The Analysis and Design Strategy in the Deployment of Wireless Communications for Innovative Campus Networks

Jamaludin Sallim

Faculty of Computer Systems & Software Engineering,
University College of Engineering & Technology Malaysia
Locked Bag 12, 25000 Kuantan, Pahang, Malaysia.

Abstract. This paper describes the fundamental concept of analysis and design strategy for an effective deployment of wireless communications for innovative universities or colleges campus that insistently deploys the wireless networks. The extensive use of wireless technologies in university campus has made various respective computer applications such as electronic transactions and electronic learning (e-learning) environments become more energetic. Usually, for the innovative campus network, when deploying wireless communications, most IT Managers/Engineers begin the project by jumping into technical matters, such as deciding upon which approach, technique or standard to use, which vendor to select, and how to overcome the various limitations. These are important elements of implementing wireless communications for innovative campus; however prior to getting too far with the project, the respective IT Managers/Engineers must give vigilant attention to analysis and design strategy in order to wind up with an effective deployment.

1 Introduction

Innovative campus doesn't mean 'new campus' but it refers to learning and teaching environment that desires sophisticated infrastructure and electronic-based transactions with latest and appropriate technology. Supported by advanced technologies, an innovative campus is designed to optimize efficiencies of management, education, and research productivity of the campus, through systematic management of campus information flows.

The innovative universities, with many students, should deploy sufficient wireless communications throughout the campus. Students and faculty are able to take advantage wireless solution. Since the usage at the various faculties growing rapidly, officials needed to ensure students and faculty had enough bandwidth to do research and studies now and into the future. The wireless network covers much, but not all of the campus, including many open spaces, because of leakage from surrounding buildings. It is possible to walk across campus without losing connection. If the connection is lost, eg, when changing floors within a building, then it is automatically restored without needing to log on again.

Sallim J. (2005).
The Analysis and Design Strategy in the Deployment of Wireless Communications for Innovative Campus Networks.
In *Proceedings of the 4th International Workshop on Wireless Information Systems*, pages 124-137
DOI: 10.5220/0002572101240137

Higher bandwidth applications are needed to support the broad variety of academic programs at the university. In campus, wireless communications also encourages students to use laptops so the freedom to move around in a lab or other locations and still have access to the intranet or internet from anywhere is critical. Requirements analysis of wireless deployment in campus includes immediate and future needs of the users, university, and the existing information system. Requirements analysis are what the wireless communications must comply with, such as range, throughput, security, battery longevity, application software, operating systems, end-user hardware, etc. Some of these requirements are obviously different and more complex than what we need to consider for wired networks, so we should pay closer attention when deploying wireless solutions.

Keep in mind that the intent of defining the requirements is to determine what the wireless communications must do, not how it will do it. Avoid making technical decisions when defining requirements unless there is company mandates in place that tell us otherwise. For example, the selection of 802.11b over 802.11a is likely not a requirement. Our choice of 802.11b in the requirements stage could limit the ability to support other requirements not yet known. Before making that selection, we first need to fully understand other requirements, such as throughput requirements of applications, number of end-users, ranges, etc. It's best to leave the technical decisions to the design stage after all requirements are well defined and agreed upon.

After we have a firm set of requirements then we will focus on design. This determines how we are going to satisfy requirements with least cost. Consider technical alternatives for satisfying the requirements by choosing appropriate standard, selecting a vendor, identifying access point locations, assigning channels to access points, choosing security mechanisms, etc. The design should fully describe what components and configurations are necessary to satisfy the requirements.

Through the design process, produce a design specification that highlights the chosen design elements and provides a diagram indicating the placement of access points within the facility. For smaller networks, we may only spend a day or so designing the solution. In larger implementations, it may take weeks or months to fully define enough technical detail before moving forward with the acquisition of hardware and installation services. These larger projects will likely benefit from simulation, prototyping, or pilot testing as part of the design to ensure we have made the right choices and the requirements are fully realizable.

2 Campus Wireless Deployment Considerations

Ahead of deploying a wireless installation in campus, a typical study should be made by obtaining the feedback from other campuses or educational institutions that already deployed wireless communications at their premises. This is very important in order to identify the deployment considerations such as RF interference, poor performance, and security holes will wreak havoc. By handling considerations during the early phases of the deployment, we will significantly increase the success of an innovative campus wireless communications. With a firm understanding of requirements, we should consider the following elements when evaluating and resolving considerations for deploying wireless communications:

2.1 RF interference

RF interference is still plaguing wireless communications deployments. Many universities have gotten by without any problems, but some have installations that don't operate as well as planned. The perils of interfering signals from external RF sources are often the culprit. As a result, it's important that we're fully aware of RF interference impact and avoidance techniques.

2.2 Interoperability issues

For huge campus that have various building infrastructure, multi-type of user, access, applications and already deployed various wireless product will contribute to this considerations. The lacks of interoperability among various wireless standard such as 802.11 FHSS, 802.11b DSSS, and 802.11a OFDM causes problems in some cases. Even though these standards are all 802.11, they don't interoperate with each other. With so many standards, we run the risk of not allowing some users on the wireless communications.

2.3 Security issues

Security is essentially one of the crucial issues related to the project. The avenues of attack and considerations which involves physical security, network security and application security are the main issues in wireless communications. Many universities use wireless Ethernet as a drop-in replacement for Ethernet when mobility is needed or when wiring is difficult or impossible. Some historic or old building are very limited in wiring possibilities so wireless Ethernet in the only option for network communications. Network that permit roaming are often large and cover vast distances. Furthermore the potential for an unauthorized person accessing corporate information is a significant threat for wireless communications.

2.4 Applications interfaces

In some cases, interfaces with applications located on various hosts and servers can bring about major problems when using a wireless communications. A relatively short loss of communications due to RF interference or poor coverage area causes some applications to produce errors. This occurs mostly with legacy applications lacking error recovery mechanisms for wireless systems.

2.5 Unclear requirements

The deployment of campus wireless communications without first clarifying requirements, then the wireless connection may not satisfy the needs of the users. In fact poor requirements are often the reason why information system projects are unsuccessful. For instant, The Engineering School was one of the first buildings to be wired, and now requires its students to have laptops. Many of the 800 students are now moving to wireless, but the building was designed for 2 Mb/s. They have 16 access points in the building; but are looking to redesign the network. Thus, this type of requirements must be identified clearly.

2.6 Product availability

Solid requirements and an effective design significantly reduce most deployment considerations, assuming the design specifies products that are actually available when we need them. The trouble is that vendors often miss projected release dates and have limited volumes when the products are first available.

3 Deployment Analysis

For the innovative campus network, there is some common wireless communications requirements analysis in the order in which we should define them:

3.1 Facility

A facility describes what the universities provide that includes the floor plan, type construction, and possible locations for mounting access points. All of this will capture the environment in a way that will help us choose the right design alternatives. Wireless communication is perceived as more flexible and convenient for campus based students and good preparation for the realities of mobile computing in real working life. Also, staff perception of wireless communication is that it is just an access technology and that the major pedagogical change was the move to laptops. There seems little overt thinking about new pedagogical opportunities created by mobile computing, although some developments in Equine Studies, using PDAs to collect data and feed it into the network are evidence of creativity.

3.2 Applications

Ultimately, the wireless communications must support electronic based transaction, teaching and learning applications, so be sure to fully define them in the requirements. This could be general office application, such as web browsing, email, and file transfer. Application requirements enable we to specify throughput and data rates when designing the system.

3.3 Users

There are various type and number of users (students, lecturers and staff) who will use the wireless services. It is required to identify whether users are mobile or stationary, which provides a basis for including roaming in the design. Mobile users will move about the facility and possibly roam across IP domains, creating a need to manage IP addresses dynamically. Some users, however, may be stationary, such as wireless desktops.

3.4 Coverage Areas

This is most important requirement that extremely affects the deployment design. The coverage area can be split to two elements as described as follows:

Coverage from a Single AP

The data rate is a function of distance, so the farther a user is from the AP, the weaker the signal and the lower the data rate. The distance at which a particular throughput can be achieved will vary with IEEE 802.11a or 802.11b WLANs. 802.11b has a data rate of 11 Mbps and a radius of 30 meters (100 feet) when indoors. 802.11a is so new that detailed measurements on coverage are scarce, but the radio manufacturers expect that we should be able to get 36 Mbps at a 23-meter (75-feet) radius.

Data Rate

Many APs have an auto-step feature that will automatically decrease their data rates as the RF signal degrades. So an 802.11b AP is expected to step down from 11 Mbps to 5.5 Mbps to 2 Mbps to 1 Mbps. Similarly, an 802.11a AP is expected to step down from 54 Mbps to 36 Mbps to 24 Mbps to 12 Mbps to 6 Mbps. Figure 1 shows the relationship between data rate and coverage.

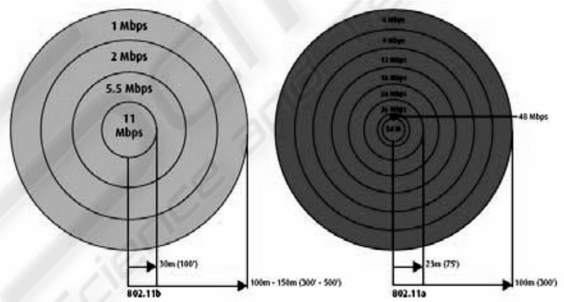
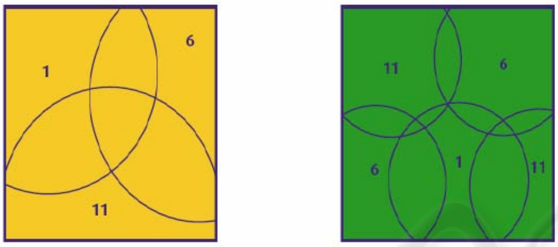


Fig. 1. 802.11 association rates are highest closest to the access point

With IEEE 802.11a WLANs we must be in very close range of an access point to maintain an association rate of 54 Mbps. It's most realistic that the average user will be within 15 meters (50 feet) of an access point, which would allow them to maintain an association rate of 36 Mbps. On the other hand 802.11b will allow a user to maintain the maximum 11 Mbps association rate at a range of up to 23 meters (75 feet). [4]

User Density and Cell Size

The number of users and their applications are major drivers of bandwidth requirements. The network architect must account for the number of users within the AP's cell diameter. In a large office or where user density is high, we should design smaller cells to achieve a higher data rate, since walls and other objects will not naturally define the cells. With smaller cells, we will need to re-use frequencies more often and thus ensure that the channels do not overlap. Figure 2 shows how different cell sizes will increase throughput and improve the user experience. [4]



100 users per office	100 users per office
11 Mb/s peak 802.11b	11 Mb/s peak 802.11b
3 APs per office	5 APs per office
17 Mbps total throughput	55 Mbps total throughput

Fig. 2. Smaller cells will achieve a higher throughput

2.5 Security

This is a requirement that describe the sensitivity of the information being stored and sent over the wireless campus network. We might need to identify a need for encryption if users will be transmitting sensitive information over the wireless communications.

2.6 End User Devices

It is required to specify the end user devices (e.g., hardware and operating system) to ensure the solution accommodates them. For instance, we should specify that users will have laptops running Windows XP or any operating system that have various of interfaces. This provides a basis for deciding on the type of 802.11 NIC and drivers to use, as well as assessing the type of middleware that we can use.

2.7 Battery Longevity

The 802.11 NIC will draw current at a couple hundred milliamps and batteries under this load will last from a couple hours to a day or so, depending on the size of the battery. These are constraints for most applications, but it's beneficial to indicate the amount of battery life that users will realistically need. The most relevant metrics in wireless networks is power. Experimental measurements indicate that communication cost in wireless ad-hoc networks is at least two orders of magnitude higher than computation costs in terms of consumed power. Note that the coverage problem is intrinsically global in the sense that, lack of knowledge of location of any single node implies that the problem may not be solved correctly. Therefore, any algorithm which aims to provide correct solution must inherently use all location data. [5]

2.8 System Interfaces

In most cases, users will need to access information located in servers on the wired-side of the system. It is required to describe applicable end-systems and interfaces so that we can properly design the wireless system interfaces.

2.9 Funding

The requirements stage of a wireless project is a good time to ask how much money is available. If funding limits are known, then we will know how much we have to work with when designing the system. In most cases, however, the university management will ask how much the system will cost. We will then need to first define the requirements and design the system before giving a cost estimate.

2.10 Schedules

It is required to nail down a realistic completion date, though, and plan accordingly. For instance, we may be defining our requirements in January, and a retail store will likely demand that a wireless price marking application be installed by the end of March.

2.11 Coverage and physical installation restrictions

Part of the end user requirement is a desired coverage area, and possibly some physical restrictions to go along with it. Physical restrictions, such as a lack of available electrical power and network connections, can be mundane. Some universities may also require that access points and antennas are hidden; this may be to maintain the physical security of the network infrastructure, or it may be simply to preserve the aesthetic appeal of the building. Some universities may want to provide coverage outdoors as well, though this is confined to mild climates. Any equipment placed outdoors should be sturdy enough to work there, which is largely a matter of waterproofing and weather resistance.

4 Deployment Design

Designing wireless network for innovative campus is a new craft, even for many experienced network architects. When it comes to designing a wired network, most IT managers or engineers are familiar with the steps to ensure sufficient capacity for the users and applications. With IEEE 802.11 wireless LANs, a new factor comes into play: The tradeoff between radio-frequency (RF) coverage and capacity.

4.1 Designing for Signal Loss Factors

A major difference between designing for wired and wireless communications is the RF signal loss caused by attenuation from walls, doors, windows and other objects in the building. The building construction also has an impact: Concrete absorbs more signal than plaster. For instance, a cloth cubicle partition has less attenuation than a concrete wall.

If we are building an 802.11b network, avoid placing APs within a few feet of devices that transmit within the same 2.4 GHz frequency, such as the microwave oven in the lunchroom, any 2.4 GHz cordless phones and Bluetooth devices. 802.11a has fewer interference problems.

4.2 Computing the Number of APs

Once we know the expected total bandwidth, we need to define a minimum over-the-air rate at which the system should function. Some locations may exceed that baseline rate, but we must design for the minimum data rate. For campus-style deployments, a good rule of thumb is to set these baseline association rates as 11 Mbps for 802.11b and 36 Mbps for 802.11a. From there, we can compute the number of APs required for a given service area using the following equation:

$$\frac{\text{Bandwidth x Number of Users x \% Activity Rate per User}}{\text{\% Efficiency x Baseline Association Rate per AP}}$$

where Percentage Efficiency represents the overall overhead efficiency factor, including MAC inefficiency and error correction overhead. For instance, using 802.11b technology, a medium-sized call center wants to provide 500 kbps bi-directional data for 100 employees where the activity rate per user is high throughout the day. The company wants the maximum association rate per AP – with 802.11b technology that translates as 11 Mbps up to 23 meters (75 feet) – and the network is running at 50% efficiency.

The numbers would run like this (multiplying bandwidth by 2 for bi-directional data):

$$\frac{(2 \text{ x } 500 \text{ kbps}) \text{ x } 100 \text{ x } 25\%}{50\% \text{ x } 11 \text{ Mbps}}$$

$$\frac{(1\ \text{Mbps}) \times 100 \times 25\%}{5.5\ \text{Mbps}}$$

$$\frac{25\ \text{Mbps}}{5.5\ \text{Mbps}}$$

4.5 = **5 APs needed**

Always round up the total to the next whole number to ensure adequate capacity. Therefore, in this example, five APs are needed to meet the demands of the call-center's wireless network capacity. Once we have computed the number of APs required based on capacity, we need to calculate how many APs are required for adequate coverage. For high-speed campus deployments, expect that capacity will exceed coverage. We can compute the extent of the AP's coverage at a particular association rate using the receiver sensitivity of the receiving device in conjunction with propagation analysis.

4.3 Placement and Final Settings of APs

Once we know the number of APs required, we can place them appropriately in the coverage area and configure their channel assignments. When allocating channels to the APs, be sure that adjacent APs use non-overlapping channels. 802.11b provides three non-overlapping channels, while 802.11a offers eight or more, depending on the country. For high-speed campus deployments, because the number of APs required for proper capacity is likely to be greater than the number for coverage alone, we will want to lower the AP's transmitted power or set the AP's transmit power appropriately. This will enable us to re-use frequencies while reducing co-channel interference (CCI). Be sure that the chosen brand of APs allows the transmit power to be easily modified from its default (typically maximum) value.

4.4 The Topology Archetype Design

Figure 3 shows how many wireless communications deployments evolve.

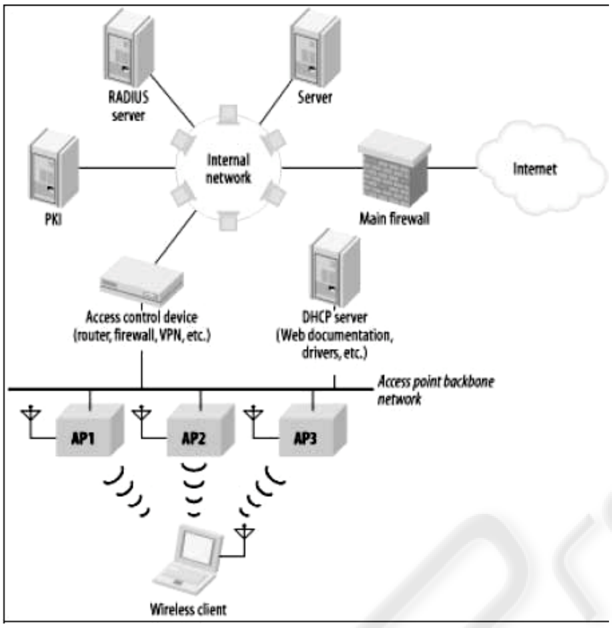


Fig. 3. Standard wireless deployment topology

Some deployments may look like multiple instances of Figure 3. The topology shown in the figure provides seamless mobility between the access points connected to the access point backbone network. In very large deployments, such as a campus-wide deployment across a large number of buildings, it may be desirable to limit the coverage areas in which seamless roaming is provided. One common strategy is to provide seamless mobility within individual buildings, but not provide roaming between buildings. Each building would have a wireless LAN that looked something like Figure 3, and all the access point backbone networks would ultimately connect to a campus backbone.

4.5 Roaming and Mobility Design

In Figure 3, the network linking all the access points, which we call the access point backbone, is a single IP subnet. To allow users to roam between access points, the network should be a single IP subnet, even if it spans multiple locations, because IP does not generally allow for network-layer mobility. To understand this design restriction, it is important first to appreciate the difference between true mobility and mere portability. The "single IP subnet backbone" restriction of the design in Figure 3 is a reflection on the technology deployed within most campuses.

4.6 Limits on mobility

The access point backbone network must be a single IP subnet and a single layer-2 connection throughout an area over which continuous coverage is provided. It may span multiple locations using VLANs. Large campuses may be forced to break up the access point backbone network into several smaller networks, each of which resembles Figure 3. 802.11 allows an ESS to extend across subnet boundaries, as in Figure 4.

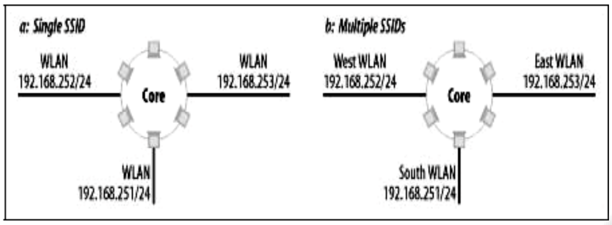


Fig. 4. Non-contiguous deployments

When a campus is broken into several disjointed coverage areas as in Figure 6, be sure to preserve the mobility most important to the users. In most cases, mobility within a building will be the most important, so each building's wireless network can be its own IP subnet. In some environments, mobility may be restricted to groups of several buildings each, so the islands in Figure 6 may consist of multiple buildings.

4.7 Address assignment through DHCP

Multiple independent data sets that must be synchronized are an accident waiting to happen in any field. With respect to wireless LANs, they present a particular problem for DHCP service. To make life as easy as possible for users, it would be best if stations automatically configured themselves with IP network information. DHCP is the best way to do this. Access points frequently include DHCP servers, but it would be folly to activate the DHCP server on every access point.

4.8 Mobile IP and Roaming

Instead of being fixed in a set location, however, access points note when the mobile station is nearby and relay frames from the wired network to it over the airwaves. It does not matter which access point the mobile station associates with because the appropriate access point performs the relay function. The station on the wired network can communicate with the mobile station as if it were directly attached to the wire. Within the context of Figure 3, there are two places to put a DHCP server. One is on the access point backbone subnet itself. Use a single DHCP server per access point backbone or DHCP relay at the access point network router to assign addresses to wireless stations.

4.9 Deterministic Coverage

In order to achieve deterministic coverage, a static network must be deployed according to a predefined shape. The predefined locations of the sensors can be uniform in different areas of the sensor field or can be weighted to compensate for the more critically monitored areas. An example of a uniform deterministic coverage is the grid-based sensor deployment where nodes are located on the intersection points of a grid. In this case, the problem of coverage of the sensor field reduces to the problem of coverage of one cell and its neighborhood due to the symmetric and periodic deployment scheme. [5]

An essential goal in wireless deployment is to ensure all areas are adequately covered. The coverage of each wireless cell depends on the location of the access point and the antenna used. Office spaces often have internal walls and obstacles and are rarely circular. A careful plan is necessary to maximize coverage and performance with the fewest possible access points and least susceptibility to co-channel interference. Due to variability in the composition and thickness of building materials the only guaranteed way of determining the cell coverage area of an access point is by on-site measurement. However, there are some general guidelines that will help with planning: [13]

a. In an open plan office such as those with cubicles, there should be little attenuation of the radio signal. An 802.11b or 802.11g access point with an omni directional antenna will provide a cell with radius of around 328ft/100m (100ft/30m of this at maximum data rate). An 802.11a access point will cover an area with an approximate radius of 164ft/50m (30ft/10m at the maximum data rate). [13]
b. 2.4 GHz (802.11b and 11g) wireless signals will generally penetrate internal walls although there may be some signal attenuation, especially if the walls are made from cinderblock. It is worth noting that internal walls often have part-metal construction and this can increase signal attenuation, too. [13]
c. 5 GHz (802.11a) signals do not penetrate interior walls well and this should be taken into account when planning. [13]
d. In a multi-floor building, there may be some signal leakage between floors. For example, an access point mounted midway between the floor and ceiling on the second floor may radiate signals through to adjacent floors depending on the gain and coverage of the antenna. This can be especially relevant for the floor above a ceiling-mounted antenna. [13]

5 CONCLUSION

Colleges and universities are embracing wireless-networking technology with an enthusiasm that gives new meaning to the term "academic freedom”. Wireless campus networks require elegant deployment planning, analysis and design because every faculty, centers has its own requirements. Wireless campus networks depend on having a solid, stable, well-designed wired network in place. If the existing network is not stable, chances are the wireless extension is doomed to instability as well.

Wireless communications must scale to meet universities demands, ensuring high throughput, secure mobility, and a seamless integration with the wired network.

ACKNOWLEDGEMENT

This study is based on author's experiences, observations and findings when studying and working in few universities and companies since four years ago. With reviewing some of wireless conference and white papers, a lot of useful ideas had been taken to emerge a fundamental exercise for IT Managers/Engineers in universities in deploying wireless communications in their campus. The author would also like to thanks to all parties who give a generous and brilliant ideas in producing this paper.

REFERENCES

1. Shotsberger, P, G, Vetter, R, "Teaching and learning in the wireless classroom", Computer, Vol, No 34, March 2001, pp 110-111.
2. Holmes, A, Schmidt, K, J, "Do mobile and wireless technologies add value to higher education", In Proceedings of Frontiers in Education (FIE), Boston MA. Vol, No 1, November 2002, pp 455-458.
3. J. Geier : WLAN Deployment Risks. White Paper, Wi-Fi Planet, USA, 2004.
4. "Designing WLANs", White Paper, Trapeze Networks, USA, 2004.
5. Seapahn Meguerdichian, Farinaz Koushanfar, Miodrag Potkonjak, Mani B. Srivastava, "Coverage Problems in Wireless Ad-hoc Sensor Networks", Infocom 2001.
6. S. Arnesen and K . Haland, "Modeling o f Coverage in WLAN," PhD Thesis , Agder Univ ersity, 2001.
7. M. Haenggi, "Analysis and Design of Diversity Schemes for Ad Hoc Wireless Networks", IEEE Journal on Selected Areas in Communications, 2004. Accepted for publication.
8. Koo, S. G. M., Rosenberg, C., Chan, H. -H., and Lee, Y. C. , "Location Discovery in Enterprise-based Wireless Networks: Implementation and Applications", In Proceedings of the 2nd IEEE Workshop on Applications and Services in Wireless Networks (ASWN 2002), Paris, France, Jul 3-5, 2002.
9. J. N. Laneman and G. W. Wornell, "Energy-Efficient Antenna Sharing and Relaying for Wireless Networks",' in Proc. IEEE Wireless Comm. and Networking Conf. (WCNC), Chicago, IL, Sept. 2000.
10. V. Erceg et al, "Channel Models for Fixed Wireless Applications," IEEE 802.16a standards document, July 2001.
11. Maxim, M, Pollino, D, "Wireless Security", 1st ed., McGraw-Hill/Osborne: pp.191-195.
12. Franklin, Tom, "Wireless Local Area Networks", White Paper, TechLearn,.
13. "Deploying 802.11 Wireless LANs", 3Com White Paper. www.3Com.com/wireless