system and environmental parameters on the detection range are examined. Therefore, the research attempts to identify the effects of the position of antennas and building materials on how the signal can be intercepted around of the boundaries of the structure. Systems designers generally address these issues from the coverage point of view. For a secure wireless PTP system, the issues must also be considered from an interceptability point of view.

The following steps were taken in order to achieve the goals of this thesis:

1. Familiarization with the **Urbana** Toolset and validation of some simple antenna patterns matching those typically found in point-to-point communications.
2. Modeling a directional antenna used in PTP wireless transmission.
3. Generation of several building models, and modeling of various coating materials.
4. Simulating a realistic PTP link environment and identifying any potential regions that may be susceptible to interception.

## **E. THESIS OUTLINE**

Chapter II discusses the various hardware used with wireless PTP networks. The **Urbana** Wireless Toolset will be described.

Chapter III discusses some of the theoretical considerations of electromagnetic propagation. Specifically, the chapter will introduce the antenna characteristics, Fresnel zones, path loss, and VSWR.

Chapter IV validates the basic component of the simulation process. The simulation process flowchart is presented for the **Urbana** suite of programs. A two-building model was created using the *cifer.x* program, in order to validate the software.

Chapter V introduces an airbase building model. The model consists of several building blocks with different facets and materials (cement, glass, perfect electric conductor (PEC), etc.). Two 2.4-GHz antennas are placed on top of two buildings and various signal contours are plotted. Several other realistic scenarios were also simulated.

Chapter VI summarizes the simulations and presents some conclusions based on the data from Chapters IV and V. Suggestions for further research are also presented.

Appendix A lists down some of the commonly found wireless peripherals, Appendix B compiles the Matlab codes used in this thesis and Appendix C shows the input script file for **Urbana**.

## II. BACKGROUND

Wireless PTP communications systems are implemented as an extension to WLANs within a building to provide an entire grid of wireless connectivity between distant buildings. This chapter looks at the various components of a wireless PTP system and the tools used for the simulations.

### A. WIRELESS POINT-TO-POINT NETWORKS

WLANs are based on the IEEE 802.11 standard [3]. The 802.11b standard operates in the 2.4-GHz license-free frequency band and provides data rates up to 11 Mbps. The new IEEE 802.11g and 802.11a operate in the 5-GHz license-free frequency band and provide data rates up to 54 Mbps. Commercial-off-the-shelf (COTS) PTP wireless systems [4] indicate a maximum of 4.5-Mbps data throughput. Most current systems are capable of supporting both 2.4 GHz and 5.8 GHz. Appendix A shows the spectrum allocation at various RF bands.

Wireless point-to-point configurations vary from simple two building structures, to more complex, multi-building infrastructure networks. In a typical wireless PTP or point-to-multipoint (PTM) infrastructure configuration, as shown in Figure 1, there exists one main consideration, the transmitting and receiving antenna placement. From the antenna, the signal is relayed into the building via a low loss RF cable into the local WLAN network. The typical distance of a line-of-sight (LOS) communication system varies from several hundred meters to tens of kilometers depending on several factors. Some of these factors include the gain of the antenna, the bridge performance, path loss, availability of a RF booster, etc.

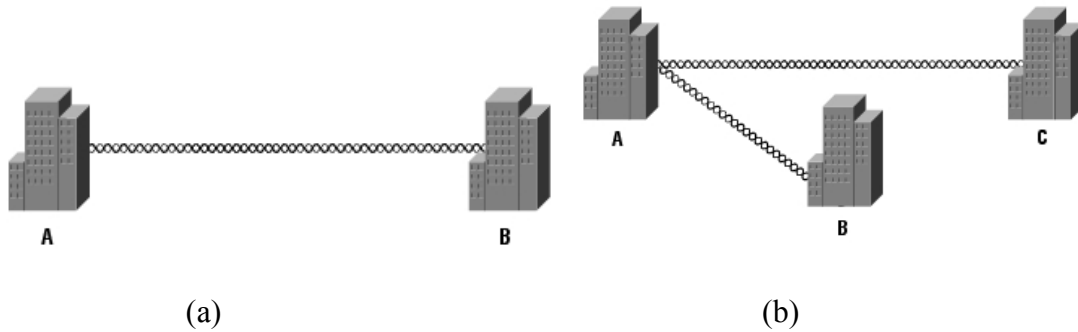


Figure 1. (a) Point-to-point (b) Point-to-multiple points (From Ref. [7].)

Receiver sensitivity is defined as the minimum signal power level (in dBm or mw) for the receiver to accurately decode a given signal. Typical receiver sensitivity is about  $-84$  dBm [2]. Depending on the various data rates, the WLAN receiver sensitivity may vary according to Table 1.

340 series client adapters	<ul style="list-style-type: none"> <li><math>-90</math> dBm at 1 Mbps</li> <li><math>-88</math> dBm at 2 Mbps</li> <li><math>-87</math> dBm at 5.5 Mbps</li> <li><math>-83</math> dBm at 11 Mbps</li> </ul>
350 series client adapters	<ul style="list-style-type: none"> <li><math>-94</math> dBm at 1 Mbps</li> <li><math>-91</math> dBm at 2 Mbps</li> <li><math>-89</math> dBm at 5.5 Mbps</li> <li><math>-85</math> dBm at 11 Mbps</li> </ul>
5-GHz client adapters	<ul style="list-style-type: none"> <li><math>-85</math> dBm at 6 Mbps</li> <li><math>-84</math> dBm at 9 Mbps</li> <li><math>-82</math> dBm at 12 Mbps</li> <li><math>-80</math> dBm at 18 Mbps</li> <li><math>-77</math> dBm at 24 Mbps</li> <li><math>-73</math> dBm at 36 Mbps</li> <li><math>-69</math> dBm at 48 Mbps</li> <li><math>-68</math> dBm at 54 Mbps</li> </ul>

Table 1. WLAN Receiver sensitivity (From Ref. [2].)

Some of the typical antennas used in PTP wireless systems include the dish antenna and the Yagi antenna. Line-of-sight is required in PTP systems and most commercial installations will take Fresnel zones into consideration.

## **B. TOOLS FOR PROPAGATION MODELING**

### **1. Geometric Optics**

At high frequencies, the geometrical optics approximation adequately describes wave propagation. In a homogeneous isotropic medium, the waves propagate in straight lines called rays and in an inhomogeneous isotropic medium the rays are curved. Geometrical optics (GO) describes the ray trajectories in the limit where changes in the properties of the medium are slowly varying in space [5].

The disadvantages of using simple GO techniques to predict field strength include the inability to predict field strength in the shadow region and handle flat or singly curved surfaces.

### **2. Geometrical Theory of Diffraction**

The geometrical theory of diffraction (GTD) was conceived to alleviate many of the problems associated with GO. The strongest diffracted fields arise from edges, but ones of lesser strength originate from point discontinuities such as tips and corners.

GO and GTD rays can be combined (e.g., reflected rays could subsequently become diffracted) to obtain the following combinations:

- Reflected then reflected (multiple reflection)
- Reflected then diffracted
- Diffracted then reflected
- Diffracted then diffracted (multiple diffraction).

An accurate (converged) solution must include all significant contributions. Figure 2 illustrates the combination of direct, reflected and transmitted waves in a wireless PTP communication scenario.

In order to achieve accurate prediction of the received signal, it is essential to model the reflection and diffraction coefficients of the material properties of the buildings. Diffractions from corners and edges are important in diverting signals into shadowed regions.

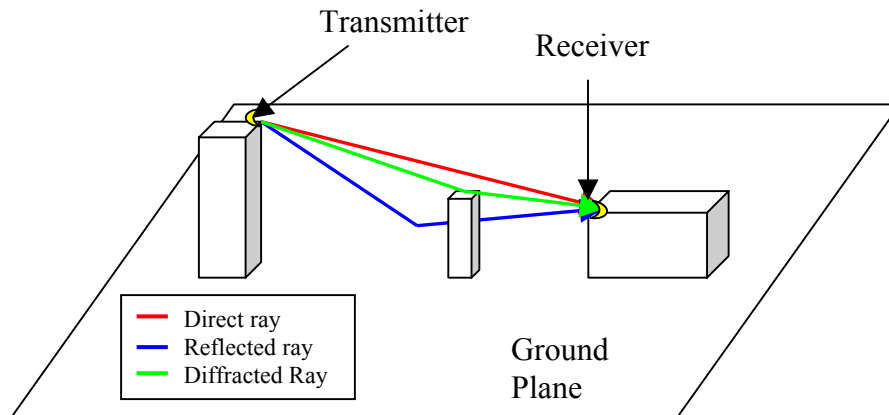


Figure 2. Illustration of the direct, reflected, transmitted and diffracted wave components

### 3. Urbana Wireless Toolset

The Science Applications International Corporation's (SAIC) **Urbana** toolset is a robust computational electromagnetic (CEM) tool for simulating wireless propagation and near-field radiation in complex environments. The toolset utilizes a ray tracing physics engine that aggregates GO and GTD to produce a high-fidelity 3-D simulation [6]. The number of contributing bounces can be varied by changing the *\*.ur\_input* file settings, as shown in Appendix A.

**Urbana** models wireless systems exhibiting frequency, spatial, and field polarization dependence. **Urbana** also allows the user to evaluate the effects of different materials. Its modeling tools allow analysis of spatial dependencies that arise from the physical complexity of the environment.

The **Urbana** toolset is a UNIX based toolset comprised of the following components:

1. **Cifer** – Build, modify, translate and change of building properties.
2. **Urbana** – Determine received power levels at specific points throughout an indoor structure or an external area.
3. **Xcell** – Used to visualize the facet models and the results of the propagation simulations of **Urbana**.

In conjunction to this toolset, a Matlab graphic user interface (GUI) was written as an aid. The building models are built using **cifer**. It is assumed that the size of the scattering objects is much larger than a wavelength, which is the case of 2.4 GHz, where the wavelength is 0.125 m. At each observation point generated from the GUI, **Urbana** computes the aggregate of multipath components reaching the specified point. The model includes the effects of angle of incidence, polarization, and material dielectric constant and antenna patterns. Predictions can also account for diffraction effects around corners, which is particularly significant for outdoor environments.

A Silicon Graphics Inc. (SGI) Octane computer with 1 GB of memory was used to run **Urbana**, **Cifer** and **Xcell**. The Matlab GUI was run on a typical desktop computer. The **Xcell** displays a 3-D model and perspective views of signal strengths in and around the building. The transmitting parameters were selected to accurately represent a commercially available 802.11a network system. The relationship between the suite of programs is illustrated in the flow chart shown in Figure 3.

This chapter presented the background research on wireless PTP systems and the tools for PTP propagation modeling. Chapter III discusses the aspects of the electromagnetic model applicable for wireless PTP systems.

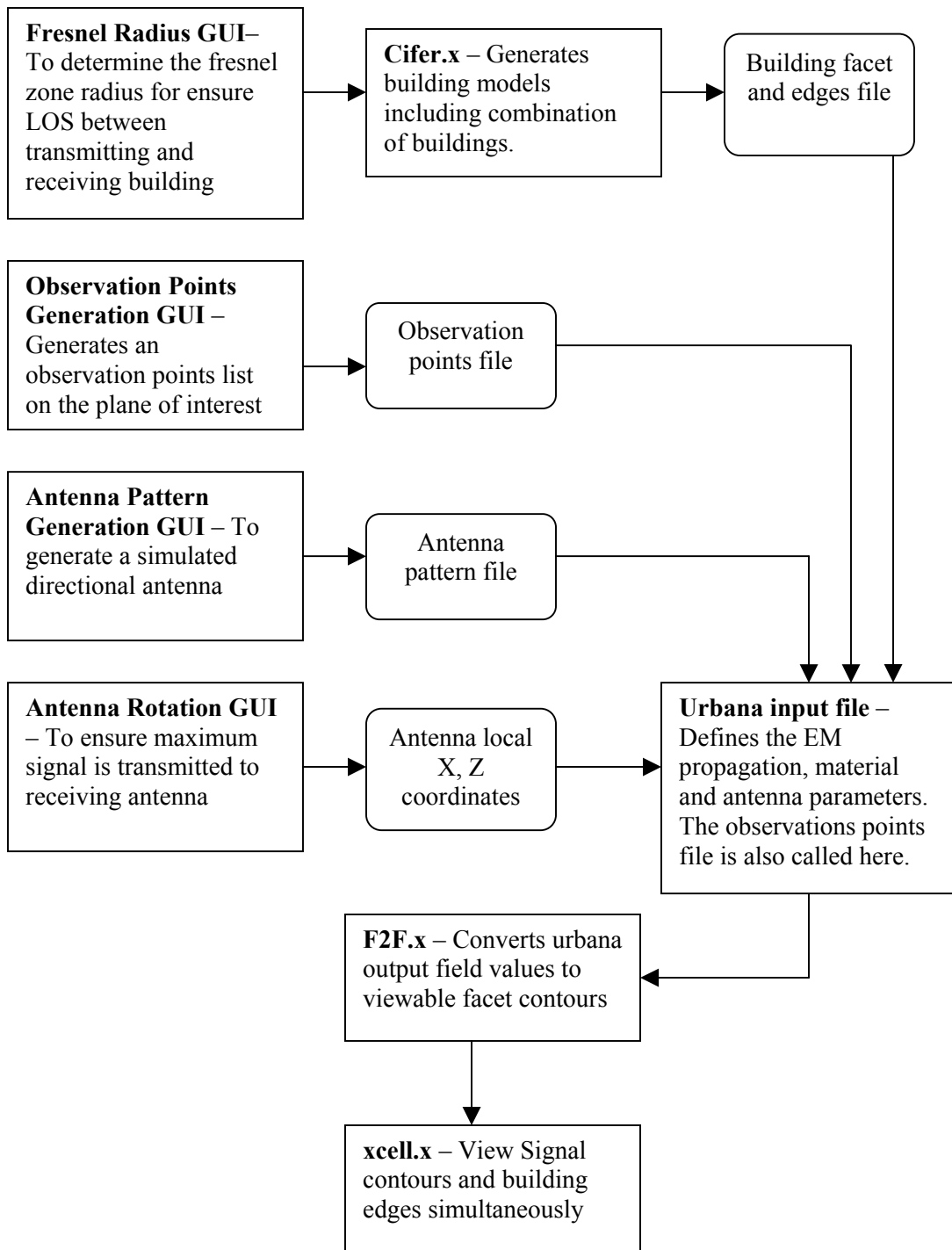


Figure 3. **Urbana** flow diagram

### III. ASPECTS OF THE ELECTROMAGNETIC MODEL

There are several electromagnetic issues pertaining to the performance of a wireless PTP system. This chapter will focus on several factors that affect the propagation behavior of the electromagnetic waves specific to wireless PTP communication systems. The topics discussed include radiation pattern of the antenna, Fresnel zones around the direct ray, path loss, multipath effects, and VSWR.

#### A. RADIATION PATTERNS

The radiation pattern of an antenna is a plot of the far-field radiation from the antenna. More specifically, it is a plot of the power radiated from an antenna per unit solid angle, or its radiation intensity  $I$  (in watts per unit solid angle). It is desirable that the pattern of a typical antenna used in wireless point-to-point communication systems be directional for several reasons. First, directional antennas have high gain, which yields a higher signal-to-noise ratio at a fixed distance. Secondly, a narrow beam reduces the probability of the signal being intercepted by unauthorized persons. High-gain antennas can be used because of the fixed point-to-point nature of the transmitter and receiver, and the fact that a clear LOS exists between them.

Some common parameters used to compare radiation patterns are [7]:

- The half-power beamwidth (HPBW)  $\theta_B$ , or just the beamwidth, is the angle subtended by the half-power points of the main lobe.
- The front-back-ratio is the ratio between the peak amplitudes of the main beam and back lobe, usually expressed in decibels.
- The sidelobe level is the amplitude of the biggest sidelobe, usually expressed in decibels relative to the peak of the main lobe.
- Gain or directivity describes the RF power relative to an isotropic transmitter. There is an inverse relationship between beamwidth and gain.

## 1. Simulation of a PTP Antenna Using a Uniform Circular Aperture

A widely used microwave antenna is the circular aperture (e.g., satellite dish). One of the attractive features of this configuration is its simplicity in construction. In addition, closed-form expressions for the fields of all the modes that exist over the aperture can be obtained [5].

A uniform circular aperture is one that has constant amplitude distribution. The half-power beamwidth for  $a \gg \lambda$  is given by  $HPBW = 58.4(\lambda/2a)$  degrees where  $a$  is the antenna aperture radius and  $\lambda$  is the wavelength (meters). The first side lobe level of any uniform circular aperture is 17.6 dB. The directivity is given by  $D_u = 4\pi^2 a^2 / \lambda^2$  [7].

Using the equivalent magnetic current formulation where  $\vec{E}$ , the far field of the aperture, is [7]

$$\vec{E}(r, \theta) = \hat{p} E_o \pi a^2 j \beta \frac{e^{-j\beta r}}{2\pi r} f(\theta) \quad [3.1]$$

where it has been assumed that the field in the aperture is  $\vec{E}_a = E_o \hat{x}$ ,  $\beta = 2\pi/\lambda$  and  $\hat{p} = (\hat{\theta} \cos \phi - \hat{\phi} \sin \phi \cos \theta)$  is the polarization unit vector. The pattern function for the circular aperture is

$$f(\theta) = \frac{2J_1(\beta a \sin \theta)}{\beta a \sin \theta} \quad [3.2]$$

where  $J_1$  is the Bessel function of the first kind with order 1.

Due to the circular symmetry of the aperture distribution,  $f(\theta)$  is independent of  $\phi$ . In the  $E$ -plane,  $\phi = 0^\circ$  and  $\hat{p} = \hat{\theta}$ . This means that  $f(\theta)$  represents the  $E_\theta$  component. The above expressions were implemented in Matlab and the codes can be found in Appendix B. Figure 4 shows the calculated radiation pattern of a uniform circular aperture ( $a = 0.24$  m) at 2.4 GHz.

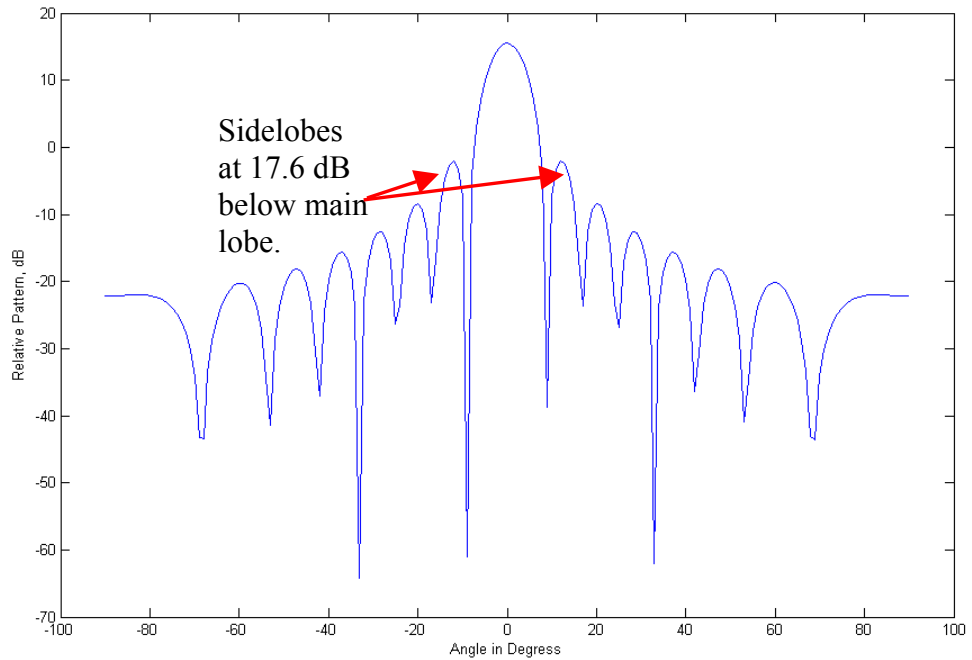


Figure 4. Radiation pattern of a 7.5°-HPBW, 2.4-GHz antenna

## 2. Antenna Rotation

In a typical wireless PTP communication system, the antenna is rotated or tilted on top of the building to ensure maximum power is transferred to the receiving antenna. As such, a series of transformations has to be performed to obtain the required relationship between the local and global coordinate variables and their unit vectors before passing the parameters to **Urbana**.

The global coordinates are given by  $(x, y, z)$  and the local coordinates are  $(x'', y'', z'')$ . The double primed variables can be obtained by a series of two rotations of the global coordinate variables. The first rotation is about the  $z$ -axis by an angle  $\alpha$  and the second rotation is about the  $y$ -axis by an angle  $\beta$  [8]. Figure 6 shows the local coordinate system and the different parameters used in the calculations.

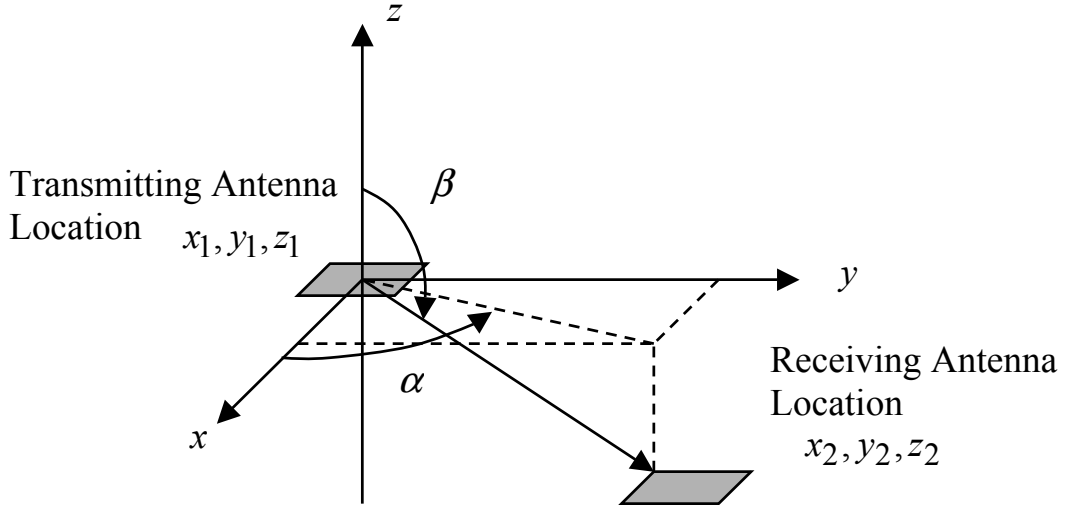


Figure 5. Antenna coordinates system

Define the following variables:

$$\Delta x = x_2 - x_1, \Delta y = y_2 - y_1, \Delta z = z_2 - z_1 \quad [3.3]$$

$$\alpha = \tan^{-1} \left( \frac{\Delta y}{\Delta x} \right) \quad [3.4]$$

$$\beta = \frac{\pi}{2} - \tan^{-1} \left( \frac{\Delta z}{\sqrt{\Delta x^2 + \Delta y^2}} \right). \quad [3.5]$$

The transformation matrices are determined from geometry and are given by

$$\begin{bmatrix} \hat{x}' \\ \hat{y}' \\ \hat{z}' \end{bmatrix} = \begin{bmatrix} \cos \alpha & \sin \alpha & 0 \\ -\sin \alpha & \cos \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \hat{x} \\ \hat{y} \\ \hat{z} \end{bmatrix} \quad [3.6]$$

$$\begin{bmatrix} \hat{x}'' \\ \hat{y}'' \\ \hat{z}'' \end{bmatrix} = \begin{bmatrix} \cos \beta & 0 & -\sin \beta \\ 0 & 1 & 0 \\ \sin \beta & 0 & \cos \beta \end{bmatrix} \begin{bmatrix} \hat{x}' \\ \hat{y}' \\ \hat{z}' \end{bmatrix}. \quad [3.7]$$

Using the transformation matrices in Equations [3.6] and [3.7], the unit vectors are

$$\begin{bmatrix} \hat{x}'' \\ \hat{y}'' \\ \hat{z}'' \end{bmatrix} = \begin{bmatrix} \cos \beta & 0 & -\sin \beta \\ 0 & 1 & 0 \\ \sin \beta & 0 & \cos \beta \end{bmatrix} \begin{bmatrix} \cos \alpha & \sin \alpha & 0 \\ -\sin \alpha & \cos \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \hat{x}' \\ \hat{y}' \\ \hat{z}' \end{bmatrix}. \quad [3.8]$$

An antenna rotation Matlab GUI based on the Equations [3.3] to [3.8] was written to assist the user in determining the transformation.

## B. FRESNEL ZONES

Wireless point-to-point communication utilizes LOS to obtain maximum possible signal transmission. As such, Fresnel zones must be taken into consideration. Fresnel zones can be thought of as reflecting surfaces that gives alternating constructive and destructive interference. Figure 6 illustrates the effects of the Fresnel zone clearance. Contributions within the first zone are all in phase, so any obstructions that do not enter this zone will have little effect on the received signal. The Fresnel zone radius [7] is

$$r_n \approx \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}} \quad [3.9]$$

where  $d_1$  = transmitter direct path to the point where  $r_n$  is measured, meters

$d_2$  = receiver direct path to the point where  $r_n$  is measured, meters

$r_n$  = radius of the  $n^{\text{th}}$  zone, meters

$n$  = Fresnel zone number

$\lambda$  = wavelength, meters

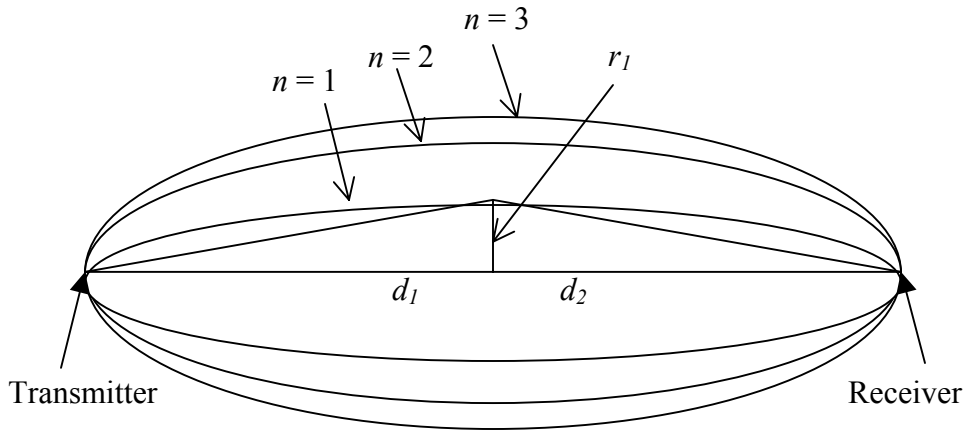


Figure 6. Fresnel zones

This clearance is often used as a criterion to decide whether an object is to be treated as a significant obstruction. If  $0.6r_1$  is kept clear then the total path attenuation will be practically the same as in the unobstructed case.

As shown in Figure 7, objects closer than  $0.6r_1$  from the LOS path are potential obstructions. An approximate formula [9] for calculating the minimum height clearance when setting up the link geometry is

$$r \text{ [ft]} = 43.3 \left( \frac{d}{4f} \right) (0.6) \quad [3.10]$$

where  $d$  is distance in nautical miles, and  $f$  is the frequency in GHz.

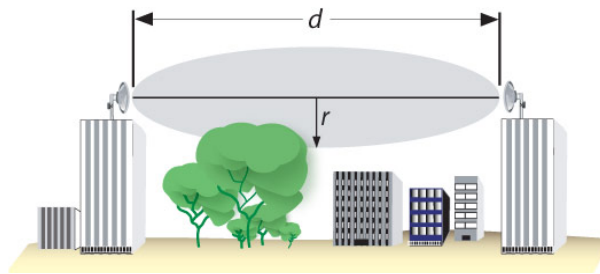


Figure 7. Approximate Fresnel zone clearance (From Ref. [9].)

### C. PATH LOSS

The most basic and predictable propagation mechanism is the unobstructed free space path loss. Quite simply, as electromagnetic signals propagate, they are attenuated due to spherical wave spreading of the power. The free space propagation loss factor in dB is defined by

$$L_p(\text{dB}) = 20 \log\left(\frac{4\pi d}{\lambda}\right) \quad [3.11]$$

where  $\lambda$  is the free space wavelength and  $d$  is the distance from source. Based upon this formula, some typical path loss values are computed for various wireless frequencies and listed in Table 2 [10]. The Matlab codes are appended in Appendix B.

Frequency \ Distance	915 MHz	1920 MHz	2.45 GHz	5.78 GHz
0.1 km	71.68	78.11	80.23	87.70
0.2 km	77.69	84.13	86.25	93.72
1 km	91.68	98.11	100.23	107.7
2 km	97.69	104.13	106.25	113.72
10 km	116.67	118.11	120.23	127.70

Table 2. Distance versus path loss (dB) for typical wireless frequencies (Ref. [10].)

The power received  $P_r$  out of a receiver antenna with gain  $G_r$  at a range  $d$  from a transmit antenna with gain  $G_t$  is given by the Friis equation [7]

$$P_r = \frac{P_t G_t G_r}{L_p} \quad [3.12]$$

where  $P_t$  is the transmit power. By the reciprocity theorem the same result will be obtained when the transmitter and receiver locations are interchanged. Figure 8 shows the distance versus path loss for frequency of 2.4 GHz.

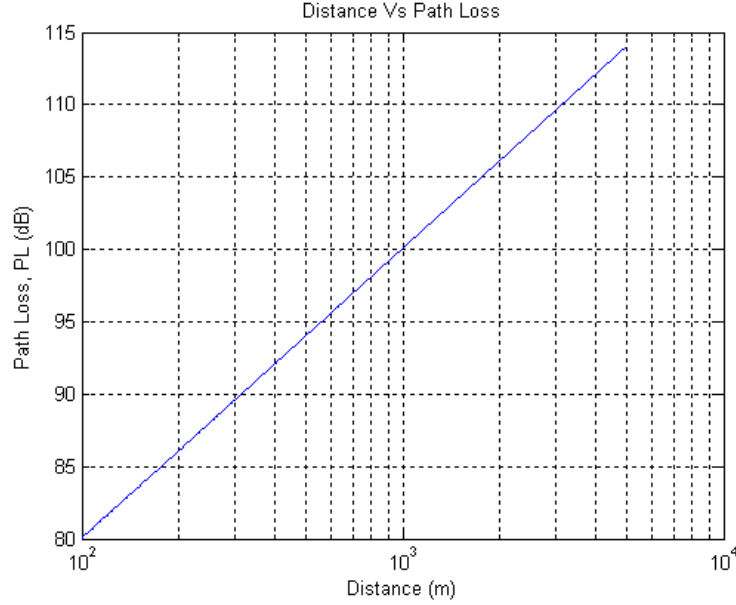


Figure 8. Distance versus path loss for frequency of 2.4 GHz

For a hypothetical scenario, the path loss was computed using the Friis equation in dB form.

$$L_p \text{ (dB)} = 20 \log\left(\frac{4\pi}{\lambda}\right) + 20 \log(d) - G_t \text{ (dBi)} - G_r \text{ (dBi)} \quad [3.13]$$

If the two antenna gains are not specified, it is assumed that they are 0 dBi. At 2 km using a frequency of 2.4 GHz gives  $L_p \text{ (dB)} \approx 106$  dB. The received power in dBm is computed using  $P_r \text{ (dBm)} = P_t \text{ (dBm)} - L_p \text{ (dB)}$ . Since  $P_t = 1 \text{ W} = 30 \text{ dBm}$ , then  $P_r \text{ (dBm)} = 30 - 106.07 \approx -76 \text{ dBm}$ .

Assuming the receiver has a sensitivity of  $-70.07 \text{ dBm}$ , the transmitting antenna would require a gain of approximately  $-6 \text{ dB}$ . The above scenario is not completely realistic; one needs to take into account fading, cable and connector losses and filter insertion loss.

## 1. Effective Isotropic Radiated Power

The effective isotropic radiated power (EIRP) refers to the product  $P_t G_t$  where  $P_t$  is the power into the antenna [2]. EIRP is rated in either dBm or Watts. EIRP is the value that regulatory agencies such as the FCC or European Telecommunications Standards Institute (ETSI) use to determine and measure power limits in applications such as 2.4-GHz wireless equipment. EIRP is calculated by adding the transmitter power (in dBm) to antenna gain (in dBi) and subtracting any cable losses (in dB). Table 3 is a sample calculation of EIRP. The cable and connector losses are accounted for in the **Urbana** by adjusting the transmit power.

Part	Cisco Part Number	Power
A Cisco Aironet Bridge	AIR-BR350-A-K9	20 dBm
that uses a 50 foot antenna cable	AIR-CAB050LL-R	3.35 dB loss
and a solid dish antenna	AIR-ANT3338	21 dBi gain
has an EIRP of		37.65 dBm

Table 3. Typical wireless PTP system EIRP (From Ref. [2].)

## D. MULTIPATH DISTORTION

When an RF signal has more than one possible path between a transmitter and receiver, multipath interference [2] may occur. This occurrence is particularly strong in regions that have a large amount of metallic or other RF reflective surfaces.

The multiple signals combine in the receiving antenna and they will cause distortion of the signal as shown in Figure 9. Multipath interference can cause the energy at the antenna to be higher or lower than the free space value depending on whether constructive or destructive interference occurs. Multipath also leads to dispersion that causes interference. Changing the type of antenna and its location can help reduce multipath interference.

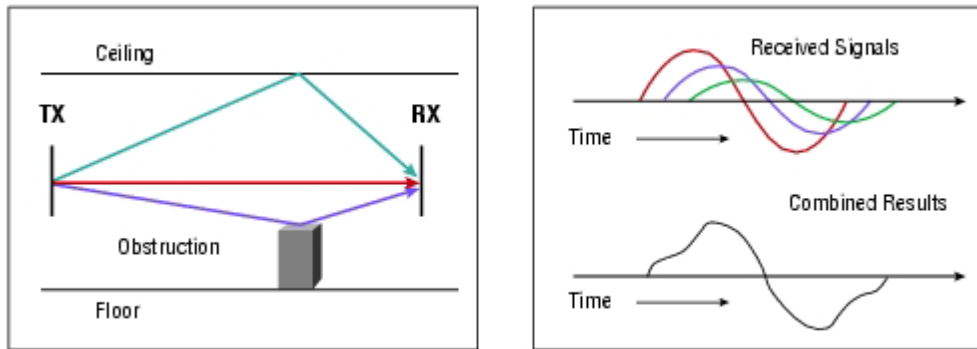


Figure 9. Distortion of signal caused by multipath inside a building (From Ref. [2].)

The position of either one of the antennas may be adjusted to move the reflection point so that it is blocked by an obstruction or strikes an uneven surface. In Figure 10, the height of the transmitting antenna has been reduced so that the reflected signal is dispersed by rocky terrain before hitting the smooth water surface. This method is effective if the reflection point is fixed.

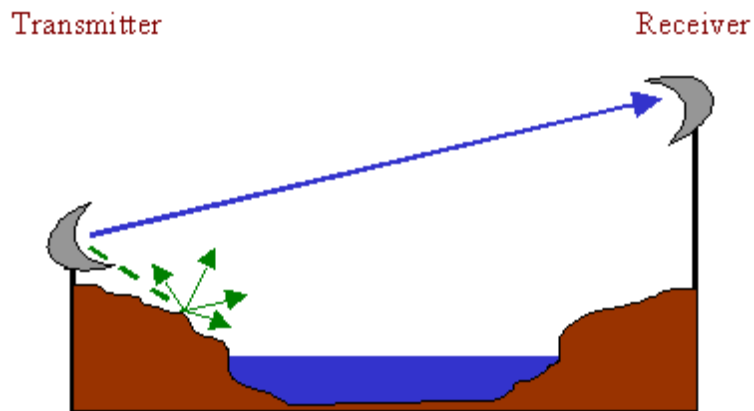


Figure 10. Transmitting antenna height reduced to avoid reflections (From Ref. [11].)

### E. VSWR AND RETURN LOSS

Voltage standing wave ratio, or VSWR, is a measure of the degree to which a perfect match exists between two microwave devices. Thus, the lower the VSWR, the better the match, and the more efficient the power transfer. A practical maximum VSWR

is 1.5:1 as seen in Appendix A for typical directional antennas. Obtaining values below this is proportionately more expensive, and may not be economically justified [12].

In wireless communication systems, VSWR is relatively easy to measure, and may be measured at any convenient point along the line such as at connector interfaces. Measuring the VSWR at the transceiver output port, looking towards the antenna, provides a composite reading. This reading is in fact determined by the distributed VSWRs of the various components that are present in the path. The return loss is a dB

measure of the VSWR and is given by  $RL(\text{dB}) = 20 \log \left( \frac{VSWR + 1}{VSWR - 1} \right)$ .

As shown in Figure 11, as VSWR decreases, the return loss becomes a more sensitive measure of transmission line performance than VSWR. Thus, a VSWR change of 1.1 to 1.5 is equivalent to a return loss change of from 26.4 to 13.9, or approximately 13 dB. The Matlab codes are included in the Appendix B.

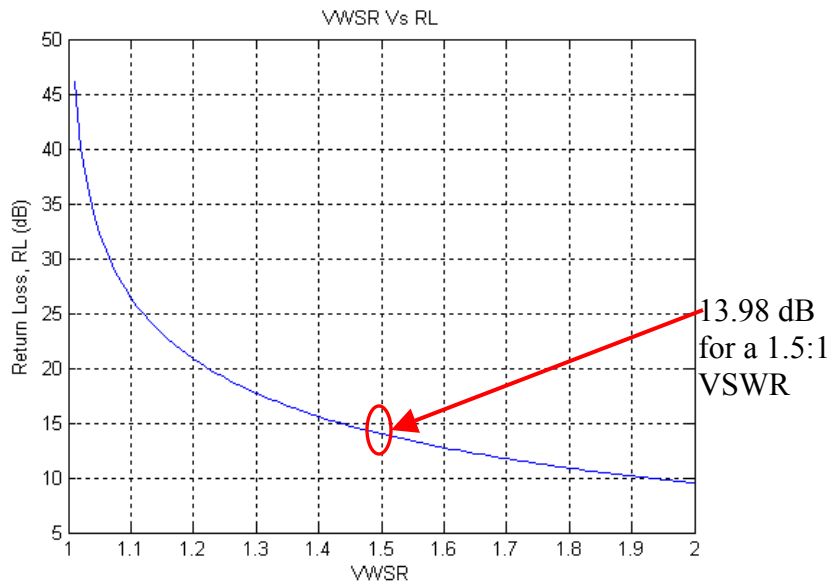


Figure 11. VSWR versus Return Loss

## F. OTHER THEORETICAL CONSIDERATIONS

Other high frequency techniques include physical optics (PO), which is similar to GO except that it is a current based method rather than ray based. The physical theory of diffraction (PTD) represents edge-diffracted fields in terms of edge currents. Both methods (GO/GTD and PO/PTD) give identical results in the limit of  $\lambda \rightarrow 0$ . However, GO/GTD is generally faster when there are only a few major contributions to the total signal. **Urbana** is capable of using PO/PTD; however, for all simulations GO and GTD were used.

The following chapter examines the radiation patterns of a simulated directional PTP antenna and how diffraction and reflection affect propagation within a building.

## IV. URBANA TEST SIMULATIONS

In this chapter, a flat planar surface was used to simulate a perfect electric conducting (PEC) ground, and a uniform circular transmitting antenna was designed to create a simple scattering model. To create the model and generate the field contours, the process outlined in Figure 3 of Chapter II is used. The simple geometry is used to illustrate the signal contours of the transmitting antenna. General antenna information can be found in Chapter IV. The following, in chronological order, highlights the steps involved in generation of a simulated directional antenna model.

### A. INPUT DATA GENERATION

#### 1. Creation of a Directional Antenna Pattern

One type of commercially available directional antenna found in wireless PTP systems is the Uda-Yagi antenna (or simply the Yagi antenna). Several other antennas found in wireless PTP are listed in Appendix A. Most of these antennas can be approximated by an equivalent uniform circular antenna of appropriate radius. The Matlab code is as shown in Appendix B and a Matlab GUI was written to enhance ease of use as shown in Figures 12 and 13. The antenna pattern generation GUI lets the user define the half-power beamwidth (HPBW) and the frequency of the antenna. Once the program is executed, a pattern file is generated and saved for use in **Urbana**. More on this topic can be found in Chapter II. For this simulation, the HPBW was selected to be  $15^\circ$  and the frequency was 2.4-GHz.

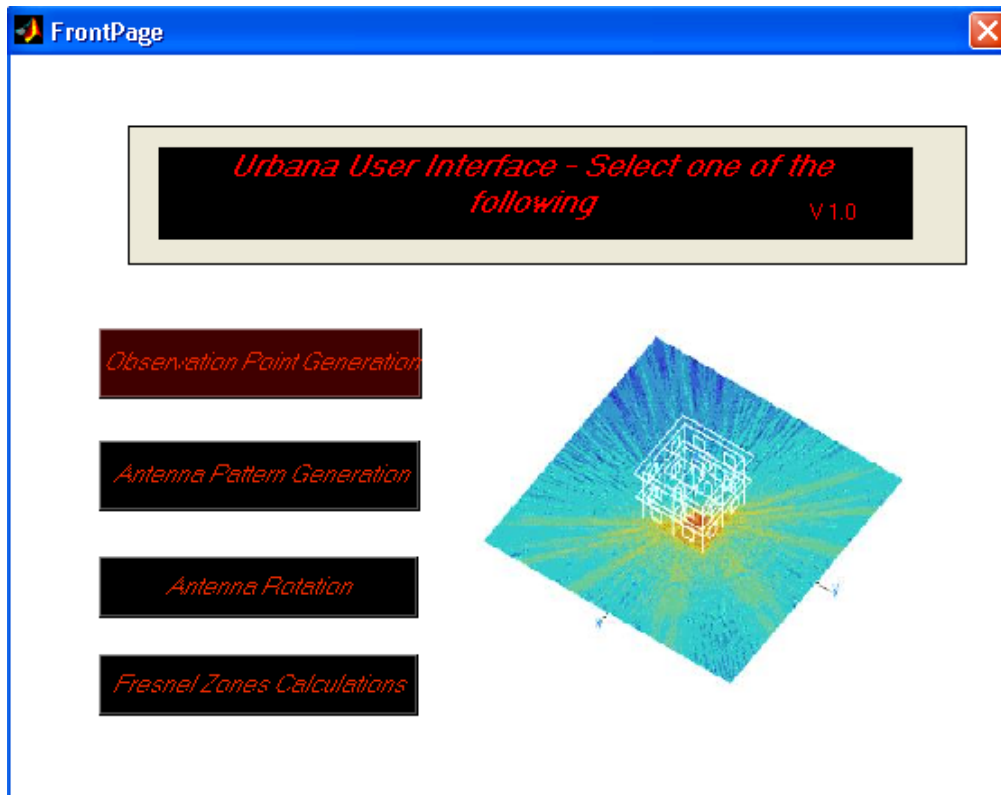


Figure 12. Main GUI interface page

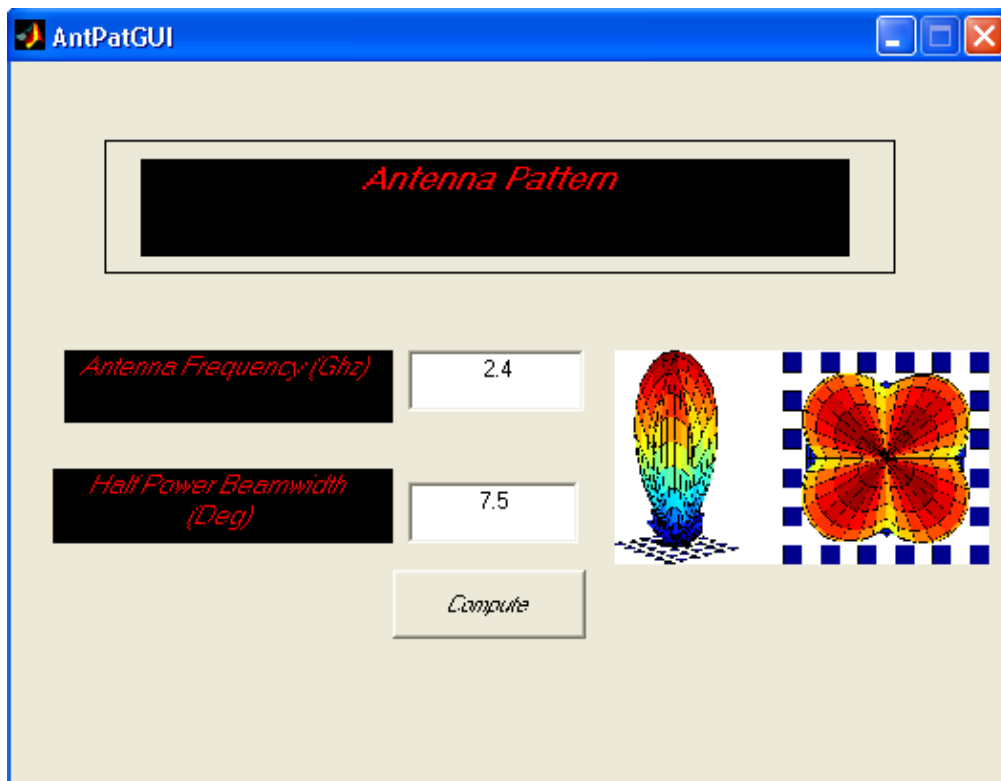


Figure 13. Antenna pattern generation GUI

## 2. Creating the Geometry Facets

The **Urbana** toolset represents physical objects by triangular facets. The faceted models can be generated in CAD software, but for simple objects, such as rectangular building blocks, the **cifer** GUI can be used. Using the **cifer** “Facet Editor” menu, simple shapes such as curves, boxes and planes can be built. This suits the purpose of modeling a simple rectangular building.

In this model (Figure 14), there are two major components, the ground plane and an antenna. The X-axis and Y-axis ground extended from  $-100$  m to  $100$  m and  $-100$  m to  $240$  m, respectively. The antenna is centered at  $(0, -70, 16)$ .

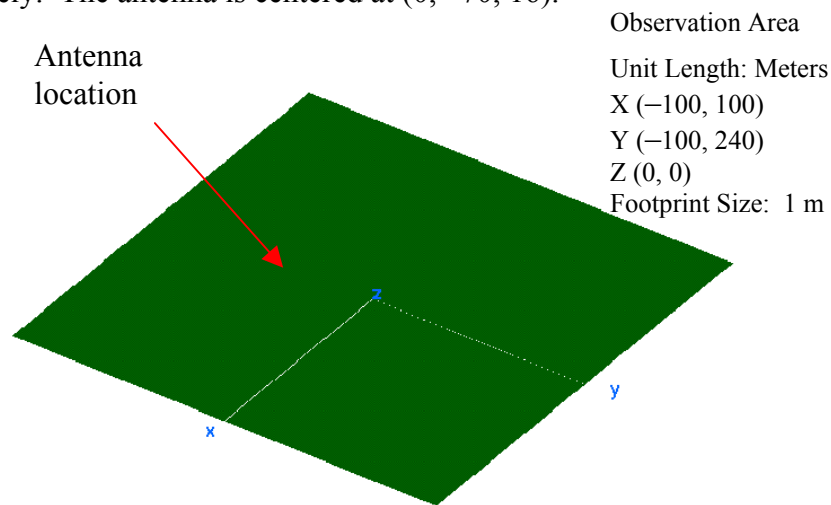


Figure 14. Ground plane facet

The material characteristics for each of the facets are specified by the coating material and are defined by the input variable ICOAT. For this case, the ground plane was assigned as a PEC. Each facet has a material variable that describes the type of material, as defined in a master list of material properties. Sumagasay [13] explains some of the different material compositions and how **Urbana** calculates the diffraction and attenuation of walls. In this model, the ground plane had  $\text{ICOAT} = 0$ .

## 3. Creating Observation Points

In order to effectively observe the antenna patterns, a grid of observation points needs to be set up over the area of interest (AOI). For this model, the observation area of

interest has the same dimensions as the ground plane. For the purpose of investigating the electromagnetic contours at different heights, a Matlab GUI was written as shown in Figure 15.

The  $X_{min}$ ,  $X_{max}$ ,  $Y_{min}$ ,  $Y_{max}$  inputs let the user define the exact size of the observation plane while the  $Z_{Offset}$  input defines the height of the plane with reference to the global coordinates. The  $Foot\ Print\ Size$  input lets the user defines the size of the observation cell.

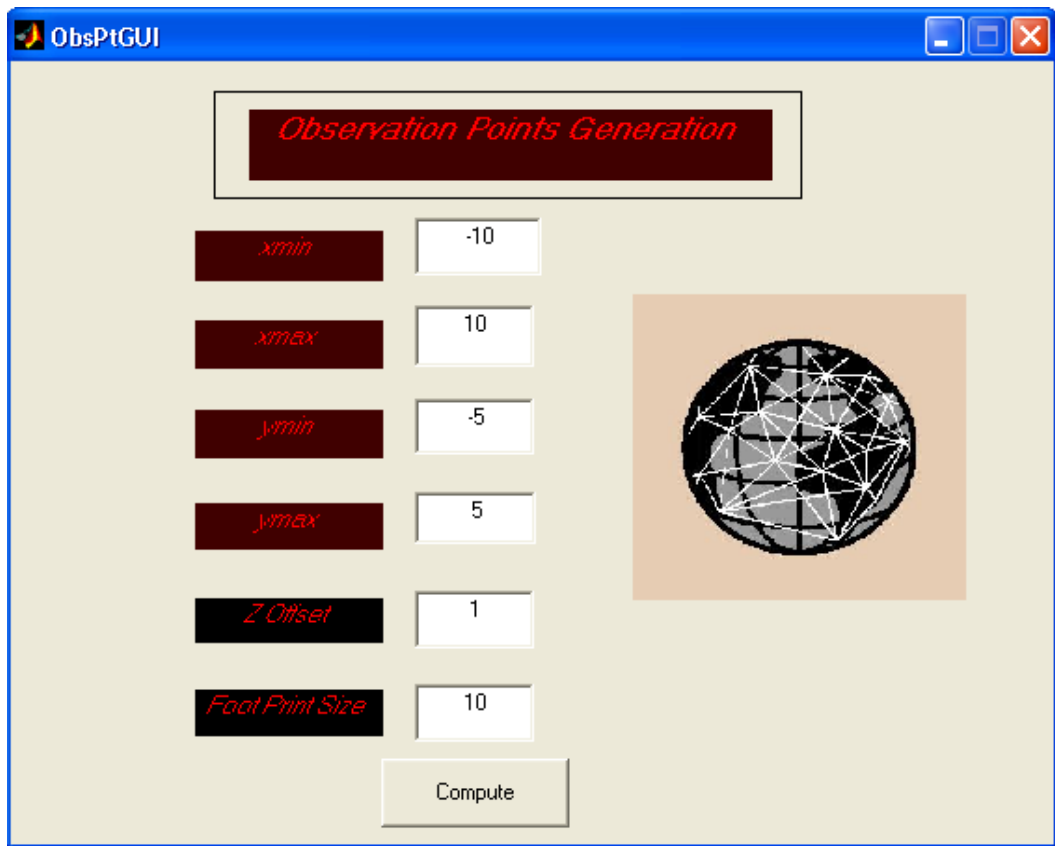


Figure 15. Observation point generation

Once all the inputs are specified, the observation point generation program is executed, and an observation list file is created and saved. The antenna pattern file and the observation point file can then be input to **Urbana** upon execution. The Matlab GUI program code is shown in Appendix B.

## B. INPUT FILE GENERATION AND EXECUTING URBANA

Using the **Urbana** input file (*gnd\_plane.ur\_input*), which consists of ASCII text with a specific set of input code words, the software **Urbana** then calculates and plots the field file. Table 4 lists some of the parameters specified in the **Urbana** input file.

INPUT PARAMETER	VALUES/OPTION
Facet Model	<i>gnd_plane.facet</i>
Length Unit	meters
Frequency	2.4 GHz
Antenna Description	By File: <i>dummy.antenna</i>
Antenna Type	Pattern File: Circular
Antenna Origin	0.0, -70.0, 5.0
Antenna local coordinates	X(1,0,0), Z(0,0,1)
Observation Points	<i>gnd_plane.list</i> (FTP from Matlab GUI)
Rx Antenna	No (Saving of *.couple file)
Computation Method	GO (geometric optics)
Edge Diffraction	No (UTD)
Edge Model	<i>dummy.edge</i>
Ray Spacing	2.0 degree
Max Bounces	5
Materials	ICOAT = 0 (perfectly electric conducting material)
ADVANCED FEATURES	SWITCHED OFF

Table 4. Important **Urbana** Input Parameters

## C. DISPLAYING RESULTS

There are two steps involved in displaying the field contours:

1. By utilizing the *f2f.x* (field to facet) program, the computational results are translated into a color-coded facet file that can be viewed in **XCell**. In this step, the **Urbana** output file (*gnd\_plane.field*) was used to create the output facet file for visualizing the transmitted signal levels. The program *f2f.x* requires the user to input the data as shown in Table 5.

REQUIRED INPUT	RESPONSE
Type of E-Field	Magnitude of E-Tot
Number of Field Files	1
Name of Field File	<i>gnd_plane.field</i>
Antenna Scale Level	1
Histogram Interval	10 dB
Max and Min Clip values	-5 dBm, -75 dBm
Max and Min Range values	-5 dBm, -75 dBm
Number of Levels	25
Lowest Coating Code	1
Name of Output Facet File	<i>Gnd_output.facet</i>
Side of Footprint Square	1 (meters)
Shift according to Z-data	Y
Enter z-offset footprint	0

Table 5. Inputs For Running *f2f.x*

2. The second step requires the created file *gnd\_output.facet* to be loaded into **XCell** with the following steps.

**Run XCell**

Load a preference file (from **Xcell** menu): *ncsa\_white.xedge\_pref*

Load the field output facet (from **Xcell** menu): *gnd\_plane.facet*

The displayed data consists of the color-coded power contours of signal strength. Figure 16 shows the contours for the data in Table 6, from a transmitting 2.4-GHz uniform circular antenna. The plot shows the antenna pattern on the PEC ground plane. Recall that this antenna was placed at a height of 16 m off of the ground, thus explaining the contours shown. The high intensity regions where the ground intercepts the main beam and sidelobes are evident.

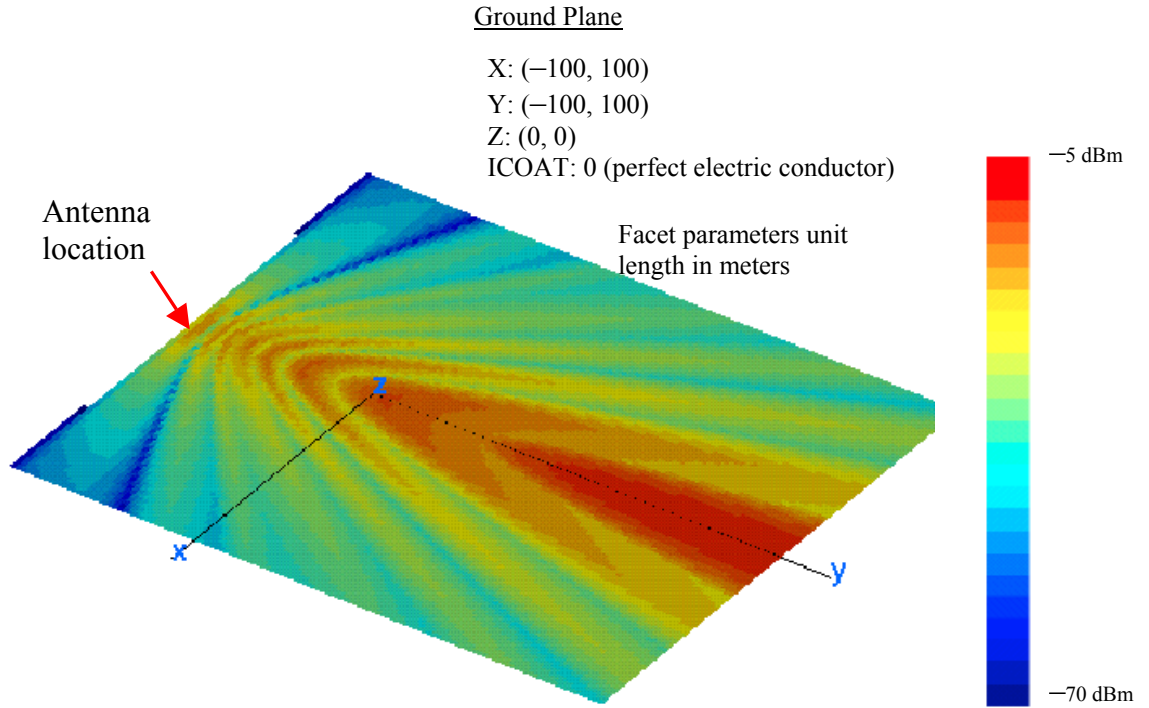


Figure 16. Ground plane with transmitting antenna signal contour for input data shown in Table 4

<p>Ground Plane</p> <p>X: (-100, 100)          Y: (-100, 100)          Z: (0, 0)          ICOAT = 0 (PEC)</p>	<p>Antenna</p> <p>Position: X = 0, Y = -70, Z= 5          Power: 30 dBm          Type: Pattern File          Frequency: 2.4 GHz</p>
<p>Observation Area</p> <p>X (-100, 100)          Y (-100, 100)          Z (0)</p>	<p>Facet Color Observation</p> <p>Range Min: -70 dBm          Range Max: -5 dBm          # Levels: 25          Lowest Coating Code: 1          Sample Footprint: 5</p>
<p>Footprint Size: 1m</p>	<p>Unit Length: Meters</p>

Table 6. Data for the antenna pattern test case results of Figure 16

#### D. VARIATIONS OF THE GROUND PLANE TEST CASE

Changes to the observation plane illustrate some important features of the radiation pattern behavior of the antenna. In this section, the observation plane was raised to observe the changes in signal levels. Figure 17 shows the contours for the data in Table 7. The radiation pattern is at a 7-m offset from the ground. As expected, since the observation plane was raised, the signal strength has increased as compared to Figure 16. The beamwidth is also narrower due to the raising of the observation plane.

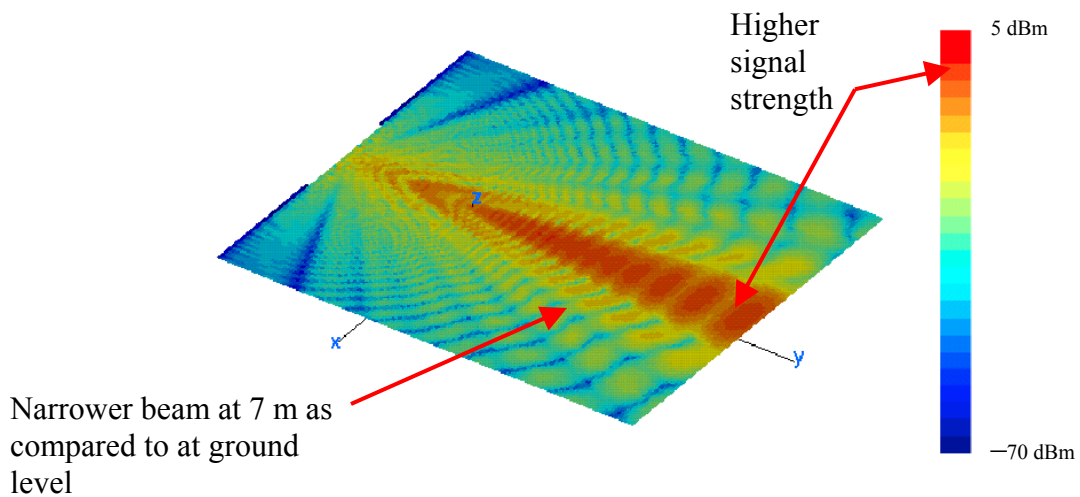


Figure 17. Radiation pattern at 7 m

<b>Ground Plane</b> X: (-100, 100) Y: (-100, 100) Z: (0, 0) ICOAT = 0 (PEC)	<b>Antenna</b> Position: X = 0, Y = -70, Z = 5 Power: 30 dBm Type: Dipole Frequency: 2.4 GHz
<b>Observation Area</b> X (-100, 100) Y (-100, 100) Z (7)	<b>Facet Color Observation</b> Range Min: -70 dBm Range Max: 5 dBm # Levels: 25 Lowest Coating Code: 1 Sample Footprint: 1
<b>Footprint Size: 1 m</b>	<b>Unit Length: Meters</b>

Table 7. Data for the antenna pattern test case results of Figure 17

Next the **Urbana** input file was modified to examine the antenna power at its transmitting level of 16 m and the HPBW was changed to  $7.5^\circ$ . The geometry facet model used was the same *gnd\_plane.facet* file. The field contours are as shown in Figure 18, and the input parameters are shown in Table 8.

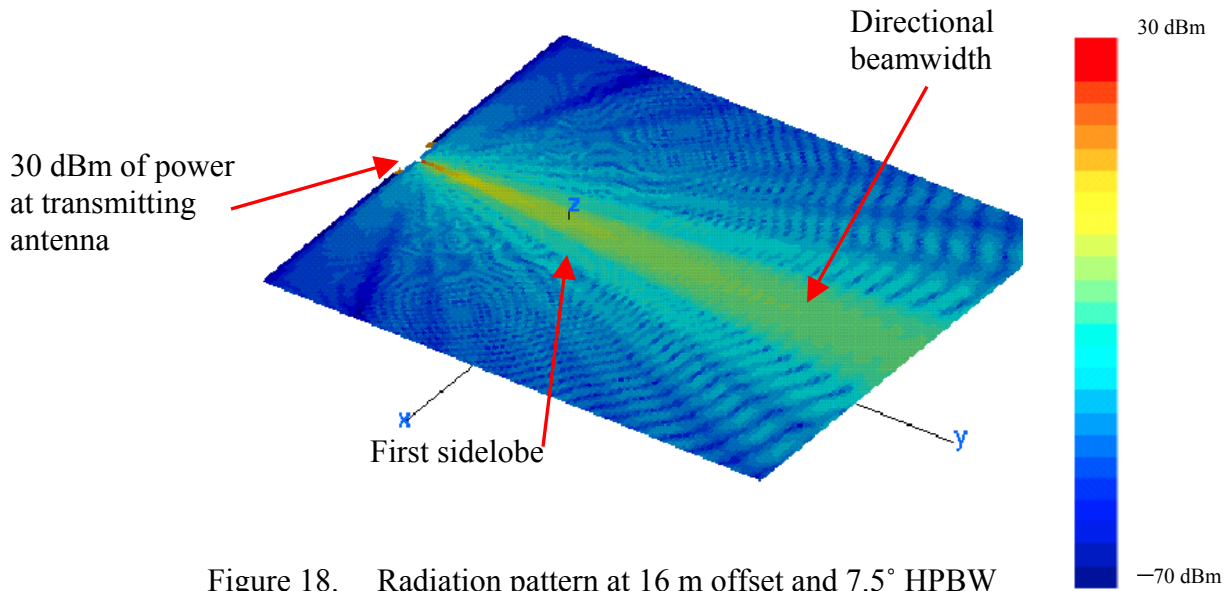


Figure 18. Radiation pattern at 16 m offset and  $7.5^\circ$  HPBW

Ground Plane X: (-100, 100) Y: (-100, 240) Z: (0, 0) ICOAT = 0 (PEC)	Antenna Position: X = 0, Y = 20, Z = 5 Power: 30 dBm Type: Dipole Frequency: 2.4 GHz
Observation Area X (-100, 100) Y (-100, 100) Z (16)	Facet Color Observation Range Min: -80 dBm Range Max: 30 dBm # Levels: 25 Lowest Coating Code: 1 Sample Footprint: 1
Footprint Size: 1 m	Unit Length: Meters

Table 8. Data for the antenna pattern test case results of Figure 18

Next, the effects of scattering by a single building were investigated. In particular, the effects of the building diffraction were explored. The building was selected to have absorbing facets, which means that the direct rays from the transmitting antenna would be

absorbed, and only diffracted rays would appear in the contours. Diffraction caused by the building edges below the antenna is evident, as shown in Figure 19. The input parameters are shown in Table 9.

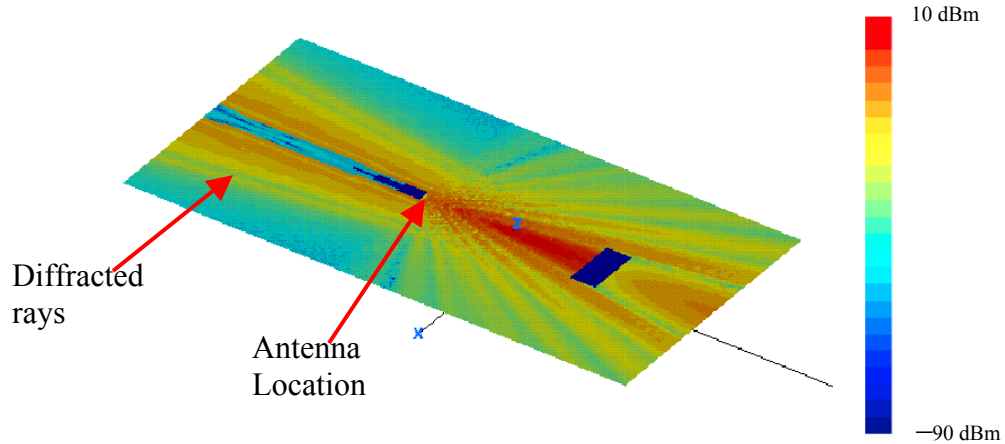


Figure 19. Antenna radiation pattern in the presence of a building with absorbing facets

<b>Ground Plane</b> X: (-100, 100) Y: (-100, 100) Z: (0, 0) ICOAT = 0 (PEC)	<b>Antenna</b> Position: X = 0, Y = -25, Z = 5 Power: 30 dBm Type: Dipole Frequency: 2.4 GHz
<b>Building 1</b> X: (25, -25) Y: (50, 80) Z: (0, 16) ICOAT = 1 (Concrete)	<b>RF Observation</b> Min Power: -90 dBm Max Power: -10 dBm Histogram Interval: 5 dB Clip Min: -90 dBm
<b>Observation Area</b> X (-100, 100) Y (-100, 100) Z (5)	<b>Facet Color Observation</b> Range Min: -90 dBm Range Max: 10 dBm # Levels: 25 Lowest Coating Code: 1 Sample Footprint: 1
<b>Footprint Size: 1 m</b>	<b>Unit Length: Meters</b>

Table 9. Data for the results of Figure 19

A second test was performed using two buildings, the second in the LOS of the first. Using the *Cifer.x* program, the second building was created. The new building's

height was fixed at 10 m, and the observation plane was taken at 5 m. The fields are shown in Figure 20. The field plot for the buildings coated with absorbing facets and there were no reflected rays can be seen in the region between the buildings. The input parameters are shown in Table 10.

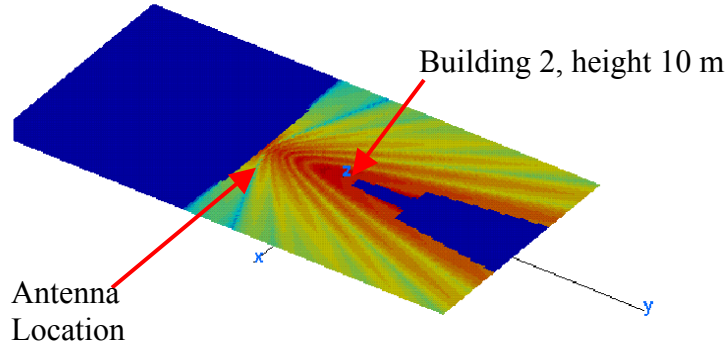


Figure 20. Two antennas with input data shown in Table 10

<b>Ground Plane</b> X: (-100, 100) Y: (-100, 100) Z: (0, 0) ICOAT = 0 (PEC)	<b>Antenna</b> Position 1: X = 0, Y = -25, Z = 5 Position 2: X = 0, Y = 20, Z = 5 Power: 30 dBm Type: Dipole Frequency: 2.4 GHz
<b>Building #1</b> X: (25, -25) Y: (0, 0) Z: (0, 25) ICOAT = 888 (Absorbing Facets) <b>Building #2</b> X: (25, -25) Y: (0, 0) Z: (0, 10) ICOAT = 888 (Absorbing Facets)	<b>RF Observation</b> Min Power: -66.8 dBm Max Power: 7.53 dBm Histogram Interval: 5 dB Clip Min: -80 dBm <b>Facet Color Observation</b> Range Min: -80 dBm Range Max: 10 dBm # Levels: 25 Lowest Coating Code: 1
<b>Observation Area</b> X (-100, 100) Y (-100, 100) Z (0, 0)	Sample Footprint: 1
Footprint Size: 1 m	Unit Length: Meters

Table 10. Data for the results of Figure 20

## E. SUMMARY OF TEST CASE RESULTS

This chapter examined some of the capabilities of the **Urbana** Wireless Toolset. In addition, a typical scenario using a generic antenna pattern file was explored, and the resultant signal patterns were used to identify important pattern features, and scattering and diffraction effects.

As apparent from the patterns, because the antenna is fairly directional, it is not necessary to construct too large of an observation plane (in the  $X$ -direction). However, this will change as more buildings are added. Also to minimize losses, the antenna should be rotated to point directly at the receiving antenna. The antenna rotation can be introduced by providing the appropriate antenna system unit vector in the input file as shown in Chapter II.

The effects of additional buildings in the LOS will be more complex due to multiple scattering and diffraction. This will be explored further in Chapter V.

## V. AIRBASE MODEL

Wireless installations are commonly found in the commercial world, but not usually found in a military environment because wireless transmission are often deemed insecure. This chapter looks a near future application of wireless on an airbase and discusses its vulnerability.

### A. AIRBASE BUILDING MODEL

In the near future, aircraft pre-launched codes, including weapons stores data, waypoints coordinates and other mission critical data will be transmitted via a wireless link to the hangar where it is then disseminated through a local WLAN to the various aircraft being housed. The different types of aircraft housed in the hangar will perform different roles depending if they are an escort or a forward fighter. Thus, it is critical that the correct codes are being uploaded. The aircraft, upon successfully receiving the codes and uploading them to their respective mission computers, will then transmit back an acknowledgement signal. Security measures are in place throughout the airbase, including patrols around the perimeter, except perhaps a limited number of office buildings that are open to contractors and visitors. The objective is to run the **Urbana** toolset to determine if there are any possible security weaknesses that could arise. In particular, are there areas inside of the public buildings where sufficient signal strength exists so that interception is possible?

#### 1. Building the Model

The airbase building physical model was developed using *Cifer*. It consists of two main buildings, a control tower and an aircraft hangar both seated on a flat concrete ground plane measuring 2.4 km by 1 km. There are clusters of other office buildings that are situated within the LOS of the transmission path. Each building block was created separately and then combined using *cifer.x*, following the steps in [14]. The file was

saved as *airbase.facet*. The building edges were also created in *cifer.x* and saved under *airbase\_edge.facet*. The airbase model facet file is shown in Figure 21.

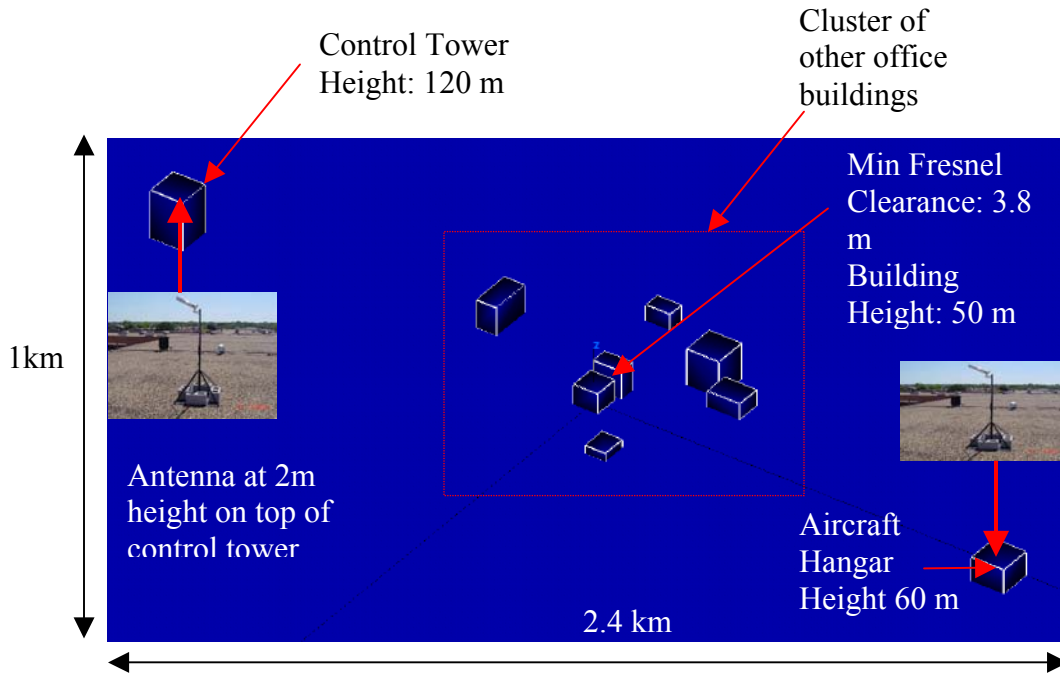


Figure 21. Hypothetical airbase model

The buildings represent a worst-case scenario, in that they are entirely composed of glass. A 1-W directional antenna transmitter and receiver pair was used to simulate the data transfer. Various test cases were run to compute the signal levels at different heights above the ground plane. The building materials were later modified to examine the effects of doped (tinted) glass and other composite materials.

## 2. Creating Observation Points

The observation area of interest does not have the same dimensions as the ground plane. The reason is that the HPBW of the simulated antenna has a narrow beamwidth. The Matlab GUI for generating the observation plane was used. Table 11 shows the coordinates of the observation plane used as the GUI inputs.

Observation plan	Min	Max
X	-400	400
Y	1200	1200
Z offset	2 m	
Footprint Size	10 m	

Table 11. Observation plane size

To make direct comparisons of data for the various cases, the observation plane size was kept constant, with the exception of the Z offset.

## B. INITIAL URBANA SIMULATIONS

Several **Urbana** simulations were run by modifying the input file (*airbase.ur\_input*). There are many other trial cases that were run during the course of testing, but only a few of the results are presented here. Table 12 summarizes the first 6 test cases. The radiation patterns from both the control tower and aircraft hangar at different observation planes were recorded.

TEST CASE	TRANSMIT ANTENNA LOCATION	RECEIVE ANTENNA LOCATION	BUILDING MATERIALS	GROUND PLANE MATERIALS	Z-OFFSET FROM GROUND
1	(X,Y,Z) (40,1000,62)	(X,Y,Z) (0,-1000,122)	glass	concrete	2 m
2	(X,Y,Z) (40,1000,62)	(X,Y,Z) (0,-1000,122)	glass	concrete	62 m
3	(X,Y,Z) (40,1000,62)	(X,Y,Z) (0,-1000,122)	glass	concrete	122 m
4	(X,Y,Z) (0,-1000,122)	(X,Y,Z) (40,1000,62)	glass	concrete	2 m
5	(X,Y,Z) (0,-1000,122)	(X,Y,Z) (40,1000,62)	glass	concrete	62 m
6	(X,Y,Z) (0,-1000,122)	(X,Y,Z) (40,1000,62)	glass	concrete	122 m

Table 12. Summary of initial test cases

From Table 12, the heights of the transmitting and receiving antenna are not equal level. Thus, in order to minimize polarization losses, the antenna, specifically the radiation pattern, had to be rotated. This was accomplished using a Matlab GUI as shown in Figure 22, which requires the user to enter in the locations of the transmitting and receiving antenna locations. The GUI then computes the rotated antenna unit vectors according to Equation [3.6]; these are subsequently entered into the input file (*airbase.ur\_input*).

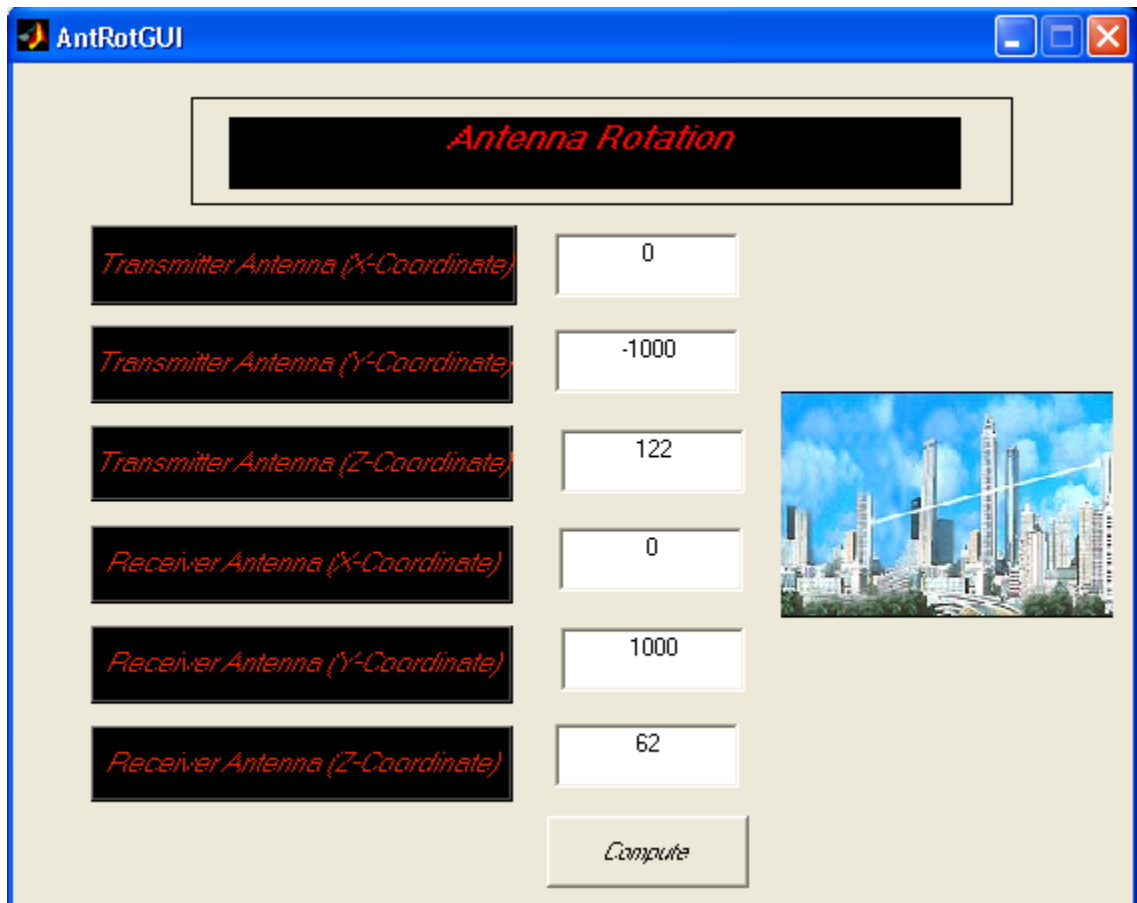


Figure 22. Antenna rotation GUI

Table 13 lists some of the parameters specified in the input file as they pertain to the airbase model.

INPUT PARAMETER	VALUES/OPTION
Facet Model	<i>airbase.facet</i>
Length Unit	meters
Frequency	2.4 GHz
Antenna Description	By pattern file: <i>antennapat.antenna</i>
Antenna Type	Directional Antenna
Antenna Origin	40.0, 1000.0, 62.0
Antenna Local Coordinates	X' unit vector x,y,z components: 0, -0.03, -1 Z' unit vector x,y,z components: -0.02, -1, 0.03
Observation Points	<i>obvpoints</i>
Rx Antenna	No
Computation Method	SBR
Edge Diffraction	Yes (UTD)
Edge Model	<i>airbase.edge</i>
Ray Spacing	2.0 degree
Max Bounces	5
Materials	ICOAT = 0 (perfectly electric conducting material) ICOAT = 1 concrete (Ground Plane) ICOAT = 2 Not Used ICOAT = 3 Not Used ICOAT = 4 glass (Buildings)

Table 13. **Urbana** input parameters for airbase building model

There are two computers used for the **Urbana** simulations. The first (EMAG 2) is a UNIX based Silicon Graphics Indigo Workstation computer with the following specifications: a 150-MHz IP22 processor, data cache size of 16 kB, and main memory size of 320 MB. The second is a newer SGI Octane workstation with the following specifications: a 300-MHz IP32 processor, data cache size of 32 kB, and main memory size of 1 GB. The computation time depends on the footprint size and the size of the observation region. A typical run time was an hour on EMAG 4.

**Urbana** then creates the output file *airbase.field* that contains the computed signal levels. The program *f2f.x* is then executed to translate the field results into a color-coded facet file that can be viewed in **Xcell**. Table 14 shows the input sequence. This input sequence is kept constant for the entire initial 6 test cases, with the exception of the range levels [13].

REQUIRED INPUT	RESPONSE
Type of E-Field	Magnitude of E-Tot
Number of Field Files	1
Name of Field File	<i>airbase.field</i>
Antenna Power Level	30 dBm
Histogram Interval	5 dB
Max and Min Clip values	-200 dBm, 30 dBm
Max and Min Range values	-100 dBm, 30 dBm
Number of Levels	25
Lowest Coating Code	1
Name of Output Facet File	<i>airbase_out.facet</i>
Side of Footprint Square	10 meters
Shift according to Z-data	Y
Enter z-offset footprint	0

Table 14. Inputs for running *f2f.x*

The output file (*airbase\_out.facet*) was loaded into **XCell** to display the signal contours. Figure 23 shows the contours for the data in Table 13. Figures 24 and 25 show the signal contour at Z offsets of 62 meters and 122 meters respectively. The reason for choosing this height is due to the location of the antennas.

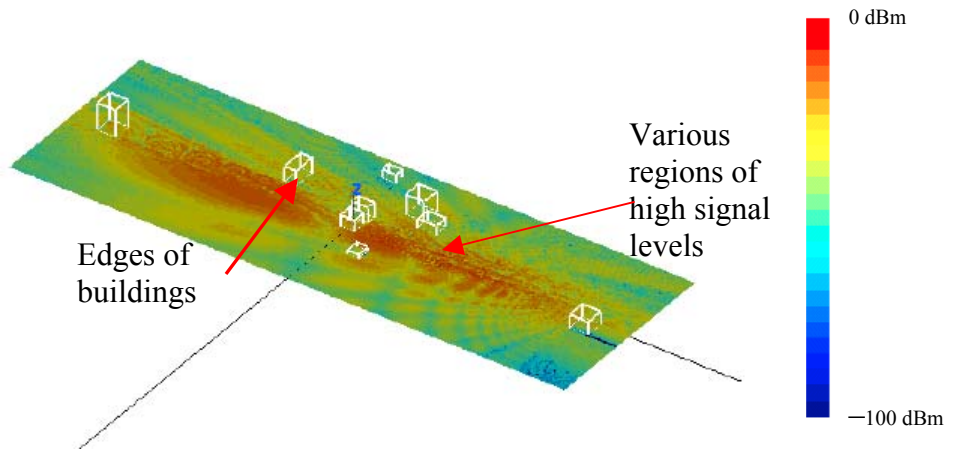


Figure 23. Signal contour of case 1 in Table 12

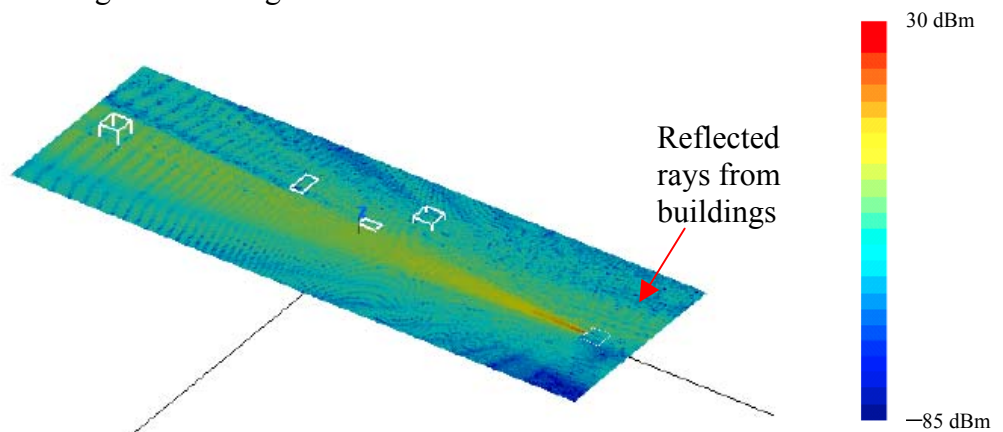


Figure 24. Signal contour of case 2 in Table 12

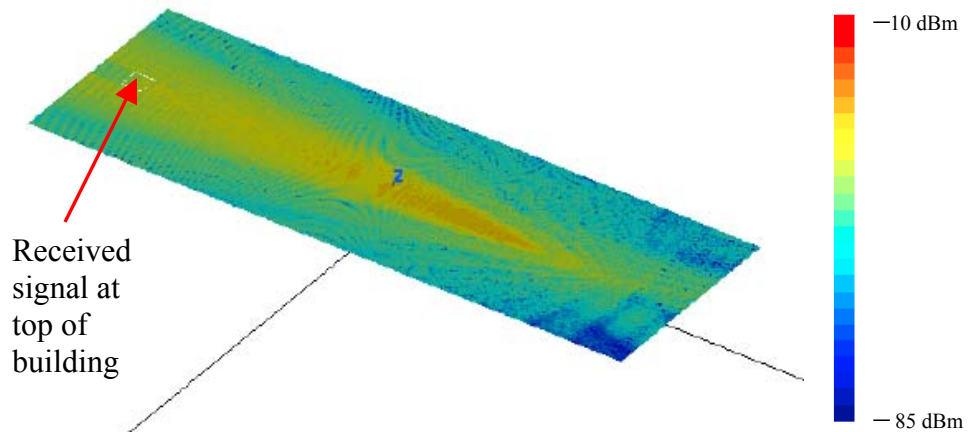


Figure 25. Signal contour of case 3 in Table 12

The calculation was repeated with the control tower transmitting to the aircraft hangar. The antenna coordinates were changed accordingly in the input file. The signal contours in Figures 26 through 28 were generated.

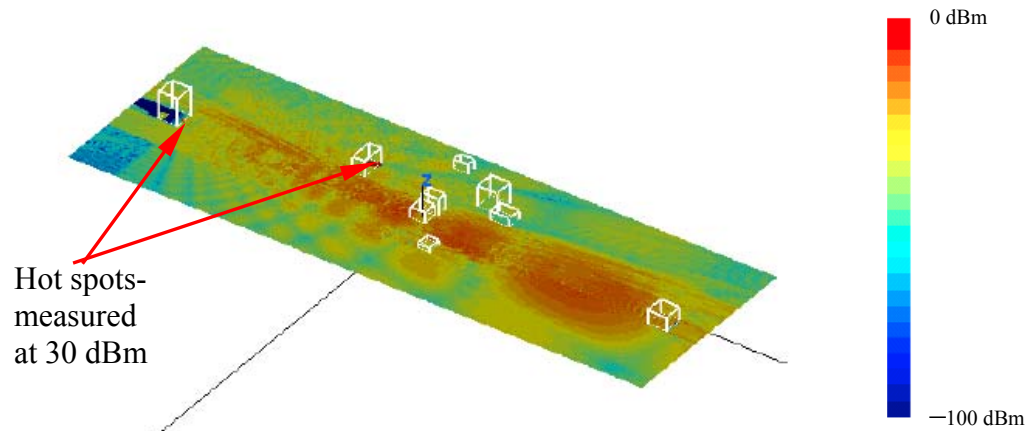


Figure 26. Signal contour of case 4 in Table 12

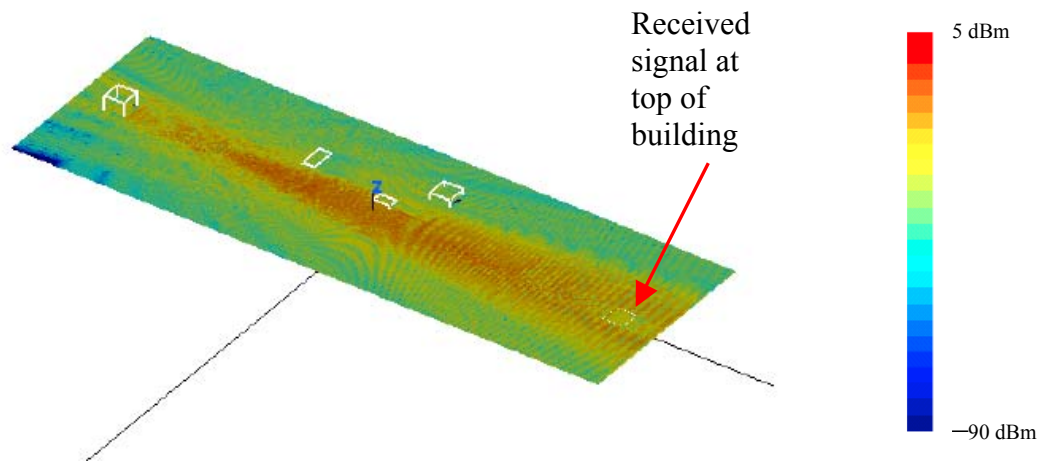


Figure 27. Signal contour of case 5 in Table 12

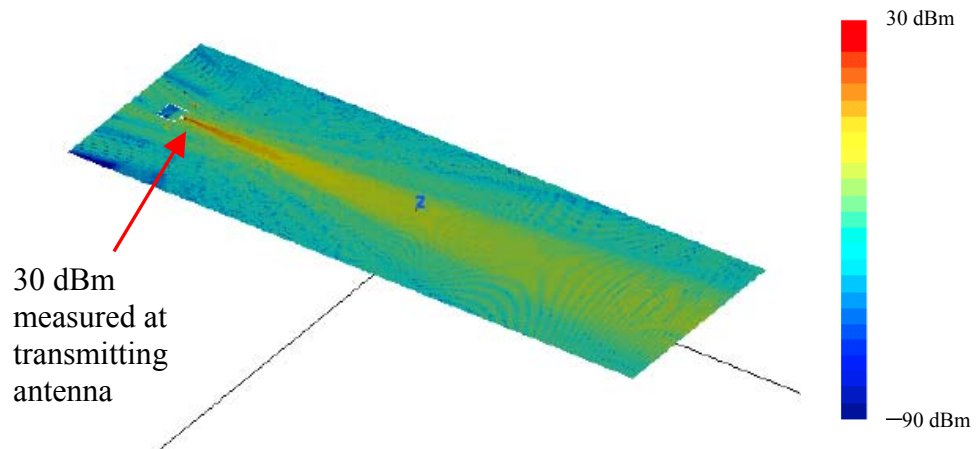


Figure 28. Signal contour of case 6 in Table 12

## 1. Summary of Initial Simulation Results

It was observed that when the control tower was transmitting to the aircraft hangar, there were two hotspots with readings near 30 dBm. This was suspected to be due to the orientation of the cluster of the buildings, which were closer to the control tower than to the aircraft hangar. The junctions of two vertical walls along with the ground plane serve as an effective “corner reflector” that can focus the signal at a limited number of nearby points. This presents a potential vulnerability for covert entities to hack into the system. There were also several regions of high signal level recorded on the ground. It is interesting to note that the hotspots caused by local features in the geometry (e.g., a corner reflector) are not reciprocal in the sense that they may be present when transmitting from control tower to the hangar, but not when transmitting from the hangar to the control tower. The next section will further examine the various findings of this section.

## C. INVESTIGATION INTO LOCALIZED SCATTERING EFFECTS

### 1. Building Orientation and Multipath

In order to confirm that the phenomenon seen in Section B was indeed caused by the orientation of the building, the *cifer.x* program was used to edit the *airbase.facet* to translate the building. Originally there was a hotspot as shown in Figure 26. Figure 29 shows the hotspot no longer exists when the building was moved to  $X = +50$ .

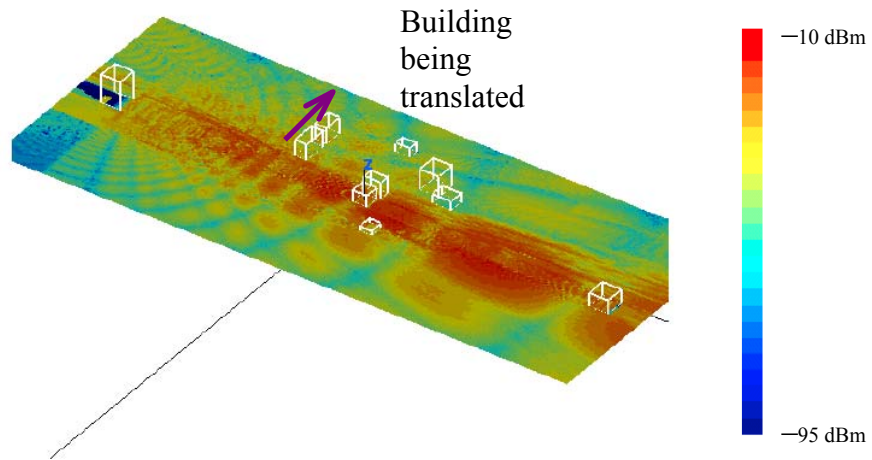


Figure 29. Signal contours when buildings are translated

To substantiate the reasoning that the hotspot could be due to multipath, the number of ray bounces was adjusted. Figures 30 to 32 show the results of varying the ray bounces. From the figures, we can deduce that increasing the number of ray bounces has an effect on the signal contours. The **Urbana** toolset recommends leaving the settings at 5–10 ray bounces under normal conditions. The actual number required for convergence at a point depends on the number and strength of the reflections and diffractions at that point. This information is not known in advance and therefore 5 to 10 bounces is a good rule of thumb for a starting point.

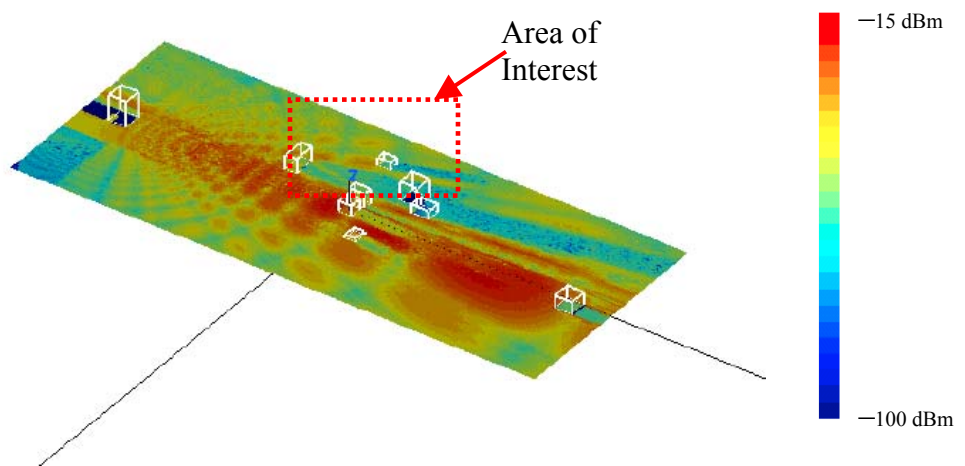


Figure 30. Signal contour at 2 m with one ray bounce

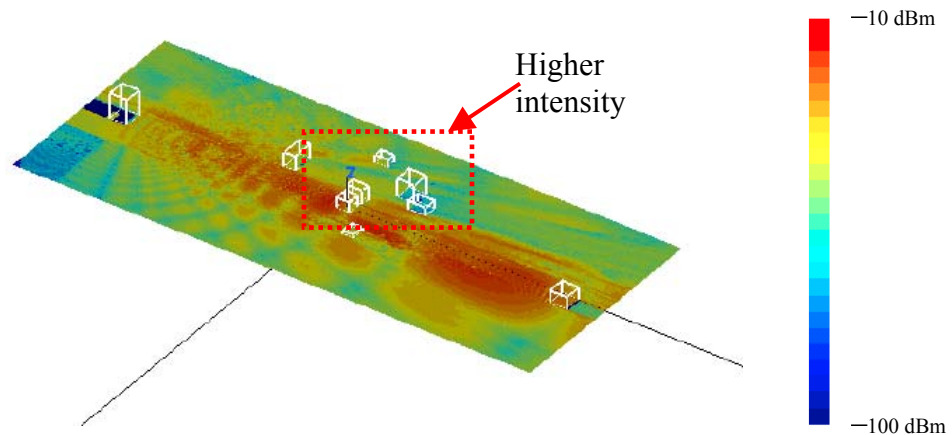


Figure 31. Signal contour at 2 m with two ray bounces

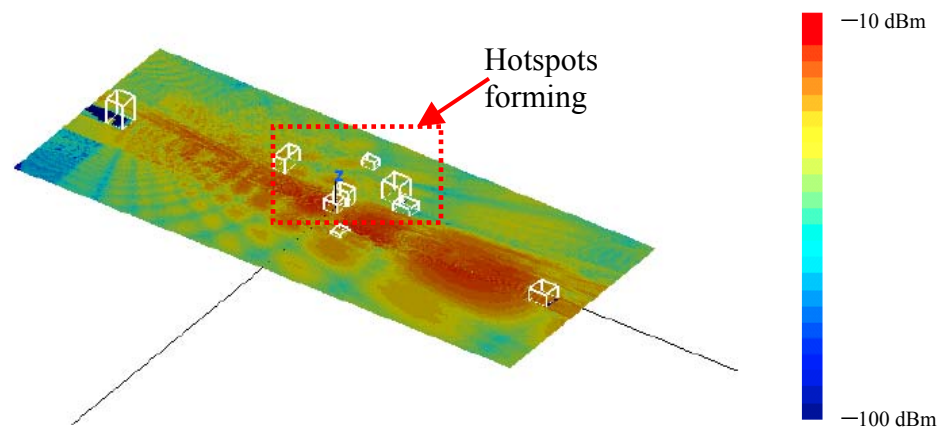


Figure 32. Signal contour at 2 m with four ray bounces

## 2. Zooming in on the Hotspot

Using the same *airbase.facet* file, the observation plane was reduced in size so that a smaller cell size could be used to enhance the resolution of the signal contour. Table 15 shows the updated observation plane inputs to the Matlab GUI, while Figures 33 and 34 show the signal contours at 2 m and at 68 m (corresponding to the first and top floors). The figures illustrate that as the observation plane increases in height, the signal strength diminishes. This indicates that the hotspot is due to a local corner reflector effect. Multiple reflection from the walls and ground add constructively at about 2 m above the ground.

Observation plan	Min	Max
X	-200	-50
Y	-250	-400
Z offset	2	
Footprint Size	1m	

Table 15. Observation plane size

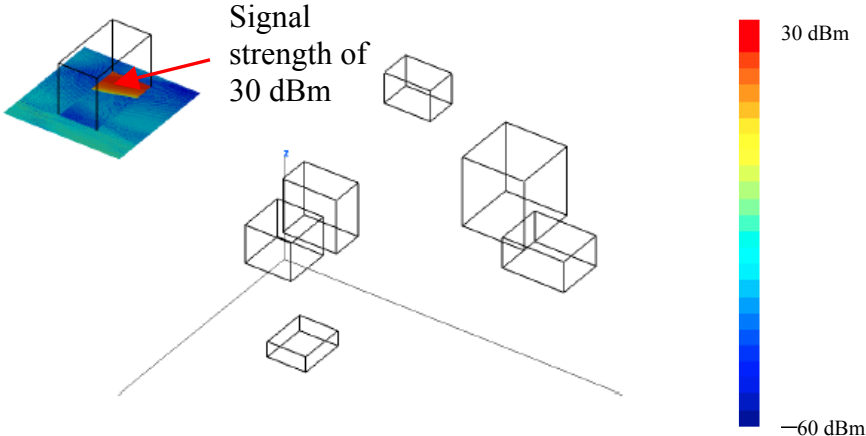


Figure 33. Signal contour at 2 m

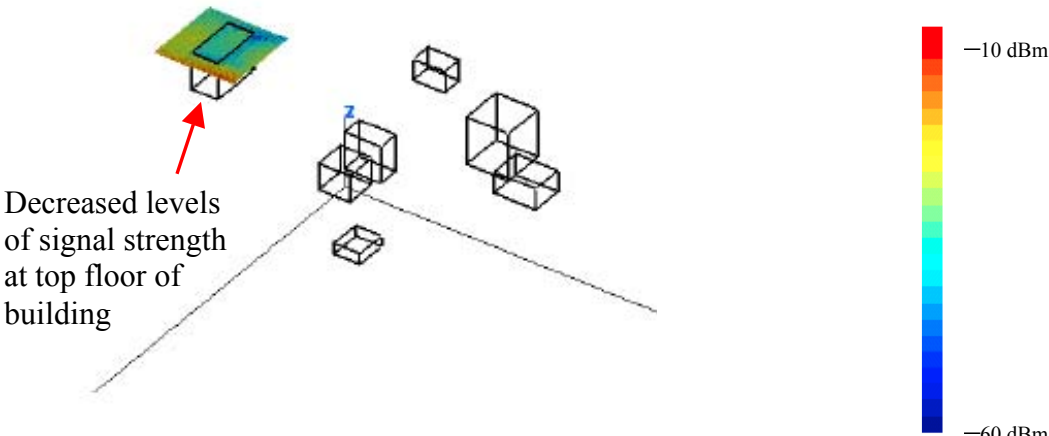


Figure 34. Signal contour at 68 m

**3. Absorbing Walls**

The occurrence of a hotspot is not desirable from a security point of view and eliminating it is preferred. Shielding the affected building by some means could eliminate the hotspot. To demonstrate this, a two-meter wall made of absorbing materials was

added using **cifer.x**. With all other parameters remaining unchanged from Case 4 in Table 12, with exception of the wall having absorbing facets, Case 4 was re-run. Figure 35 shows that the previous hotspots seen in Figure 26 ceased to exist. Of course, to erect a 2-m by 100-m wall in front of a building is not exactly cost-effective and has other disadvantages, e.g., reduction in visibility, accessibility, etc.

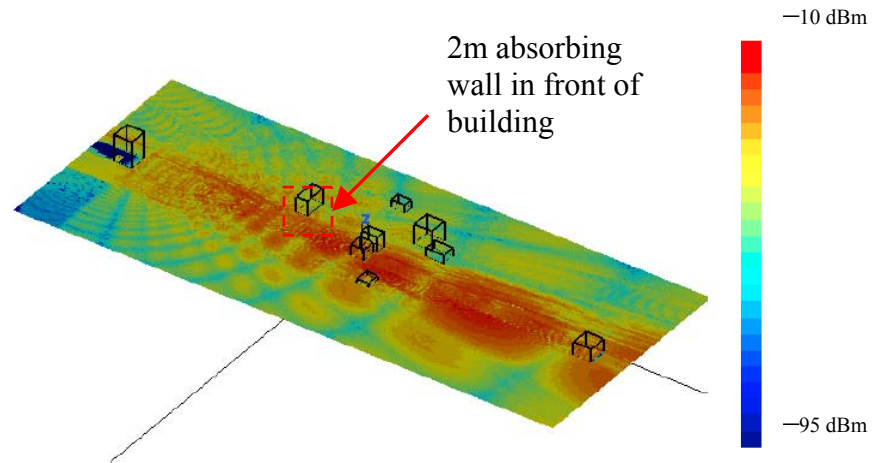


Figure 35. Signal contour with a 2-m absorbing wall in front of the affected building

#### 4. Doped (Tinted) Glass

If the building has a large percentage of glass instead of solid walls, it would be possible to cover the entire window area with a tint. The partially silvered glass should prevent signals from penetrating into the building relative to plain glass, thus providing some additional shielding. Thus the *airbase.facet* was amended to have a single side of the wall coated with tinted glass as shown in Figure 36.

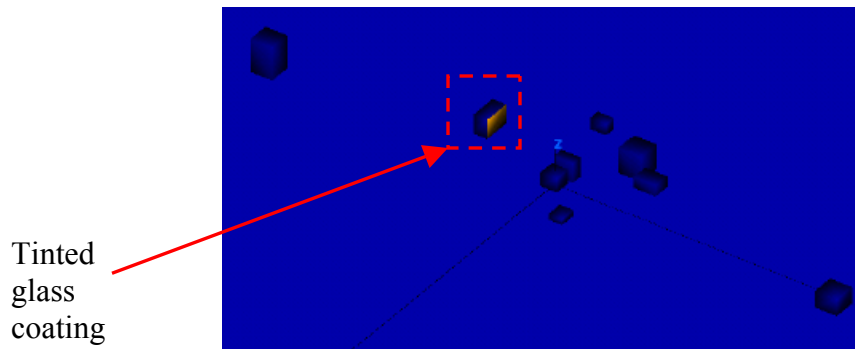


Figure 36. Tinted glass on single side of building

Tables 16 and 17 show the input parameters used for this test case and Figure 37 shows the signal contours with doped glass coating on one side of the building wall.

<b>Observation plan</b>	<b>Min</b>	<b>Max</b>
<b>X</b>	-400	400
<b>Y</b>	1200	1200
<b>Z offset</b>	2 m	
<b>Footprint Size</b>	10 m	

Table 16. Observation plane size

INPUT PARAMETER	VALUES/OPTION
Facet Model	<i>airbase.facet</i>
Length Unit	meters
Frequency	2.4 GHz
Antenna Description	By pattern file: <i>antennapat.antenna</i>
Antenna Type	Directional Antenna
Antenna Origin	0.0, -1000.0, 122.0
Antenna Local Coordinates	X' unit vector x,y,z components: 0, -0.03, -1 Z' unit vector x,y,z components: 0.02, 1, -0.03
Observation Points	<i>obvpoints</i>
Rx Antenna	No
Computation Method	SBR
Edge Diffraction	Yes (UTD)
Edge Model	<i>airbase.edge</i>
Ray Spacing	2.0 degree
Max Bounces	5
Materials	ICOAT = 0 (perfectly electric conducting material) ICOAT = 1 concrete (Ground plane) ICOAT = 2 tinted glass (Building wall) ICOAT = 3 Not Used ICOAT = 4 glass (Buildings)

Table 17. **Urbana** input parameters for the airbase building model with tinted glass

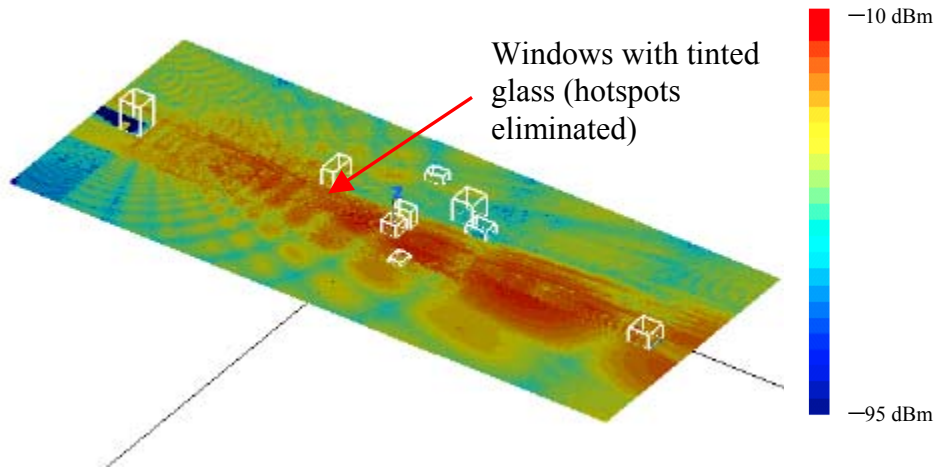


Figure 37. Signal contours showing doped glass coatings on wall

## 5. Urbana Simulation Summary

From the findings above, it was concluded that a certain building geometry and orientation may actually give rise to localized regions of high signal strength. The cause is constructive interference of multiple reflections from the building walls and floor. The locations of these hotspots are generally not predictable by a casual examination of the building layout and geometry. Thus accurate simulations are crucial in predicting the presence of these hotspots. For glass buildings, a cost effective method of reducing hotspots is to coat the windows with tinting.

## D. OTHER SCENARIOS

The various scenarios above highlight a typical airbase with a wireless PTP system. The following three scenarios look at the effect of shifting the antenna position, together with coating the roof with absorbing facets, to reduce possible multipath reflections. The effects of several parked cars along the LOS of the antenna beam, and the changing of the antenna HPBW and frequency are also examined.

### 1. Antenna Position

Keeping the same observation plane, the Antenna Rotation GUI was run to compute the local coordinates and Table 18 shows the updated input file parameters. It

was observed in Figure 38 that the signal spatial dispersion is much less than that seen in Case 4 in Table 12 of the initial test run. Figure 39 shows that, despite the antenna position change, there is still adequate signal strength at the receiving antenna.

INPUT PARAMETER	VALUES/OPTION
Facet Model	<i>airbase.facet</i>
Length Unit	meters
Frequency	2.4 GHz
Antenna Description	By pattern file: <i>antennapat.antenna</i>
Antenna Type	Directional Antenna
Antenna Origin	0.0, -1080.0, 122.0
Antenna Local Coordinates	X' unit vector x,y,z components: 0, -0.0289, -1 Z' unit vector x,y,z components: 0.02, 1, -0.0289
Observation Points	<i>obvpoints</i>
Rx Antenna	No
Computation Method	SBR
Edge Diffraction	Yes (UTD)
Edge Model	<i>airbase.edge</i>
Ray Spacing	2.0 degree
Max Bounces	5
Materials	ICOAT = 0 (perfectly electric conducting material) ICOAT = 1 concrete (Ground plane) ICOAT = 2 Absorbing roof facet ICOAT = 3 Not Used ICOAT = 4 glass (Buildings)

Table 18. **Urbana** input parameters for the airbase building model with tinted glass

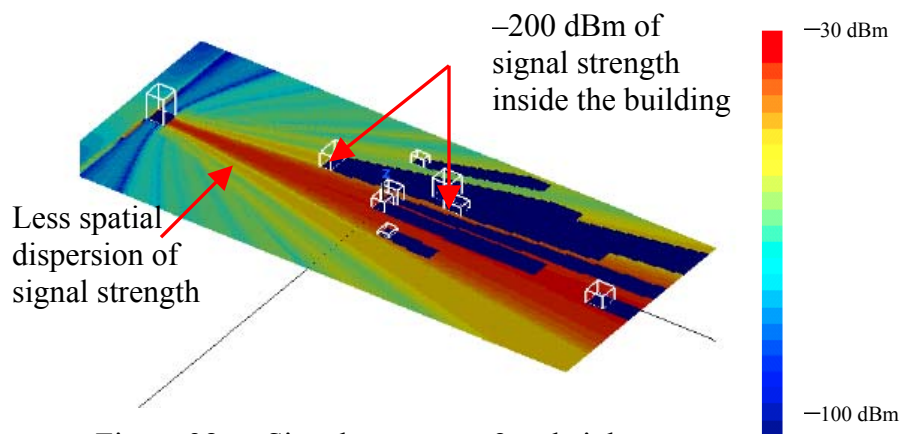


Figure 38. Signal contour at 2-m height

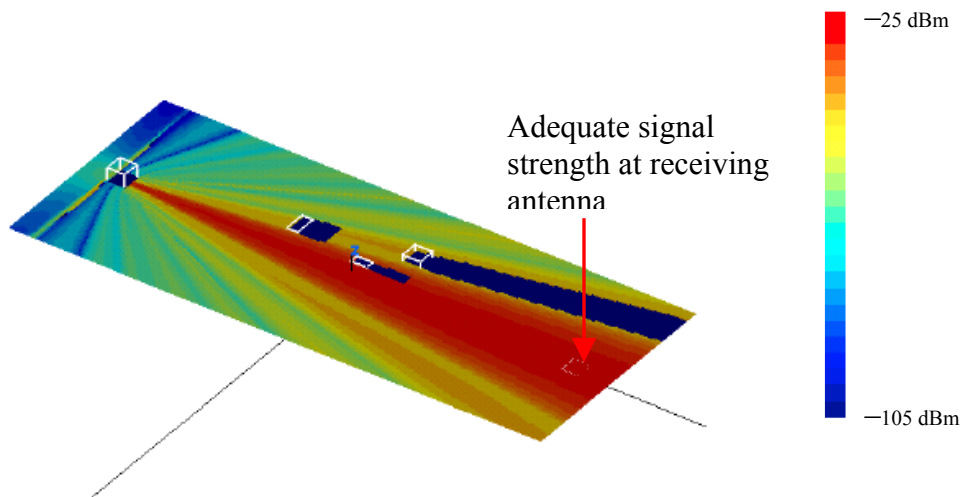


Figure 39. Signal contour at 62-m height

## 2. Parked Cars

An airbase without ground vehicles is not realistic. Vehicles are primarily made of metal and glass and can potentially cause large reflection that changes with time, thereby causing abnormalities in the signal contours. Several clusters of cars were generated in *ACAD* [14] and their facets were combined with the *airbase.facet* using *cifer.x*. Table 19 shows the input parameters for this scenario and Figure 40 depicts the signal contours and illustrates the effect of scattering due to the parked cars. Comparing with Case 1 in Table 12, there are signs of increased signal strength due to the reflection of rays from the parked cars.

INPUT PARAMETER	VALUES/OPTION
Facet Model	<i>airbase.facet</i>
Length Unit	meters
Frequency	2.4 GHz
Antenna Description	By pattern file: <i>antennapat.antenna</i>
Antenna Type	Directional Antenna
Antenna Origin	40.0, 1000.0, 62.0
Antenna Local Coordinates	X' unit vector x,y,z components: 0, -0.03, -1 Z' unit vector x,y,z components: -0.02, -1, 0.03
Observation Points	<i>obvpoints</i>
Rx Antenna	No
Computation Method	SBR
Edge Diffraction	Yes (UTD)
Edge Model	<i>airbase.edge</i>
Ray Spacing	2.0 degree
Max Bounces	5
Materials	ICOAT = 0 (perfectly electric conducting material) ICOAT = 1 concrete (Ground plane) ICOAT = 2 PEC (Metal portions of the cars) ICOAT = 3 Not Used ICOAT = 4 glass (Buildings and glass on cars)

Table 19. **Urbana** input parameters for the airbase building model with parked cars

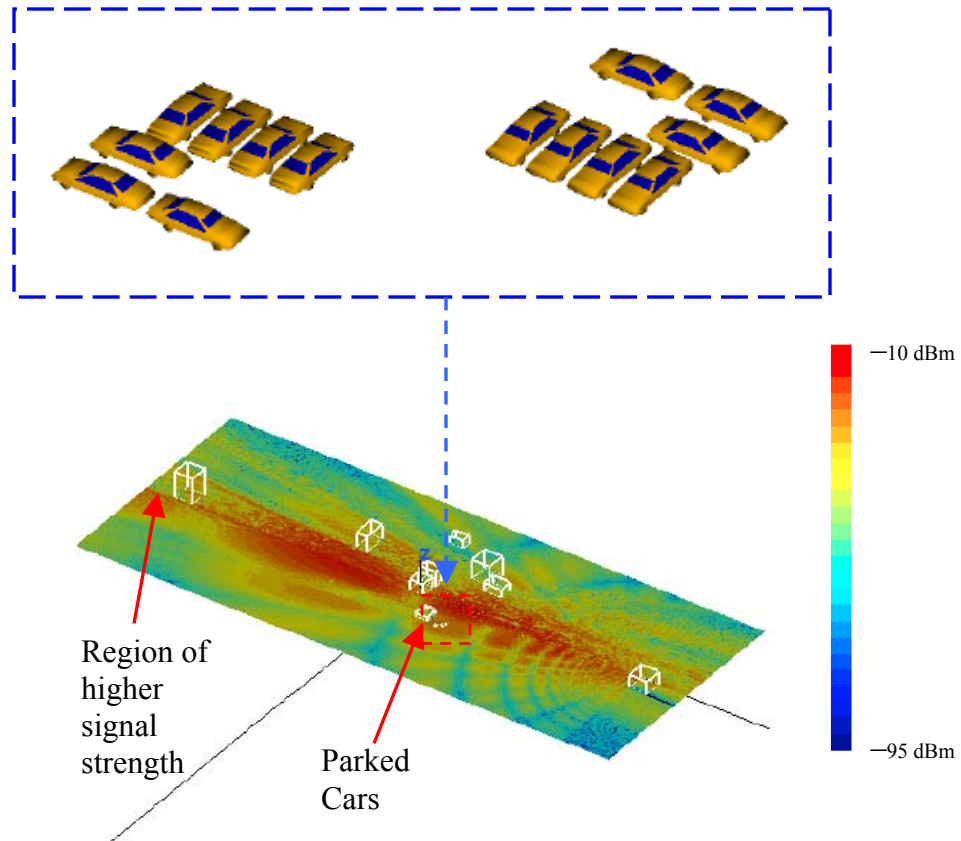


Figure 40. Signal contour at 2 m offset with parked cars

### 3. HPBW and Frequency

Using the Antenna Generation GUI, the antenna pattern was changed. Figure 41 shows the signal contours resulting from the **Urbana** simulation. As shown in Figure 41, due to a broader antenna beamwidth, there are larger regions of high signal levels. Therefore, the probability of being able to intercept the signal is much higher.

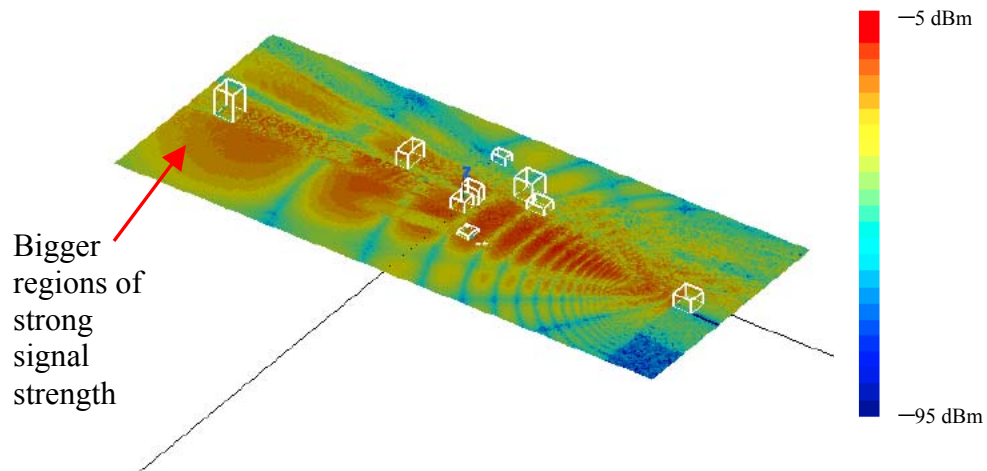


Figure 41. Signal contour at 2 m offset with a broader beamwidth

#### 4. Summary

With the parked cars it was shown that there would be some additional high signal areas. It may be difficult to predict these locations, because the cars may not be parked in the same manner every day. As expected, the effects of using a broader beamwidth increase the probability of intercept.

#### E. SUMMARY

This chapter presented several simulations for a typical airbase model. With the exception of the final test case, a 2.4-GHz, 1-W transmitting generic antenna was used throughout the experiment

By properly selecting the beamwidth, frequency and building coatings, some of the unwanted regions of strong signal strength may be eliminated. However, there are still regions of hotspots on the ground and they present a potential vulnerability to the systems installed.

## **VI. SUMMARY AND CONCLUSIONS**

### **A. SUMMARY**

This research has established a process that can be used to predict the signal levels of wireless PTP communications in an outdoor urban environment. The worst case scenario was used throughout all test cases to present a clear representation of any possible vulnerabilities. A series of simulations was performed with various antenna patterns, building materials, building locations and parked autos. Signal contours were plotted and high signal areas that are susceptible to interception were identified. The signal level for detection has not been specified, because it can vary widely depending on the sophistication of the intercept receiver. Typical values might range from  $-80$  dBm to  $-140$  dBm.

### **B. CONCLUSIONS**

The findings presented in Chapters IV and V indicate that there are numerous vulnerabilities associated with wireless PTP communication systems that may not be apparent through physical examination of the building layout. The simulation results from tinting windows and using a narrower antenna beamwidth was demonstrated to be effective in eliminating potential security problems due to hotspots.

There is a widely held misconception that PTP wireless systems are not interceptable because they use a narrow beam antenna. Furthermore, the antennas are generally at building rooftops, which makes it difficult for intercept receivers to position themselves directly in the antenna's field of view. However, this research has demonstrated that adequate signal strength for interception most likely exists well outside of the antenna main beam. The fact that the wireless PTP systems are inherently an outdoor system make them more susceptible to interception. This research has demonstrated that local hotspots frequently occur on the ground outdoors or near corners inside of a building.

Some precautions that can be taken to reduce covert entities hacking into the system include:

1. Perform a high fidelity EM simulation of the proposed wireless path to identify hotspots.
2. Proper adaptation of receiver sensitivity so that the minimum power level can be transmitted. This technique is known as power management.
3. Stepping up physical security in the regions where the signal is strong enough for interception.
4. Implementation of software encryption.
5. Selective frequency hopping to reduce the probability of intercepting the signal.

### **C. FUTURE WORK**

Apart from tinting, it would seem ideal to utilize as narrow a beam as possible, and one solution is to use Free Space Optics (FSO) [15] or laser point-to-point communication. Figure 42 shows a COTS FSO product overview. Laser point-to-point communications have a narrow divergence of the beam, but there are some disadvantages in using a laser beam.

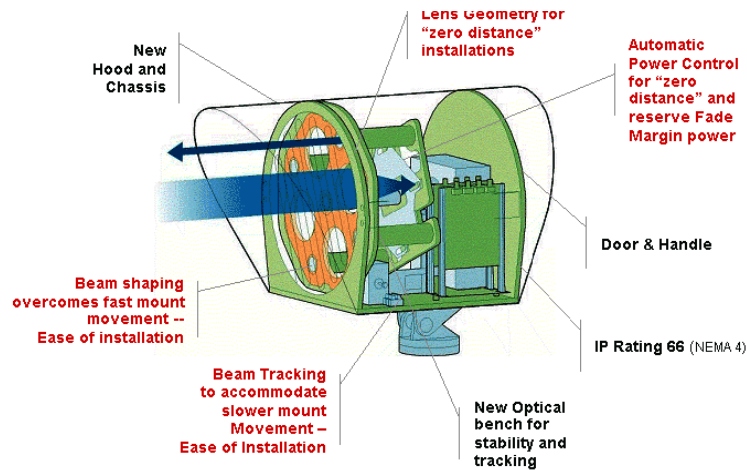


Figure 42. FSO product overview (From Ref. [15].)

As FSO uses a laser beam to transmit data between transceiver units, that laser must always have a clear path to travel. In the case of an airbase scenario, LOS may not be a problem but in crowded cities, having a clear LOS can be problematic. The weather alone may cause problems. Dense fog or heavy rain can shut an FSO system down. Figure 43 shows an operational FSO equipment setup.

Small flying objects, such as MUAVs or even small birds can interrupt the transmission link for an instant. Since most FSO gear are designed to send and receive via rooftop installations, any type of building movement can degrade on an FSO system.



Figure 43. An operational FSO equipment setup (From Ref. [15].)

In the case of point-to-multipoint, system designers are dealing with these FSO reliability issues can work around using redundant design. By creating extra links through either ring or mesh topologies, data traffic can be re-routed around broken links. But this is only useful if there is a network of buildings in the vicinity.

The most notable new approach is adding wireless RF transmitters to the mix, so if the laser link goes down, wireless transmission can kick in and keep data flowing. This is also known as graceful degradation. Reference [16] highlights the benefits of integrating a WLAN system with FSO. As a first step in direct comparison of RF and FSO, the urban optical propagation behavior should be examined, similar to what has been done here at RF.

## APPENDIX

### A. WIRELESS POINT-TO-POINT PERIPHERALS

#### 1. RF spectrum allocation

As wireless communication are anticipated to dominate in numerous enterprises such as education, airports and other public meeting spaces. There is a need to allocate different frequencies for the various wireless communities. Figure 44 shows the various RF spectrum allocation for different purposes.

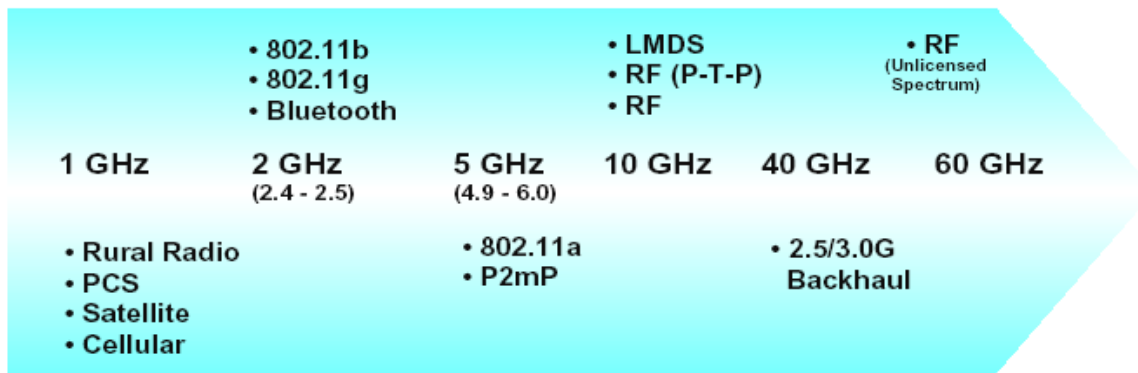


Figure 44. RF spectrum allocation (From Ref. [15].)

#### 2. Antennas

A Yagi antenna is composed of an array of linear elements, parallel to one another and attached perpendicular to and along the length of a metal boom. The feed is attached to only one of the elements. The elements on one side of the feed element are longer and act as reflectors; elements on the other side are shorter and act as directors. This causes the antenna to radiate in a beam out of the end with the shorter elements. The actual pattern depends on the overall geometry, including the number of elements, element spacing, element length, etc. Sometimes the antenna is enclosed in a protective tube that hides the actual antenna geometry, as shown in Figure 45.

The antenna pattern is a beam pointed along the boom toward the end with the shorter elements. The beamwidth varies with antenna geometry but generally is proportional to the length (where longer length produces a narrower beam).

The antenna gain is typically from 6 to 15 dBi but this also varies with antenna geometry, but generally is proportional to the length (where longer length produces higher gain). The antenna polarity is linear (parallel to the elements, perpendicular to the boom).

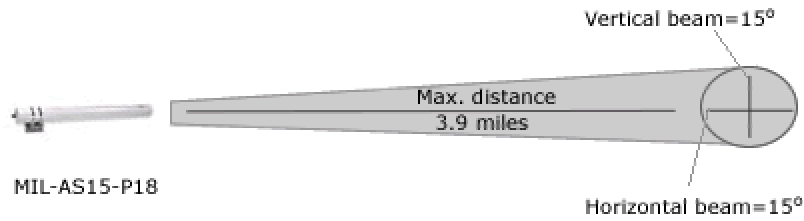


Figure 45. A commercial off the shelf (COTS) Yagi antenna (From Ref. [17].)



Typical Characteristics		
Frequency Range	2.4–2.83 GHz	5.725–5.825 GHz
VSWR	Less than 2:1, 1.5:1 Nominal	1.5:1 Nominal
Gain	13.5	28 dBi
Front to Back Ratio	Greater than 30 dB	-
Polarization	Vertical	Vertical/Horizontal

Table 20. Typical client adapter antennas (From Ref. [6].)

### 3. Bridges

Wireless bridges are designed to connect discrete sites into a single LAN, even when they are separated by obstacles such as freeways, railroads, and bodies of water that are practically insurmountable for copper and fiber-optic cable. The Cisco Aironet wireless bridges [2] deliver high data rates and superior throughput for data-intensive, line-of-sight applications. The high-speed links between Cisco Aironet wireless bridges delivers fast throughput thus eliminating the need for expensive and difficult to install leased lines or fiber-optic cable. Table 21 lists the specifications of two COTS bridges commonly found in wireless PTP systems.


Wireless Bridges		
Typical Characteristics	<ul style="list-style-type: none"> <li>➤ 10/100 Mbps Auto sensing</li> <li>➤ Data Rates ranging from 1.5 to 12 Mbps</li> <li>➤ “Plug and Play” setup</li> <li>➤ SNMP and Telnet Time Division Duplexing</li> <li>➤ Up to 40 km</li> <li>➤ 2.4 and 5.8 GHz</li> </ul>	<ul style="list-style-type: none"> <li>➤ 11 Mbps</li> <li>➤ Capable of PTP or point to multipoint communications</li> <li>➤ Up to 25 miles range</li> <li>➤ 2.4 GHz</li> </ul>

Table 21. Typical COTS bridges (From Ref. [2, 17].)

## B. MATLAB CODES

The following is a list of Matlab codes, which includes: the observation plane generation, plot of pathloss versus distance at a 2.4-GHz frequency, antenna pattern file, the antenna rotation file and a plot of VWSR Vs Return Loss (RL).

```
% Observation points generation
```

```
%-----
```

```
clc;  
clear;
```

```
i = 1;  
y = 10;
```

```
for x = -5:1:5  
    for z = 0:1:10  
        y = 10;  
        M(i,:) = [x, y, z];  
        i = i + 1;  
    end  
end
```

```
save obvpnts M -ASCII;
```

```
%-----
```

```
% Plotting of Pathloss (PL) Vs Distance at a fixed 2.4Ghz Frequency
```

```
%-----
```

```
clc;  
clear;
```

```
Freq = 2.4e9;  
lamda = 3e8/Freq;  
Distance = 100:2:5000;  
PL = 20*log10(4*pi*Distance./lamda);
```

```
semilogx(Distance,PL)  
xlabel('Distance (m)')  
ylabel('Path Loss, PL (dB)')  
title('Distance Vs Path Loss')  
grid on;
```

```
%-----
```

```

% Antenna Pattern File
%-----
clc;
clear;
%warning off;

lamda = (3*10^8)/(2.4*10^9);
HPBW = 7.5; % in degrees (
a = 58.4 * lamda / (2*HPBW); %Uniform Circular Aperature Size
beta = 2*pi/lamda;
E0 = 1;
c = j*beta*E0*pi*a^2/(2*pi); %Contant term in E field

step1 = 45; %Vertical Steps
step2 = 180; %Horizontal Steps
d_theta = 180/(step1);
d_phi = 360/(step2);
k = 0;
ip = 0;
iq = 0;

for phi = 0:d_phi:360
    for theta = 0.01:d_theta:180.01
        k = k+1;
        f = 2*besselj(1,beta*a*sin(theta*pi/180))/(beta*a*sin(theta*pi/180))
        e_theta = cos(phi*pi/180)*c*f;
        e_phi = -sin(phi*pi/180)*cos(theta*pi/180)*c*f;
        if theta > 90
            e_theta = 0;
            e_phi = 0;
        end
        if phi == 0
            ip = ip + 1;
            et0(ip) = 20*log10(abs(e_theta));
            ep0(ip) = 20*log10(abs(e_phi));
            eth(ip) = theta;
        end
        if phi == 90
            iq = iq + 1;
            et90(iq) = 20*log10(abs(e_theta));
            ep90(iq) = 20*log10(abs(e_phi));
            eth90(iq) = theta;
        end
        phi
        A(k,1:4) = [real(e_theta), imag(e_theta), real(e_phi), imag(e_phi)];
    end
end

```

```

    end
end

save antenapat1 A -ASCII;

figure(1)
plot(eth,et0,eth,ep0)
figure(2)
plot(ETH90,ET90,ETH90,EP90)
%-----

% Scattered field of a plate rotated by beta and alpha
%-----
clc;
warning off;
rad=pi/180;
% unit vector
r=[x2-x1 y2-y1 z2-z1];
rhat=r/abs(r);
alpha=atan2(r(2),r(1))
beta=pi/2-atan2(r(3),sqrt(r(1)^2+r(2)^2))

disp(' ')

disp(['Antenna location (x,y,z): ',num2str(x1),' ',num2str(y1),' ',num2str(z1)])
disp(['Observation location (x,y,z): ',num2str(x2),' ',num2str(y2),' ',num2str(z2)])
disp(['Alpha (deg): ',num2str(alpha/rad)])

disp(['Beta (deg): ',num2str(beta/rad)])
% Local direction cosines
ca=cos(alpha); sa=sin(alpha); cb=cos(beta); sb=sin(beta);
T1=[ca sa 0; -sa ca 0; 0 0 1]; T2=[cb 0 -sb; 0 1 0; sb 0 cb]; %Defining transformation
matrix 1 & 2
T=T2*T1;

for i=1:3, for k=1:3, if abs(T(i,k))<1e-10, T(i,k)=0; end, end, end
disp(['x" unit vector x,y,z components: ',num2str(T(1,1)),...
', ',num2str(T(1,2)),' ', ',num2str(T(1,3))])
disp(['z" unit vector x,y,z components: ',num2str(T(3,1)),...
', ',num2str(T(3,2)),' ', ',num2str(T(3,3))])

h = msgbox([' Results generated! See Command Window! ', 'Result']);

%-----

```

```
% Plotting of VWSR Vs Return Loss (RL) for a Cisco Yagi Antenna
%-----
clc;
clear;

VWSR = 1.01:0.01:2.0;
RL = 20*log10((VWSR+1)./(VWSR-1));

plot(VWSR,RL)
xlabel('VWSR')
ylabel('Return Loss, RL (dB)')
title('VWSR Vs RL')
grid on;
%-----
```

## C. URBANA INPUT SCRIPT FILE

The following is a listing of the **Urbana** input file *vertical\_plane.ur\_input*:

```
--- input Urbana v 2.5
#
# *****
# A---scatterer file,length & freq
# *****
#--- name of scatterer file in ACAD format (e.g. wall.facet)
vertical_plane.facet
#--- length unit:1=inch, 2=cm, 3=meter, 4=mm, 5=mil
3
#--- uniform freq (GHz): start freq, end , nstep
# (nstep=0 means: just do first freq. CAUTION: antenna patterns are
# assumed to be indep. of freq and is calculated at end freq)
2.4 2.4 0
#
# *****
# B--- Antenna Description and List
# *****
#
#---Enter method of describing antennas.
# (1 = here, 2 = file):
1
#---If described in file, enter file name:
dummy.antenna
#---If described here, fill in sections B1, B2, B3.
# If described in file, use dummy data in sections B1, B2, B3
# (specify one dummy antenna type, dummy antenna origin,
# and one dummy item in antenna list).
#
# *****
# B1: Define Antenna Types
# *****
#
# Two lines for each type.
# Line1: type ID, ant code
# Line2: parameters
#
# Type ID must start from 1 and increment by 1 thereafter
#
# Ant Code meaning parameters
# -----
# 1 pattern file filename(ascii)
```

```

# 2 dipole length(real)
#
# Antenna Types list:
#
# Enter number of antenna types:
1
# Type #1
1 2
1.0
#
# *****
# B2: Enter origin of antenna coord in main coord
# *****
#
0.0 20.0. 5.0
#
# *****
# B3: Create Antenna List
# *****
#
# Three lines for each antenna.
# Line1: Type ID, location (x,y,z), power (watts), phase(deg)
# Line2: Local x-axis in main coord.
# Line3: Local z-axis in main coord.
#
# Enter number of antennas:
1
#
# Antenna #1
1 0.0 0.0 8.0 1. 0.
1. 0. 0.
0. 0. 1.
#
# *****
# C---Observation points
# *****
#--- Observation points defined with respect to main coord. system 7.
# Enter method of specifying list of points.
# (1 = here, 2 = file):
2
#--- If points are listed here, enter number of points (kobot):
1
#--- If listed here (1 above), List xyz of points in main coord 7
# (one point at a line). If 2 above, include one dummy line.
1. 2. -11.00
#--- If points listed in file (2 above), enter name of file.

```

```

vertical_plane.list
#--- Include direct Tx to observer contribution.
# If you turn on the direct contribution from the transmitter to the
# observation point, computed result will be the total field, which is
# the incident + scattered field. For propagation analysis, this is
# the preferred setting. Otherwise, the result only includes the
# scattered field.
#
# Include direct contribution from transmitter to observation point (rx)
# (1 = yes, 0,2 = no):
1
#--- Compute received power into Rx antenna.
# Urbana always computes field levels at the observation point.
# If you specify an Rx antenna, Urbana will also compute the received
# power and record the results in the (runname).couple file.
# This causes a moderate but slow-down when using the SBR method (below).
#
# Include Rx antenna (1 = yes, 0,2 = no):
2
#--- Rx antenna specification
# Remaining entries in Section C can be ignored if not including
# an Rx antenna.
# Enter antenna type (1 = pattern file, 2 = dipole):
1
# Each antenna type requires additional parameters.
# List of expected parameters follows. Choose one.
#
# Type Description Expected Parameter(s)
# 1 Pattern File File Name (e.g., beam.antpat)
# 2 Dipole Length (in prevailing unit)
#
# Enter parameter(s) on next line:
shdip.antpat
#--- Rx antenna orientation
# Enter local x-axis of Rx in global coordinates
1. 0. 0.
# Enter local z-axis of Rx in global coordinates
0. 0. 1.
#
# *****
# D---Theoretical consideration
# *****
#--- Choose method of computation
# 0 = compute fields in the ABSENCE of the scatterer
# 1 = compute fields by SBR
# 2 = compute fields by GO

```

```

2
#--- If SBR, select a PO integration scheme at bounce points
# 1 = do integration at first & last bounce points only
# 2 = do so at all bounce points (GTD formulation)
# 3 = do so at all bounce points (PTD formulation)
2
#--- Edge diffraction
# SBR can be enhanced with PTD edge diffraction.
# GO can be enhanced with GTD edge diffraction.
# Add edge diffraction (0,2=no, 1=ILDC (SBR or GO), 3=UTD (GO only)
3
#--- If edge diffraction switched on, enter name of edge file
# (e.g., wall.edge or dummy if edge not included).
vertical_plane.edge
#--- Choose method of ray launch
# 1 = by (baby) facet, achieving a uniform first bounce surface density
# 2 = uniform angular distribution (burst launch)
# (If computation by GO, must select 2 = burst launch)
2
#--- If ray launch by (baby) facet (1 above), enter ray density:
# # rays/wavelength (normally 5-10)
5.0
#--- If burst ray launch (2 above), enter angular interval (deg).
# (Typically 0.25 - 2.0 deg)
2.0
#--- max permissible ray bounces (normally 5-10)
5
#--- max-voxdepth = max depth of BSP tree (normally 20)
# max-voxl = max facets in each voxel(normally 10)
# (Larger voxdepth & smaller voxl lead to faster ray tracing
# but more computer memory)
15,10
#--- ICOAT for absorbing facets
888
#--- IQMATRIX for divergence factor
# 1 = calculated by Q-matrix
# 2 = ignored except for the spherical wave spread
2
#--- IF using Q-matrix, name target curvature file(e.g. wall.curv)
dummy.curv
#--- IPEC=1 if all pec, =2 if coating present
2
#--- For PEC scatterer, give the magnitude of reflection coeff
# (use 1.0 for ideal PEC, use less for rough PEC--fudging)
1.0
#--- IF PEC, the rest coating info is dummy

```



```

# -----
# For GO method, terrain generates 100% blockage, and blocked rays leave
# no energy behind a hill. With this feature, LOS rays and UTD edge
# diffraction rays can pass through terrain, with some attenuation.
# Attenuation is measured in dB per hill. Each hill is identified
# by two passages through two terrain facets.
# Can only be used with GO method (and UTD edge option).
# Use simple terrain model: 1 = yes, 2 = no (regular case)
2
# Enter coating code range of terrain facets (e.g., 1, 2):
1 1
# Enter amount of attenuation per hill (dB, > 0):
5.
# -----
# ADVANCE3: APPROXIMATE DOUBLE DIFFRACTION MODEL
# -----
# For GO + UTD method, only single diffraction is considered.
# With this feature, double diffraction is approximated by identifying
# surfaces which block the single diffraction, such as building walls.
# If one or two facets block the path from the single diffraction point
# to the transmitter, the diffraction is still included, but with attenuation.
# Works best if "diffracting facets", marked by their coating code, are
# always associated with enclosed structures with well defined edges.
# Use double diffraction model: 1 = yes, 2 = no (regular case)
2
# Encounter coating code range of diffracting facets (e.g., 5, 10):
2 2
# Enter amount of attenuation for second diffraction (dB, > 0);
10.
# -----
# ADVANCE4: ACCELERATION
# -----
# For large scenes, run time grows both with the number of field
# observation points and the number of edges. Normally, all combinations
# of lit edges and observation points are considered. This feature
# accelerates the processing by limiting the scope of considered edge
# interactions to region around the LOS path from the transmitter
# to the observation point. For example, to run a 5 km by 5 km scene,
# one may choose a 250 m interaction radius. For each observation
# point, edges are ignored that lie outside an ellipse whose foci are the
# Tx and the observation point and whose major axis is the LOS distance
# plus 500 m (radius x 2).
# This feature can also be used to automatically filter edge files
# whose domain far exceeds the domain of observation points.
# Only use this feature for terrestrial simulations where the scene
# is nominally parallel to the x-y plane.

```

```
#
# Use large scene acceleration: 1 = yes, 2 = no (regular case)
2
# Enter radius of interaction
250.
# -----
# ADVANCE5: MULTI-DIFFRACTION
# -----
# Substitute for Adv. #3. Uses ray rubber-banding algorithm to find
# path from transmitter to receiver.
# Can only be used with GO. Cannot be used in conjunction with Adv. #3.
# If UTD switched on above, will take measures not to double count
# single diffraction mechanism.
# Use multi-diffraction model: 1 = yes, 0,2 = no
1
# Enter coating code range of diffracting facets (e.g. 5, 10):
2 2
```

## LIST OF REFERENCES

- [1] [www.wi-fi.org/OpenSection/pdf/Whitepaper\\_Wi-Fi\\_Enterprise2-6-03.pdf](http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Enterprise2-6-03.pdf), July 2003.
- [2] [www.cisco.com](http://www.cisco.com), August 2003.
- [3] K. Pahlavan, T. Probert, and M. Chase “Trends in Local Wireless Networks,” *IEEE Communications Magazine*, pp. 88-95, March 1995.
- [4] [www.qiiq.com/products/productsWireless.htm](http://www.qiiq.com/products/productsWireless.htm), September 2003.
- [5] Robert K. Crane, *Propagation Handbook for Wireless Communication System Design*, Chapter 1, pp. 1-20, CRC Press, Florida, 2003.
- [6] [www.saic.com/products/software/urbana/](http://www.saic.com/products/software/urbana/), September 2003.
- [7] S. R. Saunders, *Antennas and Propagation for Wireless Communication Systems*, John Wiley & Sons, New York, 1999.
- [8] Elmo Garrido, “Graphical User Interface for a Physical Optics Radar Cross Section Prediction Code,” Master’s thesis, Naval Postgraduate School, September 2000.
- [9] [www.zeuswireless.com/support/fresnel-zone.php](http://www.zeuswireless.com/support/fresnel-zone.php), September 2003.
- [10] [www.qsl.net/n9zia/wireless/pdf/best\\_doc.pdf](http://www.qsl.net/n9zia/wireless/pdf/best_doc.pdf), November 2003.
- [11] [www.proxim.com/support/all/stratum/technotes/tn2001-08-13a.html](http://www.proxim.com/support/all/stratum/technotes/tn2001-08-13a.html), November 2003.
- [12] [www.waverider.com/en/techsupport/training/basics.html](http://www.waverider.com/en/techsupport/training/basics.html), November 2003.
- [13] Paul P. Sumagasay, “Vulnerability of WLANs to Interception,” Master’s thesis, Naval Postgraduate School, September 2002.
- [14] “Urbana Wireless Toolset Training Handouts,” Science Application International Corporation (SAIC), San Diego.
- [15] [www.freespaceoptics.org](http://www.freespaceoptics.org), November 2003.
- [16] [www.freespaceoptics.org/pdf/WhitePaper\\_WLANconnect.pdf](http://www.freespaceoptics.org/pdf/WhitePaper_WLANconnect.pdf), December 2003.
- [17] [www.milan.com/wireless/shair\\_bridge\\_antenna\\_specs.html](http://www.milan.com/wireless/shair_bridge_antenna_specs.html), November 2003.

THIS PAGE INTENTIONALLY LEFT BLANK

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Chairman, Electrical & Computer Engineering Department  
Code EC  
Naval Postgraduate School  
Monterey, California
4. Professor David C. Jenn  
Code EC/JN  
Naval Postgraduate School  
Monterey, California
5. Professor Jeffrey B. Knorr  
Code EC/KO  
Naval Postgraduate School  
Monterey, California
6. Professor Richard W. Adler  
Code EC/AB  
Naval Postgraduate School  
Monterey, California
7. Professor Yeo Tat Soon  
Director, Temasek Defence Systems Institute  
Block E1, #05-05  
Singapore
8. Mr. Goh Aik Hoong  
Director (AVS), Singapore Technologies Aerospace  
540 Airport Road, Paya Lebar  
Singapore 539938