UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE ENGENHARIA ELÉTRICA E INFORMÁTICA
UNIDADE ACADÊMICA DE ENGENHARIA ELÉTRICA

ESTUDO DO DESEMPENHO ELETROMAGNÉTICO E DO ATENDIMENTO ÀS NORMAS DE UM SERVIDOR DE INTERNET SEM FIO EM AMBIENTES FECHADOS

TRABALHO DE CONCLUSÃO DE CURSO

Aluno: Leonardo Teodosio da Costa
Matrícula: 20421135
Professor Orientador: Rômulo Raimundo Maranhão do Valle

Campina Grande, Paraíba
Março de 2010

LEONARDO TEODOSIO DA COSTA

ESTUDO DO DESEMPENHO ELETROMAGNÉTICO E DO ATENDIMENTO ÀS NORMAS DE UM SERVIDOR DE INTERNET SEM FIO EM AMBIENTES FECHADOS

Trabalho de Conclusão de Curso submetido à Unidade Acadêmica de Engenharia Elétrica da Universidade Federal de Campina Grande como parte dos requisitos necessários para se obter o grau de Bacharel em Engenharia Elétrica.

Campina Grande, Paraíba
Março de 2010

LEONARDO TEODOSIO DA COSTA

ESTUDO DO DESEMPENHO ELETROMAGNÉTICO E DO ATENDIMENTO ÀS NORMAS DE UM SERVIDOR DE INTERNET SEM FIO EM AMBIENTES FECHADOS

Data de Aprovação: __ / __ / __

BANCA EXAMINADORA:

_____

Rômulo Raimundo Maranhão do Valle
Universidade Federal de Campina Grande
Professor Orientador

_____

Professor Convidado
Universidade Federal de Campina Grande
Avaliador

Campina Grande, Paraíba
Março de 2010

Dedico este trabalho aos meus queridos pais, irmãos e amigos.

Agradecimentos

À toda minha família, e especialmente aos meus pais, pelo incentivo e compreensão durante o período do desenvolvimento deste trabalho;

Ao meu orientador, Professor Rômulo Raimundo Maranhão do Valle, pela orientação e entusiasmo;

Aos meus amigos, Manoel Sátiro Neto, Éder Alelaf, Joálison Guedes, Jamison Mota, Giovanni Sátiro, Genildo Vasconcelos, Aluísio Júnior, Antonildo Pereira, entre outros, que contribuíram durante minha passagem por Campina Grande e que estiveram ao meu lado durante ao curso me ajudando nos momentos mais difíceis;

Ao técnico do laboratório LEMA, engenheiro Galba Falcão, pela contribuição direta no desenvolvimento de testes que acompanham o trabalho e pela confiança e incentivo para iniciar e completar esta empreitada.

Resumo

Recentemente, tem sido observado um crescimento explosivo da utilização de redes de acesso local sem fio (*Wireless Local Area Networks – WLANs),* utilizando equipamentos de nível de radiação restrito operando em bandas independentes de outorga de uso de rádio freqüência, tanto para uso corporativo como doméstico e para prover acesso pago em ambientes públicos como aeroportos, hotéis, centros de convenções e mesmo restaurantes e cafés. Se estas redes serão complementares ou competidoras das redes celulares de terceira e quarta gerações é ainda uma questão polêmica aberta.

Este trabalho tem como objetivo estudar a instalação e o desempenho do servidor internet sem fio DI-524 localizado nas dependências do bloco CJ do Departamento de Engenharia Elétrica da UFCG. O estudo de caso buscará avaliar o melhor modelo de estimativa do sinal para o caso “indoor”, dentre os que a bibliografia propõe.

Sumário

Lista de Figuras

1. Introdução

A internet é hoje uma ferramenta de uso generalizado na sociedade e o crescente número de usuários por serviços e entretenimento, através de seu uso, tem levado a busca de soluções tecnológicas que tornem sua utilização cada vez mais cômoda e versátil. Este é o caso da internet sem fio, solução que vem substituindo a alternativa "via cabo" não apenas em áreas de instituições comerciais e industriais mas, também, em residências bem como em parques, praças, aeroportos e outros ambientes públicos. A internet móvel passou a ser, assim, a extensão da rede mundial de informações continuando a interligar pessoas e computadores aonde possam os usuários se encontrar.

Na engenharia, a tecnologia "sem fio" se apresenta mais heterogênea do que há pouco tempo atrás. Como exemplo, citamos a atual coexistência de diversos padrões buscando espaço no mercado. Um outro aspecto se refere ao do desempenho eletromagnético do sinal radiado. Para o caso "indoor", existem questões relevantes que devem ser consideradas, já que as condições de propagação diferem consideravelmente daquelas para o caso aberto. Os níveis de potência entre o transmissor e o receptor são reduzidos devido ao fato de existir atenuação introduzida por paredes, tetos e outros elementos no caminho de propagação do sinal. Isto é reforçado ao se considerar que os níveis de potência usados em tais sistemas são muito baixos. Como existe mais que um modelo para estimar o nível do sinal, é importante que seja verificado qual melhor se ajusta aos níveis reais de radiação.

Por último, deve-se ressaltar também o fato de que, por serem redes sem fios, elas se tornam mais vulneráveis a ataques pois existem mais pontos disponíveis para acesso com informações o que facilita a ação dos "hackers".

Neste capítulo é apresentada uma visão geral da tecnologia de WLANs, padronizada pelo IEEE (padrão 802.11), vantagens e desvantagens sobre as redes cabeadas, alguns aspectos em relação à segurança das informações trafegadas e tipos de equipamentos utilizados.

O segundo capítulo aborda sobre alguns aspectos importantes para planejamento de sistemas sem fio, como interferências, polarização, diversidade de antenas, tráfego e topologia de rede, neste caso, especificamente para as WLANs. Este capítulo, dá maior ênfase às características mais importantes para ambientes *indoor.*

O terceiro capítulo apresenta alguns dos principais modelos de propagação determinísticos e semi-empíricos, utilizados para ambientes fechados, bem como uma caracterização do canal de rádio-propagação, que é a base para compreender os efeitos previstos pelos modelos.

1.1 Histórico

Nos últimos 30 anos as tecnologias de comunicações sem fio (*wireless*) se tornaram, progressivamente, bastante maduras e estáveis, tornando-se uma alternativa importante para a evolução das redes de comunicações de dados.

Em 1971 surgiu a primeira rede local sem fio (*Wireless LAN ou WLAN*) [1], um projeto de pesquisa da Universidade do Havaí, chamado ALOHANET, em função do protocolo de acesso utilizado, denominado *ALOHA*. A rede utilizava comunicações via satélite e uma topologia em estrela, com sete computadores instalados em quatro ilhas tentando se comunicar com um computador na Ilha de Oahu. Embora a *ALOHANET* não se qualifique exatamente como uma *WLAN* pela conceituação atual, em função das distâncias envolvidas, por suas demais características pode ser considerada a primeira rede "local" de dados sem fio.

Os primeiros produtos de *WLAN* começaram a surgir, em escala industrial, no início dos anos 1990. A liberação mundial das bandas *ISM* (*The Industrial, Scientific, and Medicine Frequency Bands*) nas bandas de 900 MHz, 2,4 GHz e 5 GHz, que podem ser utilizadas sem necessidade de autorização dos órgãos reguladores, desde que atendendo a limites de emissão espectral, alavancou um significativo interesse nas *Wireless LANs* e um rápido crescimento em sua utilização.

Com o caos formado pelo surgimento de diversas tecnologias proprietárias, a FCC (órgão regulamentador das telecomunicações dos EUA) solicitou ao IEEE que desenvolvesse um padrão, que viria a ser designado como 802.11, para produtos de *WLAN*. Em 1994 os primeiros produtos para a faixa de 2,4 GHz começaram a ser comercializados, e em 1997 a primeira versão do padrão IEEE 802.11 foi emitida. Em 1997 a Lucent, 3Com, Aironet (Cisco), Intersil, Nokia e Symbol se unem para formar a *WECA* (*Wireless Ethernet Compatibility Alliance*). A existência de três diferentes tecnologias dentro do padrão vinha provocando a insatisfação de fornecedores e clientes que buscavam assegurar a interoperabilidade dos dispositivos e a aliança foi criada com este objetivo. A ratificação da "próxima geração" do padrão, o 802.11b também chamado de 802.11HR ou *high rate* – foi concretizada em setembro de 1999 e englobava, além dos já tradicionais fornecedores de *WLAN*, outros mais novos na área, mas não menos tradicionais no mercado das telecomunicações, a exemplo de alguns, como Ericsson, Siemens e Compaq.

A *WECA* começou seu trabalho de associar ao 802.11 o nome *Fidelity* que indica e garante a interoperabilidade entre dispositivos certificados pela entidade. Surge o termo *Wi-Fi* (*Wireless Fidelity*, associado ao padrão 802.11b).

1.2 Visão Geral

As bases da tecnologia *WLAN* são destacadas em portabilidade e praticidade. Estes dois atributos implicam em baixos custos de instalação e operação, pois permitem maior facilidade e menor tempo de implantação e manutenção, além de permitirem mais flexibilidade. Para garantir que as vantagens destas redes fossem cada vez maiores em relação às cabeadas *LANs*, os estudos do IEEE continuaram, resultando em novos avanços na tecnologia 802.11. A tabela a seguir ilustra a evolução desta tecnologia:

	802.11b	802.11a	802.11g
Velocidade	**1,2,5.5 e 11 Mbps**	**6,9,12,18,24,36,48 e 54 Mbps**	**6,9,12,18,24,36,48 e 54 Mbps**
Freqüência	**2,4 GHz**	**5,8 GHz**	**2,4 GHz**
Tecnologia	**DSSS**	**OFDM**	**DSSS-OFDM**
Compatibilidade	**802.11g**	**802.11a**	**802.11b**

Tabela 1 – Padrões *wireless* LAN - comparação

A maioria dos projetos de *WLAN* ainda utiliza a tecnologia 802.11b, pois os equipamentos são mais baratos que os equipamentos da 802.11g, os quais ainda não estão muito difundidos no mercado. Portanto, a capacidade das redes sem fio atuais ainda são, um pouco inferiores às redes cabeadas, mas com a rápida popularização dos equipamentos 802.11g. Outra grande motivação para os estudos em torno do padrão "g" é que este poderá oferecer as mesmas taxas de transmissão do padrão "a", mas mantendo a compatibilidade com o padrão "b", que o padrão 802.11a não permite. A seguir são discutidas as principais características das *WLANs*, metodologias de projeto, vantagens e desvantagens de sua utilização.

1.3 Vantagens e desvantagens das redes sem fio *LAN*

As *WLANs* se tornaram mais populares nos últimos anos devido á redução dos custos de equipamentos sem fio no mercado de telecomunicações. Os custos de instalação de uma rede sem fio já são inferiores aos de uma rede cabeada tradicional. Esta diferença de custos não se deve apenas à redução de preços dos componentes sem fio, mas também à diferença do custo de instalação física destes dois tipos de rede.

Por esta razão, as redes sem fio não vem sendo utilizadas apenas em locais onde se exige portabilidade, como escritórios onde todos os funcionários utilizam *notebooks*, com posicionamento variável, mas também onde se utilizam d*esktops* que dificilmente mudarão sua posição na rede.

As principais vantagens de redes de acesso sem fio sobre redes cabeadas são:

a) **Mobilidade** entre usuários dentro da área de cobertura da rede;
b) **Flexibilidade** para adicionar novos usuários; necessita-se apenas configurar os computadores para que sejam conectados à rede, sem necessidade de uma nova estrutura de cabeamento;
c) **Facilidade** pela inexistência de cabeamentos; assim é possível interconectar prédios afastados, tornando uma rede sem fio muito mais prática e econômica;
d) **Rapidez** influenciando significativamente no tempo de parada (downtime) em relação à redes cabeadas, devido a problemas que no cabeamento (tais como rompimento de cabos e danos a conectores, conversores), que é extremamente maior do que em redes sem fio;
e) **Praticidade** devido à redução na utilização de cabos. A rede sem fio torna-se pronta para uso imediatamente após a configuração do sistema;
f) **Economia** na aplicação da tecnologia. Apesar de ter um custo de instalação maior que a rede cabeada, a tecnologia sem fio pode simplificar o trabalho de administração de usuários e manutenção, uma vez que é móvel, além de reduzir o tempo de inatividade (downtime) e o custo de administração de redes.

As principais desvantagens do uso desta tecnologia, que ainda são questionadas por alguns grupos de fabricantes e usuários, dizem respeito à segurança das informações trafegadas.

1.4 Componentes de *WLANs*

As *WLANs* são utilizadas para conectar usuários em redes locais ou redes em diferentes localidades fazendo acesso mais rápido e a custo competitivo. Conexões ponto-a-ponto e ponto-multiponto permitem acesso à Internet, compartilhamento de arquivos e acesso aos recursos das redes sem necessidades de utilização de fios.

Para tal, são necessários alguns componentes novos em relação aos utilizados nas antigas redes cabeadas.

1.4.1 Access Point (AP)

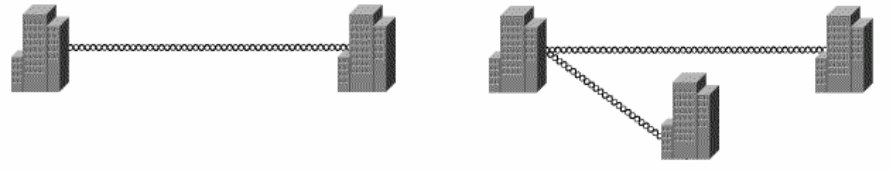
O *Access Point*, comumente chamado de *AP*, exerce a função de distribuir entre os usuários o acesso à rede. Se fizéssemos uma comparação entre as redes sem fio *LANs* e as redes cabeadas *LANs*, poderíamos dizer que um *AP* tem o mesmo papel em uma *WLAN* que um *Hub* tem em uma rede cabeada.

Figura 1 – Exemplo de Access Points(DI-524) e antenas externas.

Um *AP* fornece uma entrada para o *backbone* (cabeado) da rede e uma saída para os usuários através de RF. A maioria dos *APs* são dotados de antenas internas, isotrópicas,ou seja, é considerada um elemento puntiforme, cuja potência irradiada ou recebida é a mesma em todas as direções cobrindo uma área específica, dependendo da potência utilizada pelo *AP* e do ambiente de implantação. Alguns *APs* permitem conexão de antenas externas, para um melhor planejamento da área coberta, provendo um melhor aproveitamento da rede. Alguns *APs* oferecem funcionalidades interessantes para um bom dimensionamento da rede, como a funcionalidade de *Repeater mode* [4], em que pode se configurar o *AP* como um repetidor ativo de um sinal proveniente de outro *AP*. Esta funcionalidade, embora útil, não é muito recomendada, pois o *AP* repetidor oferece baixas taxas de transmissão, já que toda a sua comunicação com seus usuários deve ser encaminhada ao *AP* principal. Outras funcionalidades como podem ser citadas: regulagem de potência de transmissão, diversidade de antenas, saídas cabeadas diversas, criptografia ,entre outras.

1.4.2 Wireless Bridge

Uma ponte sem fio tem a função de estabelecer comunicação entre duas ou mais redes. Esta é uma necessidade comum, quando se deseja interligar dois edifícios em uma mesma rede (para que possa haver compartilhamento de arquivos, servidores etc.) e estes estão separados por uma rua, estrada ou distâncias maiores. Esta conexão é feita entre duas ou mais *Bridges*, portanto, permite configurações ponto-a-ponto ou ponto-multiponto, conforme a figura a seguir:



a) b)

Figura 2 – (a) Conexão ponto a ponto (b) Conexão multi-ponto

A maior parte das *Bridges* existentes no mercado podem ser configuradas em *Repeater mode*, funcionando como um repetidor ativo entre duas outras *Bridges*. Esta funcionalidade é muito útil para estabelecer comunicação entre longas distâncias, acarretando, entretanto, diminuição da taxa de transmissão, já que todos os pacotes recebidos devem ser retransmitidos e este tipo de equipamento é *half-duplex*

Estas interligações podem, muitas vezes, ser temporárias visando oferecer mais flexibilidade durante o processo de implantação. Este tipo de equipamento também pode ser configurado como um *Access Point* comum.

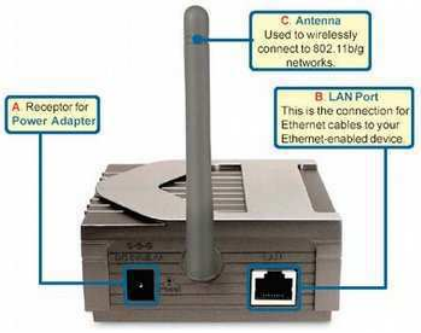


Figura 3 – Exemplo de um Wireless Bridge

1.4.3 Workgroup Bridge (WB)

A grande diferença entre uma *Workgroup Bridge*, comumente chamado de *WB*, e uma *Wireless Bridge*, é que a *WB* é um equipamento "cliente", tendo a função de estabelecer uma "ponte" para um *AP*. Isto é, quando deseja-se incluir um *AP* na rede mas não existe cabeamento até o ponto de instalação, utiliza-se uma *WB* conectada ao *AP* na posição desejada, com uma antena direcional provendo acesso ao local onde existe cobertura. Se deseja-se oferecer cobertura para um número menor que oito usuários (*wired*), não há necessidade de utilizar um *AP* conectado a uma *WB*. Se o usuário desejar instalar um equipamento, como uma impressora, no local onde se está oferecendo a cobertura através da *WB*, pode-se conectar um *Hub* na sua saída (com até 8 portas) e conectar a impressora no *Hub*.

Figura 4 – Exemplo de um Workgroup Bridge

As *WB* também permitem conexão de antenas externas, com o objetivo de estabelecer comunicação com *APs* em posições mais distantes e obstruídas.

1.4.4. Client adapter

O adaptador cliente sem fio, também chamado de *WLAN adapter* ou adaptador de acesso à rede sem fio, é o equipamento para se implementar um ambiente de rede flexível. Estes adaptadores podem ser acoplados a uma grande variedade de equipamentos e são utilizados sob qualquer topologia de rede.

São encontrados no mercado adaptadores do tipo PCMCIA, que podem ser acoplados a *notebooks* e a alguns modelos de *hand helds* (espécie de notebook em miniatura, com o mesmo desenho básico, com o teclado de um lado e a tela do outro), e adaptadores do tipo PCI, utilizados em *desktops*.

Por se tratar de equipamentos "*plug and play*", podem ser utilizados em conferências, reuniões e outros tipos de eventos realizados em ambientes sem infra-estrutura de rede implantada.

Figura 5 – Exemplo de *Client Adapters* (PCMCIA)

1.5. Segurança em redes sem fio

Em relação à segurança, espera-se algo sem falhas, sem risco de perdas, algo bastante confiável. Pensando desta maneira, as redes sem fio estão sendo cada vez mais alvo de ameaças que acabam ocasionando a elas a falta de segurança. A segurança é primordial para o bom andamento das atividades do dia a dia, não se podendo evitar que intrusos localizem sinais da rede, pois como já se sabe os transmissores são omni-direcionais, irradiando ondas de rádio em algumas centenas de metros e para todos os cantos, sendo que qualquer um é capaz de se conectar neste sinal e interceptar os pacotes. Prevendo este tipo de intrusão foram criados mecanismos de segurança para as redes sem fio, que realmente possam garantir que as conexões sem fio, estejam imunes à ingerência destes intrusos e que suas informações estejam trafegando em um ambiente preparado para sua maior confiabilidade e maior usabilidade.

Segurança é o principal problema das redes sem fio e pensando nisso, um grupo de estudo do IEEE, começou a desenvolver técnicas que realmente possam melhorar o tráfego das informações nas redes sem fio. Primeiramente no protocolo WEP(*Wired Equivalent Privacy*), protocolo este, desenvolvido para suprir deficiências das redes sem fio no quesito segurança. Este protocolo está presente em todos os padrões de redes sem fio e com seu surgimento previa-se que acabariam os problemas de segurança que rodeiam as redes sem fio. Em pouco tempo tornou-se um protocolo muito vulnerável e fácil de ser quebrado. Isto se deve ao fato da descoberta de chaves criptográficas fracas utilizadas pelo protocolo.

Com estes problemas, o IEEE iniciou a pesquisa em busca de um novo protocolo criptográfico criando o novo padrão 802.11i, denominado como WPA (Wi-fi Protected Acess). Muitas inovações fazem parte deste protocolo, que busca suprir todas as falhas apresentadas pelo protocolo WEP.

1.5.1 Wireless Equivalent Privacy (WEP)

As redes sem fio ficam expostas a vários riscos tais como, roubo de informações. Buscando proporcionar uma rede sem fio com maior segurança, o IEEE buscou melhorias no quesito segurança e o projeto foi denominado protocolo WEP (*Wired Equivalent Privacy)*. Este protocolo traz a utilização de algoritmos de chave simétrica, no qual, uma chave secreta deverá ser compartilhada entre o concentrador e as estações de trabalho, dando assim liberação para que mecanismos possam cifrar e decifrar fazendo com que as informações tenham sempre um tráfego mais confiável, onde, de acordo com, alguns critérios foram levados em consideração para o desenho deste protocolo: "suficientemente forte, auto-sincronismo, requer poucos recursos computacionais, exportável, e de uso opcional".

Assim que o protocolo WEP é inicializado em uma rede sem fio, ele codifica os pacotes de dados antes da transmissão, usando uma chave fixa que deve estar configurada inicialmente no AP *(Access Point)*, e faz a decodificação no momento da recepção; vale apenas lembrar que o protocolo WEP somente pode codificar dados entre estações 802.11.

O funcionamento do protocolo WEP se dá da seguinte maneira: inicialmente cada parte que deseja participar da transmissão, deverá possuir uma chave secreta, que será utilizada tanto para criptografar os dados a serem transmitidos, quanto para receber e descriptografar os pacotes recebidos. Este processo recebe o nome de criptografia de chave simétrica, simplesmente pelo fato da chave ser única para os dois processos. É extremamente importante que a troca de chaves entre o receptor e o transmissor deverá ser feita de maneira manual, para que não exista chance de comprometer a segurança. O fato que torna o protocolo WEP bastante vulnerável é que a mesma chave secreta utilizada para enviar e receber os pacotes, também são utilizados na autenticação, o que o faz bastante vulnerável neste aspecto.

Quando está havendo a transmissão de mensagens, as mesmas passam primeiramente por um algoritmo denominado de "CHECKSUM", que é um algoritmo que detecta erros aleatórios e que gera um ICV *(Integrity Check Value),* para que no ato da recepção possa ser verificada a integridade das mensagens.

Será utilizado um algoritmo CRC-32 para fazer o controle, esse algoritimo ele gera um ICV de 4 bytes que deverá ser exatamente igual pelo receptor da mensagem, caso contrário a mensagem recebida será imediatamente considerada errada e será descartada. Então o resultado do *checksum* mais a mensagem são concatenados ao chamado texto claro. Em um segundo estágio, é gerada uma seqüência de bits a partir da chave secreta, e de um vetor de inicialização IV (24 Bits), esta seqüência é gerada através do algoritmo de criptografia RC4.

Finalizando o processo de criptografia, faz-se uma operação XOR entre o resultado do checksum, e a seqüência gerada pelo RC4, onde o resultado desta operação constituirá o pacote a ser transmitido. Junto com o pacote cifrado, também é enviado o vetor de inicialização, para que seja possível o processo para decifrar os pacotes. A recuperação do pacote é aplicando com o processo de maneira inversa, onde o receptor terá o pacote cifrado mais o vetor de inicialização.

Em se tendo este vetor e conhecendo a chave secreta, o receptor utiliza o mesmo RC4 para gerar uma seqüência de bits, em que por uma vez tendo esta seqüência, basta aplicar o XOR entre esta seqüência e o pacote cifrado para recuperar o texto claro (pacote original).

Fazendo o XOR da seqüência RC4 com ela mesma, o resultado será zero; portando o XOR de uma seqüência de zeros com o texto claro, onde o resultado do XOR de qualquer número será ele mesmo. Desse modo é possível recuperar o pacote original. Em seguida o receptor divide a mensagem em duas, realiza o cálculo do CRC-32 e compara os resultados obtidos. Se forem iguais, significa que o pacote recebido é válido, portanto será aceito, sendo que este processo é feito para que se tenha absoluta certeza que a integridade dos pacotes foi mantida na transmissão.

1.5.2 Wi-fi Protected Acess (WPA)

Wi-Fi Protected Access (WPA) inicialmente criado para suprir deficiências de segurança é oriundo do protocolo padrão 802.11i criado pela WI-FI Alliance que promete ser o marco na segurança das redes sem fio.

O WPA inclui várias mudanças para que não persistam as mesmas deficiências do WEP. O WPA para ter um bom funcionamento trabalha juntamente com mais alguns protocolos, diferentemente do WEP. No caso o WPA trabalha como o protocolo 802.1x, que é um padrão que visa certificar que apenas o usuário autorizado tenha acesso às informações. O WPA não traz suporta as Redes Ad-Hoc, pois o WPA visa segurança a redes que possuam um AP.

O WPA substitui completamente o WEP, com inovações quanto à criptografia de dados, garantindo também a autenticação de usuários, item que o WEP não contemplava, utilizando para esta garantia protocolos como 802.1x e EAP *(Extensible Authentication Protocol).*

Em soluções mais robustas de segurança, podemos utilizar o WPA, sendo ele utilizado em diferentes modos, sendo em seu modo nativo ou com a utilização de forma combinada com outras tecnologias, bem como a utilização do protocolo 802.1x e certificados digitais. Importante lembrar, que a maior parte dos recursos disponíveis neste protocolo, não é disponível no modo Ad-Hoc.

1.5.3 Wi-fi Protected Acess2 (WPA2)

Wi-Fi Protected Access 2 é a versão melhorada do WPA. Foi oficializado com a especificação 802.11i (ratificada pelo IEEE em junho de 2004). Ela utiliza *o Advanced Encryption Standard (AES)*, ao invés do TKIP (algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacote. A sua principal característica é a frequente mudanças de chaves que garante mais segurança. A senha é modificada automaticamente por padrão a cada 10.000 pacotes enviados e recebidos pela sua placa de rede), que aceita chaves de 28,192 e de 256 bits.

2. Considerações sobre *WLAN* em ambientes fechados

Ao se planejar uma rede *WLAN* em um ambiente fechado (*indoor*), deve se levar em consideração uma série de fatores, como posicionamento dos *Access Points*, para prover a cobertura desejada, número de *Access Points*, para escoar o tráfego planejado, bem como outros parâmetros importantes para a propagação do sinal, como a diversidade de antenas, polarização do sinal e interferências.

Muitos dos fatores comentados neste capítulo, como importantes para um planejamento de uma rede *WLAN* em ambientes fechados, também se aplicam a ambientes externos, não abordados neste trabalho, pois o foco principal são os ambientes *indoor*.

2.1. Interferência

A frequência de 2,4 GHz é liberada no Brasil e em um grande número dos países, isto é, não é necessário se obter nenhum tipo de autorização junto ao órgão responsável local, o que impulsiona ainda mais a utilização de tecnologias que utilizam esta faixa, sejam as *WLANs* baseadas em 802.11, o Bluetooth ou outras tecnologias sem fio menos conhecidas.

Deve ser observado que dois sistemas operando em uma mesma região e na mesma freqüência causam interferência entre si, a ponto de nenhum conseguir estabelecer comunicação de forma satisfatória. Neste sentido, devem ser efetuadas medidas com todos os sistemas existentes em funcionamento, para monitorar o nível de interferência que está sendo gerado. Além de equipamentos de telecomunicações existem outros equipamentos que podem causar interferências na frequência de 2,4 GHz, como os fornos de microondas. Portanto é recomendado que os *Access Points* e os pontos locais mantenham uma certa distância deste tipo de equipamento para uma melhor comunicação.

Para minimizar a interferência intra-sistêmica os dispositivos 802.11 utilizam espalhamento de espectral na transmissão de seus sinais. De acordo com o padrão 802.11, existem três tipos de técnicas utilizadas: *FHSS*, *DSSS* e *OFDM*. Todas estas técnicas têm o mesmo princípio, que se baseia em espalhar a potência do sinal em uma faixa mais larga do espectro de freqüência, reduzindo a densidade de potência do mesmo em freqüências específicas e, conseqüentemente, reduzindo o efeito de interferências a outros dispositivos que utilizam a mesma faixa.

a) FHSS é uma técnica de espalhamento espectral onde a frequência de 2,4 GHz, é dividida em 75 canais, as informações enviadas utilizarão todos este canais, e serão transmitidos em uma seqüência pseudo-aleatória cuja a freqüência de transmissão vai sendo alterada em saltos.

Utilizada somente na especificação IEEE 802.11, a técnica de FHSS remete frações de dados, que são transmitidos por freqüências específicas. Controlando o fluxo com o receptor, que negocia velocidades menores comparadas às velocidades oferecidas pela técnica DSSS, mas menos suscetíveis a interferências devido a cada transmissão ocorrer seguindo um padrão diferente de saltos, minimizando a chance de dois transmissores utilizarem o mesmo canal simultaneamente. Com esse espalhamento, consegue-se um melhor desempenho do sistema, melhorando sua imunidade a ruídos, e impedindo que uma pessoa que não conheça a seqüência de saltos consiga escutar a transmissão.

b) DSSS *(Direct Sequence Spread-Spectrum)* é uma técnica ,no qual, o padrão de bits, chamado chip ou código de chip, permite aos receptores filtrar sinais que não utilizam o mesmo padrão, incluindo ruídos ou interferências. O código de chip cumpre duas funções principais:

- Identifica os dados para que o receptor possa reconhecê-los como pertencentes a determinado transmissor. O transmissor gera o código de chip e apenas os receptores que conhecem o código são capazes de decifrar os dados.
- Os dados são distribuídos pela largura de banda disponível pelo código de chips.

Permite maior possibilidade de recuperação dos dados originais. A tecnologia incorporada no rádio recupera os dados originais, usando técnicas estatísticas sem necessidade de retransmissão, caso um ou mais bits do chip sejam danificados durante a transmissão. Os receptores não desejados em banda estreita ignoram os sinais de DSSS, considerando-os como ruídos de potência baixa em banda larga. As WLANs 802.11b usam uma variação do DSSS denominada HR-DSSS *(High Rate DSSS)* e apresentam maior transferência de dados do que a contraparte FHSS, devido à menor sobrecarga do protocolo DSSS. Estas características do DSSS o tornam mais exposto a ataques.

c) OFDM é a técnica de transmissão baseada no conceito de multiplexação por divisão de freqüência (FDM), onde diversos sinais são enviados em diferentes freqüências. O FDM é utilizado em aparelhos de rádio e televisão, normalmente, cada estação é associada a uma determinada freqüência (ou canal) e deve utilizá-la para realizar suas transmissões. OFDM parte deste conceito e divide uma única transmissão em múltiplos sinais com menor ocupação espectral (dezenas ou milhares). Isto adicionado com o uso de técnicas avançadas de modulação em cada componente, resulta em um sinal com grande "resistência ortogonal" à interferência. OFDM na maioria das vezes é utilizado juntamente com codificação de canal (técnica de correção de erro), resultando no chamado COFDM. Esta tecnologia possui alto grau de complexidade para sua implementação, porém é amplamente utilizada nas telecomunicações, usando sistemas digitais facilitando o processo de codificação e decodificação dos sinais. Sua aplicação é encontrada em tecnologias de *broadcasting* e também em algumas formas de redes de computadores. Sua principal característica quanto ao desempenho, é apresentar uma boa imunidade a multi-percursos, geradores dos famosos "fantasmas" presenciados nas televisões analógicas.

2.2. Polarização

A polarização é determinada em função da orientação do campo elétrico gerado por uma antena em relação a uma referência. No caso de antenas lineares, como o campo elétrico é paralelo ao elemento irradiante, a polarização corresponde à orientação física da antena em relação ao solo. A polarização das antenas deve ser a mesma em todos os pontos de comunicação, para prover uma melhor recepção do sinal.

2.3. Diversidade de antenas

Em ambientes em que não se espera que haja muito efeito de multipercursos, isto é, ambientes com poucas paredes e obstáculos, uma única antena pode prover bons resultados de cobertura. Entretanto, em situações nas quais o sinal está sujeito ao efeito de multipercursos, é recomendável a utilização de uma segunda antena receptora.

A maior parte dos equipamentos de *WLAN* possuem duas antenas, que podem ser ativadas e desativadas pelo usuário, para fins de avaliação de desempenho. Estes equipamentos têm a capacidade de comparar a intensidade do sinal proveniente de cada uma das antenas e aproveitar o mais forte.

Medições efetuadas para comparar o desempenho com a diversidade de antenas ativada e desativada, indicam que em ambientes fechados (muito sujeitos aos efeitos de multipercursos), o nível de potência do sinal recebido é muito sujeito a desvanecimentos de pequena escala quando a diversidade está desativada, melhorando sensivelmente com sua ativação.

2.4. Cobertura

Uma determinada área está coberta por um sistema de telecomunicações quando é possível que se estabeleça comunicação de algum ponto no interior da área com o sistema em questão. No caso de *WLANs* a comunicação se dá entre um *AccessPoint* e os equipamentos dos usuários ou apenas entre equipamentos de usuários. A cobertura deve ser planejada de acordo com a demanda local, onde as variáveis mais importantes são a área a ser coberta, o tráfego, que deve contabilizar o número de usuários simultâneos e o volume de dados trafegados por cada um, bem como o custo de infra-estrutura. Existem alguns tipos de topologias básicas:

a) Redes ad hoc;
b) Redes de infra-estrutura básica;
c) Redes de infra-estrutura ou estruturadas.

As redes ad hoc, são denominadas IBSS *(Independent Basic Service Set),* são compostas por estações independentes, sendo criadas de maneira espontânea por estes dispositivos. Este tipo de rede se caracteriza pela topologia altamente variável, existência por um período de tempo determinado e baixa abrangência dos sinais emitidos.

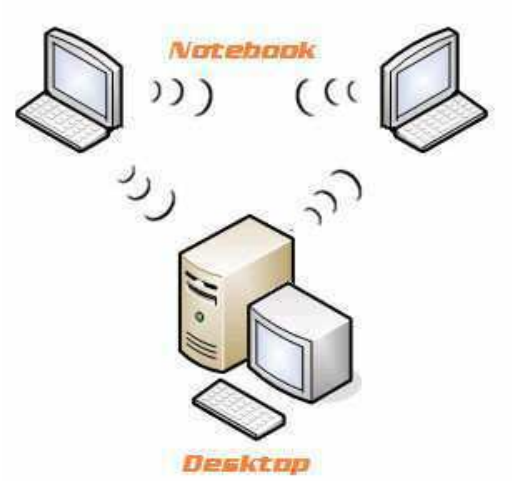


Figura 6 – Redes Ad-Hoc

Como visto em tópicos anteriores, as redes de infra-estrutura básica são formadas por um conjunto de estações sem fio, controladas por um dispositivo coordenador denominado *Access Point* (AP). Todas as mensagens são enviadas ao AP que tem a função de repassá-las aos destinatários. O AP funciona com o mesmo princípio de um equipamento concentrador (hub). O AP pode ser utilizado como uma *bridge* entre a rede sem fios e uma rede com fios. Ao utilizar essa funcionalidade, o AP passa a interagir com dados do nível de enlace das duas redes (layer 2). Estas redes são denominadas BSS *(Basic Service Set)*.

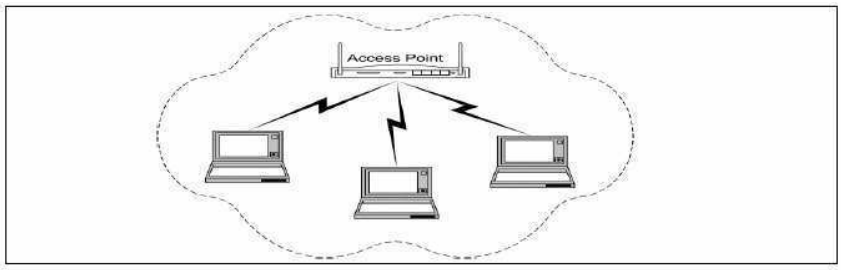


Figura 7 – Rede BSS

São denominadas ESS *(Extended Service Set)* as redes de infra-estrutura. Estas redes são as uniões de diversas redes BSS conectadas através de outra rede com ou sem fio (como uma rede ethernet, por exemplo). A estrutura deste tipo de rede é composta por um conjunto de APs interconectados, permitindo que um dispositivo migre entre dois pontos de acesso da rede. As estações vêem a rede como um elemento único.

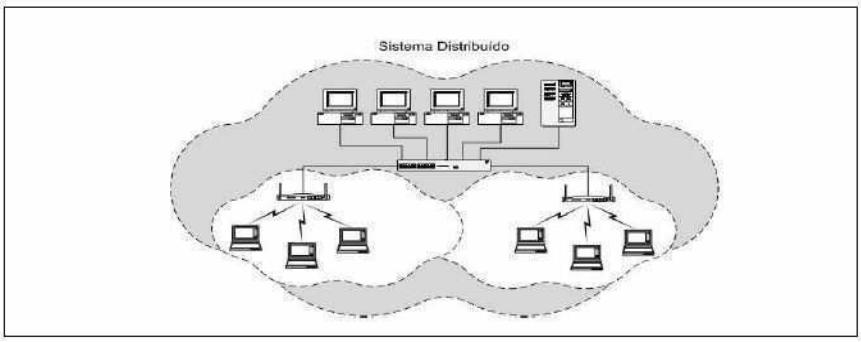


Figura 8 – Rede ESS

Devido à mobilidade das redes ESS, para que um dispositivo possa mover-se entre duas BSS (entre dois APs), é necessário que um sistema distribuído *(WDS – Wireless Distributed System)* esteja disponível na rede. Este sistema deve assegurar-se que as conexões dos dispositivos não sejam perdidas durante a troca de APs, e administrar as possíveis implicações na segurança da rede provenientes desta funcionalidade.

2.4.1. Topologia Peer-to-peer (Ad Hoc)

A topologia *Peer-to-peer*, também conhecida como rede *ad hoc* ou ainda *IBSS – Independent Basic Service Set*, não necessita de *Access Point* para que se estabeleça comunicação entre estações de trabalho. Estas se comunicam diretamente, permitindo compartilhamento de arquivos e, eventualmente, de impressoras e periféricos, acopladas a alguma das estações. Esta topologia é utilizada quando não há necessidade de comunicação com um servidor.

Figura 9 – Topologia Ad-Hoc

2.4.2. Topologia Infra-estrutura

Este tipo de topologia é constituída por um conjunto de estações de trabalho que se comunicam diretamente com um *Access Point*, que por sua vez, funciona como uma ponte entre estas estações e uma rede cabeada.

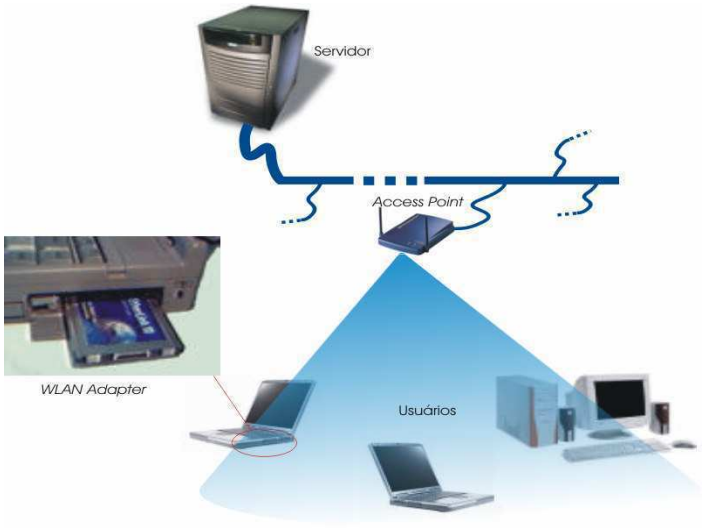


Figura 10 – Topologia infra-estrutura

2.5. Tráfego

Ao se planejar uma *WLAN* é muito importante que se faça um dimensionamento do tráfego requerido pelos usuários na área coberta e, em função deste dimensionamento de tráfego, definir a quantidade de *Access Points* necessários para cobrir a área.

A vazão total gerado em uma área é dado pela soma das vazões gerados por cada usuário. Portanto a capacidade total dos *APs* deve ser maior que este valor estimado.

Por exemplo, no caso do uso de *APs* 802.11b, com uma vazão máxima de 11 Mbps cada, seriam necessários 3 *Access Points* para atender 80 usuários com uma vazão média de 2 kbps.

Atentar para o fato que o valor de vazão nominal dos equipamentos e da regulamentação 802.11 não é o valor real a ser consumido pelos usuários, pois uma parte deste é destinado a sinalização entre as pontas.

3. Propagação em ambientes fechados

3.1. Introdução

O conhecimento do meio de transmissão é indispensável quando se objetiva realizar um bom planejamento de cobertura e desempenho radioelétrico. Nos sistemas sem fio o meio de propagação é o canal rádio, cujas características e efeitos sobre a informação trafegada são de natureza complexa, impossibilitando uma análise completamente determinística, sugerindo assim a utilização de dados experimentais. Medições indicam que as flutuações de pequena escala e de larga escala do sinal em torno do seu valor médio variam de acordo com os modelos Rayleigh ou Rice e log-normal, respectivamente [5]. A partir das medições, também é possível determinar a variação da potência do sinal devido ao movimento de pessoas no ambiente ou ao atravessar obstáculos fixos, como paredes, pisos, vidros, corredores, móveis etc. Todos estes parâmetros são importantes para a construção de um modelo de propagação condizente com a realidade, embora quanto maior a precisão desejada, mais detalhes sobre o ambiente de propagação são necessários como dados de entrada para o modelo.

3.2. Mecanismos de propagação

Há quatro tipos básicos de mecanismos de propagação, são eles: via rádio direto, reflexão, difração e espalhamento. Todos encontrados tanto em ambientes abertos quanto em fechados.

Reflexão: Ocorre quando as ondas eletromagnéticas deparam-se com obstáculos de dimensões maiores que seus comprimentos de onda, que podem ser exemplificados em ambientes indoor como paredes, mobílias, portas entre outros e no caso de ambientes abertos, podem ser montanhas, carros, prédios, casas, etc.

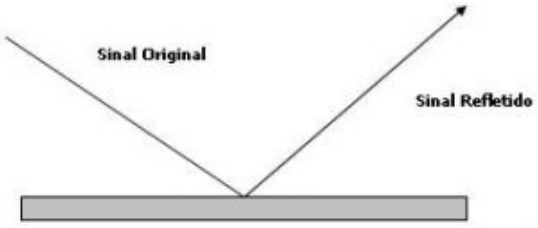


Figura 11– Reflexão do sinal

Difração: Existe quando mesmo obstruindo a passagem do sinal entre o transmissor e receptor, é possível encontrar sinal após o obstáculo. De acordo com o principio de Huygen, onde cada ponto numa frente de onda se comporta como uma fonte isolada, haverá a formação de ondas secundárias atrás do obstáculo, mesmo que não haja visada direta entre o transmissor e o receptor.

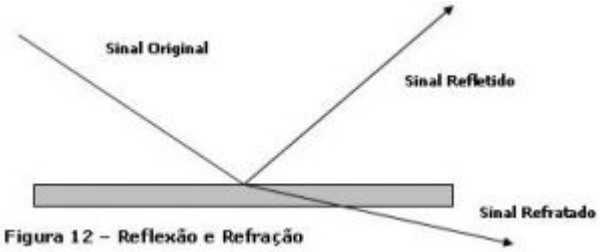


Figura 12– Difração do sinal

Espalhamento: Ocorre quando há obstáculos com tamanho de mesma ordem de grandeza ou menores que as ondas eletromagnéticas. Obedece ao mesmo princípio físico da difração espalhando o sinal do transmissor em diversas direções.

Figura 13– Espalhamento do sinal

3.2.1. Propagação e atenuação

O conceito de visibilidade é importante para rádio-propagação, visto que um enlace de rádio é dito em visibilidade se não houver obstrução, difração ou espalhamento, que o inviabilizem. Para determinar se há ou não visibilidade em um enlace é necessário calcular os limites da primeira zona de Fresnel. A zona de Fresnel é um elipsóide, criado entre as antenas de transmissão e recepção. Para que se possa identificar o raio do elipsóide da zona de Fresnel, utiliza-se a seguinte fórmula:

$$r = 547\sqrt{\frac{D1 + D2}{fxd}}$$

sendo r o raio da elipsóide, D1 a distância em metros entre a primeira antena e a parte da elipsóide que se deseja obter o raio, D2 a distância entre D1 e a segunda antena em metros, f a freqüência da onda em MHz (2.450MHz é utilizado para redes 802.11b e 802.11g) e d a distância total entre as duas antenas em metros.

Caso não existam obstáculos entre as antenas, e a zona de Fresnel esteja livre, a relação direta entre potência recebida e distância dada pela da fórmula de atenuação do sinal de microondas no ar:

$$A_{ar} = 20 \log \left(\frac{4 * \pi * D}{\lambda} \right)$$

onde A_{ar} é a atenuação em dB, D é a distância em metros e λ é o tamanho da onda em metros. Para ondas de 2,4 GHz (802.11b e 802.11g), têm se λ com o valor de 0,125 m.

3.2.2 Penetração de sinal em ambientes fechados

Conhecer a potência de sinal recebida dentro dos prédios devido a transmissores externos se faz importante, pois não é desejado com que se perca o sinal após a transposição de uma determinada barreira, no caso do transmissor externo pertencendo à própria rede, ou pode não ser desejado no caso de transmissores externos de outras empresas ou com outro tipo de aplicações que podem interferir no bom desempenho da rede interna.

Isso ocorre porque dois sinais não podem ser transmitidos pela mesma portadora (fase e quadratura), senão haverá colisão e a informação não será compreendida, além do que não é desejável que sinais de uma empresa sejam recebidos por uma outra por motivos de segurança de informações. A mensuração de penetração RF entre andares, provenientes de transmissores externos é função da altura do prédio e da freqüência. Nos andares mais baixos dos prédios os objetos urbanos tendem a diminuir a penetração de energia. Nos andares mais altos, uma linha de visada pode existir causando uma incidência mais forte de sinal nas paredes do exterior do prédio.

3.2.3 Comportamento de sinal em ambientes fechados

Em sistemas de comunicação privados, alguns parâmetros de projeto como a distância entre servidores, expectativas dos usuários e a quantidade de potência recebida em determinados possíveis pontos de recepção são diretamente relacionados com o ambiente de propagação. A quantidade de interferência de RF que pode ser esperada de usuários de co-canais também é um parâmetro igualmente importante, que é uma função direta das características de propagação de dentro do ambiente.

O ambiente de propagação é diretamente relacionado com o tipo de construção e com o mobiliário onde se localiza a rede fatores como, divisão por paredes de alvenaria, divisórias, janelas, se nos móveis há composição de superfície metálica, se existem muitas outras redes sem fio,etc. Um conceito importante e que é um fator de diferenciação entre os padrões 802.11 é se o transmissor e o receptor estão em linha de visada ou não. Um receptor e um transmissor em linha de visada e com antenas constituídas por dipolos verticais com uma pequena distância entre si, cerca de um metro, experimentos demonstraram que numa faixa de 1,5GHz a atenuação é praticamente igual a de espaço livre, esse resultado pode ser estendido para freqüências superiores, que é o caso das utilizadas no padrão 802.11.

3.2.4. Multipercursos

O efeito de multipercursos é causado por três fenômenos, a reflexão, a difração e o espalhamento. Estes fenômenos permitem que um sinal atinja um destino por diferentes percursos, além do percurso direto (*LoS – Line of Sight*), quando este existe. A interseção destes raios faz com que o sinal no dado ponto no espaço seja composto pelos diversos sinais, de modo construtivo, isto é, aumentando o nível de potência do sinal, ou de modo destrutivo, diminuindo o nível de potência do sinal.

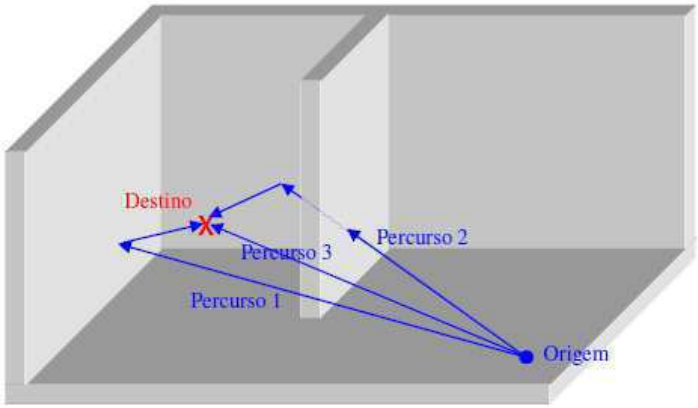


Figura 14 –Ilustração de ocorrência de multipercursos

3.3. Modelos Teóricos e Empíricos

Existem dois tipos de modelos de propagação: os modelos teóricos e os modelos empíricos. Os modelos empíricos são baseados em medidas em diferentes tipos de ambientes, de modo a possibilitar uma caracterização do modelo de propagação que melhor se adeque a um ambiente com as características utilizadas. Os modelos puramente teóricos não possuem nenhum tipo de ajuste experimental, sendo baseados somente em na solução da equação de onda consideradas as condições de contorno do ambiente. Como exemplo de modelo teórico, temos as técnicas de traçado de raios (*Ray tracing*), que simulam reflexões e difrações do sinal em obstáculos, resultando em uma composição em cada ponto do ambiente.

3.4. Modelos Teóricos

A maior parte dos modelos teóricos se baseiam em *ray tracing*, ou modelos de traçado de raios. Modelos precisos utilizam o método das imagens ou técnicas de lançamento de raios. Apresentam tempo de computação elevado e requerem uma descrição muito detalhada do ambiente, não só no que diz respeito à forma dos obstáculos como a suas propriedades eletromagnéticas, sendo de difícil implementação e utilização, principalmente devido ao segundo aspecto. Na prática, são utilizados modelos simplificados considerando um número limitado de reflexões em paredes. A seguir são apresentados dois destes modelos, conhecidos como modelo de 2 raios e modelo de 6 raios.

3.4.1. Modelo de 2 raios

Para se introduzir o conceito de lançamento de raios, assumimos um ambiente *outdoor,* em que não haja obstáculos laterais que possam gerar efeito de multipercursos relevante. Neste caso consideraremos apenas o terreno como possível refletor de raios lançados por uma antena transmissora. Como o sistema estudado neste trabalho tem limitações de potência e não envolve distâncias de transmissão maiores que 1 km, podemos assumir uma superfície plana da terra. O modelo de 2 raios [5,6] baseia-se na ótica geométrica para o cálculo da intensidade do campo no receptor. A figura a seguir ilustra os dois raios lançados pela antena transmissora e a sua recepção na antena receptora, onde são combinados em um único sinal.

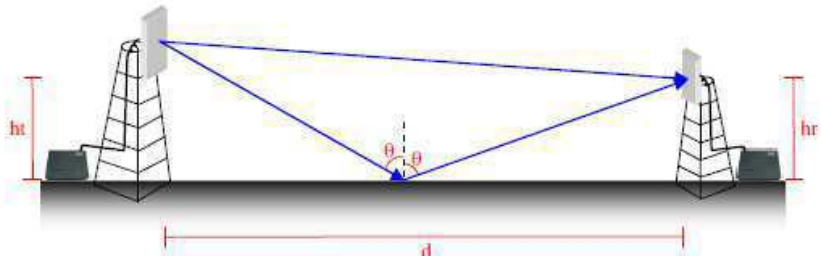


Figura 15 –Ilustração do modelo dos dois raios

A expressão abaixo da potência recebida na propagação em terra plana, usada quando são válidas as aproximações feitas. A expressão de atenuação de propagação (L) correspondente é calculada a seguir.

$$L[dB] = 20.\log.d[m] - 20.\log.ht[m] - 20.\log.hr[m] - Gt[dBi] - Gr[dBi]$$

d - distância em metros [m]
h_t - altura do transmissor
h_r - altura do receptor
G_t – Ganho do transmissor [dBi]
G_r – Ganho do receptor [dBi]

3.4.2. Modelo de 6 raios

Para sinais propagantes em ambientes que apresentam obstáculos laterais a modelagem matemática de 2 raios não é suficiente para descrever a perda de propagação do sinal. Nestes casos, utilizam-se modelos mais completos, como o modelo de 6 raios. Este modelo [5,6] se aplica tanto para ambientes exteriores, como ruas que apresentam edifícios e muros, como para ambientes fechados, onde as paredes do próprio ambiente refletem os raios.

Os 6 raios considerados neste modelo são:

· Raio direto (raio 1)
· Raio refletido no solo (raio 2)
· Dois raios refletidos nos obstáculos laterais (raios 3 e 5)
· Dois raios refletidos nas paredes laterais e no solo (raios 4 e 6)

As figuras a seguir ilustram os raios refletidos:

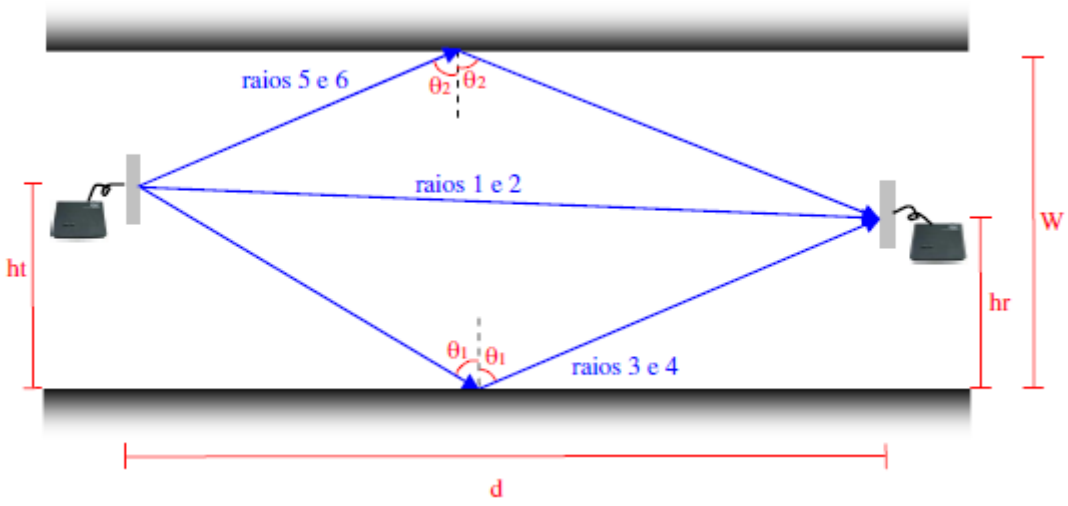


Figura 16 –Ilustração do modelo dos 6 raios(vista superior)

Os raios 4 e 6, que não ficam muito claros observando a visão superior, são melhor representados na figura a seguir.

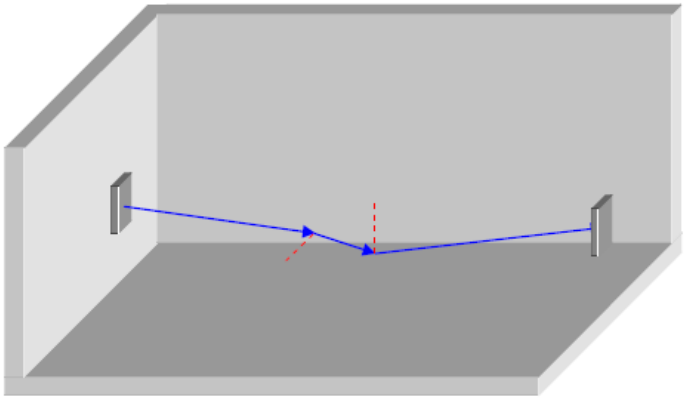


Figura 17 –Ilustração detalhada do modelo dos 6 raios(raios 4 e 6,vista lateral)

Outros modelos mais sofisticados e precisos como o modelo de 10 raios, desenvolvido por Amitay [14] podem ser utilizados para incluir a reflexão no teto do ambiente, mas não serão apresentados neste trabalho, pois nosso foco maior se concentra nos modelos semi-empíricos.

3.5. Modelos Semi-empíricos

3.5.1. Modelos Log-distance [7]

Os modelos empíricos mais simples para a perda de propagação em ambientes fechados ou micro-células em ambientes abertos podem ser representados na forma geral:

$$L_{total} = L_o + 10.n.log(d) + X_\sigma$$

onde valores típicos de n e de X_σ são encontrados na literatura técnica [5], para diferentes ambientes e faixas de freqüência.

3.5.2. ITU-R P.1238-1 [8,9]

O modelo descrito a seguir foi desenvolvido pelo ITU-R (setor que estuda as questões técnicas relativas a comunicações de rádio e gerência de freqüência de rádio internacionais (de espectro de RF) e por satellite), para predição de sinais na faixa de freqüências entre 900 MHZ e 100 GHz em ambientes fechados. Este modelo considera os seguintes efeitos de propagação:

· Reflexão e difração em objetos fixos;
· Transmissão através de paredes, pisos e outros obstáculos fixos;
· Confinamento da energia em corredores;
· Pessoas e objetos em movimento no ambiente.

$$L_{total} = 20 \,.\, log(f) + n \,.\, log(d) + L_f(\, K_f) - 28, \text{ onde:}$$

f – freqüência de operação [MHz]
n – coeficiente de atenuação com a distância
d – distância percorrida [m]
k_f – número de pisos (andares) atravessados
L_f – coeficiente de atenuação por piso atravessado [dB]

3.5.3. Modelo COST 231 Keenan e Motley [7,10,11]

Este modelo é o modelo mais completo para predição de sinais em ambientes fechados e exteriores com existência de obstáculos. Sua expressão matemática é muito abrangente, mas requer o conhecimento de um grande volume de dados, para definir o valor dos seus parâmetros de entrada.

$$L_{total} = L_o + 10 \,.\, n \,.\, log(d) + \sum_{i=1}^{I} k_{f,i} \,.\, L_{f,i} + \sum_{j=1}^{J} k_{w,i} \,.\, L_{w,i} \text{ , onde:}$$

L_0 – perda de propagação a um metro da antena irradiante [dB]
d – distância percorrida pelo sinal [m]
n – coeficiente de propagação
$L_{f,i}$ – perda de propagação do sinal através do piso i [dB]
$k_{f,i}$ – número de pisos com a mesma característica
$L_{w,i}$ – perda de propagação do sinal através da parede j [dB]
$k_{w,i}$ – número de paredes com a mesma característica
I – número de pisos atravessados pelo sinal
J – número de paredes atravessadas pelo sinal

3.5.4. Modelo COST 231 Multi-Wall [7,12,13]

O modelo Multi-Wall baseia-se no modelo de propagação COST 231 Keenan e Motley, mas considera um comportamento não linear da atenuação por múltiplos pisos.

$$L_{total} = L_o + 10 \,.\, n \,.\, log(d) + L_f \left[\frac{Lf + 2}{Lf + 1} - b \right] . \, k_f + \sum_{j=1}^{J} k_{w,i} \,.\, L_{w,i} \text{ , onde:}$$

L_0 – perda de propagação a um metro da antena irradiante [dB]
d – distância percorrida pelo sinal [m]
n – coeficiente de propagação
Lf – perda de propagação do sinal através dos pisos [dB]
kf – número de pisos com a mesma característica
b – fator de correção da atenuação dos pisos
$L_{w,i}$ – perda de propagação do sinal através da parede j [dB]
$k_{w,i}$ – número de paredes com a mesma característica
J – número de paredes atravessadas pelo sinal

4. Estudo de caso

4.1. O Software Netstumbler

Depois de se decidir sobre o melhor local para instalar o AP , é necessário que seja feita a avaliação do sistema em operação, através da verificação potência do sinal do ambiente.Dessa forma a ter-se-á uma idéia mais exata da recepção no cliente, será conhecida a área de cobertura e serão encontrados seus pontos cegos. Um software muito útil nesse sentido é o **NetStumbler**.

O Netstumbler permite listar todas as redes sem fio disponíveis na área, mostrando o canal, o tipo de criptografia e outros detalhes sobre cada uma além de, mostrar um relatório detalhado sobre a intensidade do sinal, permitindo que seja feita uma auditoria da cobertura da rede bem como a intensidade do sinal em cada ponto.

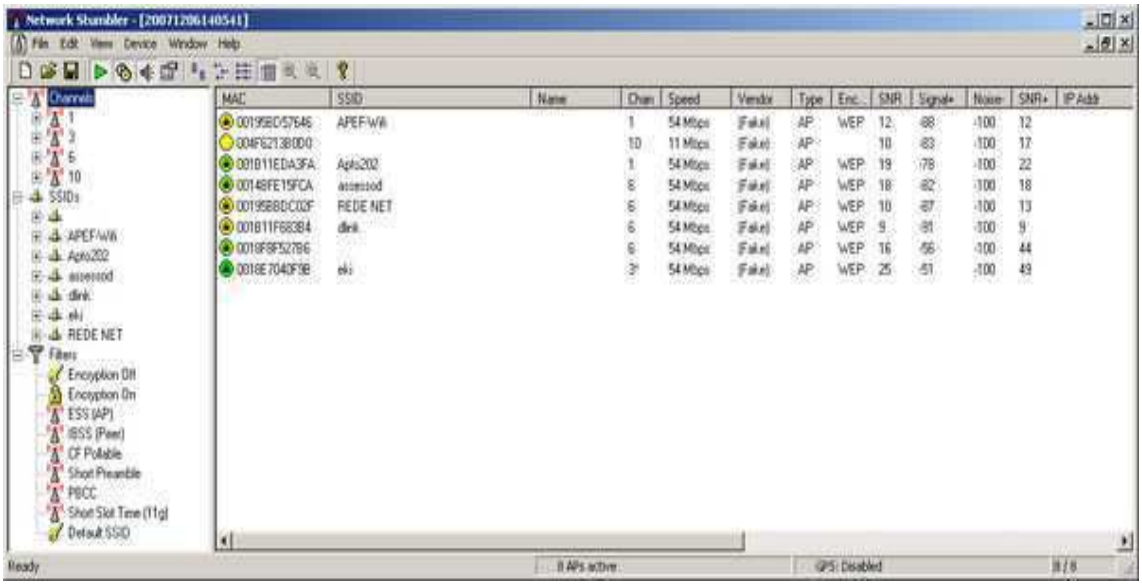


Figura 18 – Interface do NetStumbler.

Como se pode ver na Figura18, o NetStumbler mostra todos os pontos de acesso disponíveis, independentemente do canal usado. A cor do ícone indica a intensidade do sinal (cinza para muito fraco, vermelho para fraco, amarelo para regular, verde para bom) e o cadeado indica que a rede está protegida.

As três colunas mais importantes são as indicadas como, "Signal+", "Noise-" e "SNR+", que mostram, respectivamente, a intensidade do sinal (em dBm), a intensidade do ruído e a taxa de sinal/ruído para cada uma. Apenas parte das placas suportadas são capazes de medir corretamente taxa de ruído. Nas demais, a função fica desativada, com o campo exibindo um "-100" para todas as redes.

O sinal é medido em uma escala negativa, onde cada -3 dB correspondem a uma redução de 50% na intensidade do sinal, de forma que -95 dBm correspondem a apenas um quarto de -89 dBm. A maioria das placas precisa de pelo menos -92 dBm para manter uma conexão na velocidade mínima (1 Mbps) e pelo menos -72 dBm para manter uma conexão a 54 Mbps.

Em ambientes com muito ruído eletromagnético, é importante o monitoramento também da relação sinal/ruído (SNR), que indica o quanto o sinal é mais forte que o ruído. Para manter uma conexão minimamente estável ele deve ser de pelo menos 5 dB (quanto maior melhor). Este relatório das redes disponíveis é muito útil na hora de escolher qual canal usar, já que será possível avaliar quais canais já estão sendo utilizados e em qual extensão.

Outra utilidade para o relatório é detectar a presença de pontos de acesso "ilegais", instalados sem autorização pelos próprios usuários da rede. Embora às vezes a intenção seja boa, eles podem comprometer a segurança da rede, expondo-a a ataques externos.

Continuando, no menu da esquerda podem ser encontradas várias opções de filtros, as quais permitem mostrar apenas APs usando um determinado canal, com ou sem criptografia, etc. Escolhendo-se seu próprio ponto de acesso na lista, ter-se-á acesso à função mais interessante do NetStumbler, que é o gráfico de sinal,Figura 19:

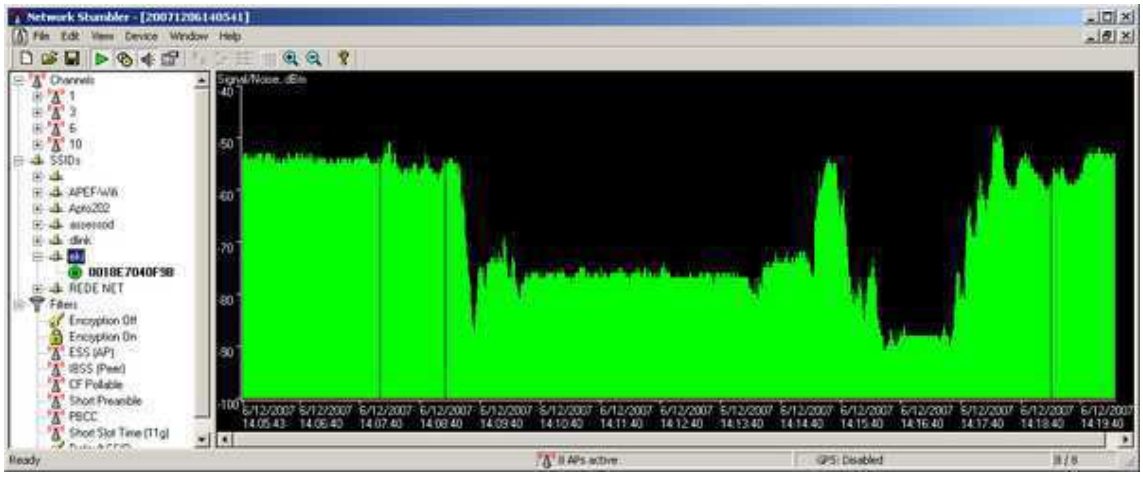


Figura 19– Exemplo de medida da potência do sinal.

Ao se usar um computador, se terá acesso ao gráfico para verificar a variação do sinal dento da área de cobertura da rede, testando diferentes combinações de antena, ou de posicionamento do AP, potência do transmissor, posição dos clientes, uso ou não de defletor e assim por diante. Ele também poderá ser bastante útil na tarefa de alinhamento das antenas quando da criação de um link de longa distância.

Outra observação importante é que mesmo estando fixada a AP,será normal que o sinal sofra pequenas variações (de 3 a 4 dBi). É justamente por isso que é importante se trabalhar sempre com uma margem de segurança ao se escolher a antena e posicionar o AP. Por outro lado, grandes variações podem indicar a presença de alguma fonte de forte interferência, como um forno de microondas ou um telefone sem fio que utilize a faixa de 2.4 GHz.

Outra curiosidade é que o ponto de acesso pode funcionar mesmo sem a antena, já que o próprio conector é suficiente para emitir um sinal fraco. Apesar disso, sem a antena, a potência do sinal cairá em 20 dB ou mais, o que fará com que a rede só funcione de forma confiável dentro do próprio cômodo onde está o AP.

4.2. Ambiente de testes

O ambiente de testes é o bloco CJ da Universidade Federal de Campina Grande e suas dependências, onde deu-se da maior ênfase a uma área de *região de sombra*, na qual o acesso a rede é muito precário. Abaixo segue a Figura 20 que demonstra as disposições das salas, dependências do bloco.Utiliza o sistema operacional Windows, com a ferramenta Netstumbler na versão 0.4 em um *notebook*. Foi instalada uma placa para redes sem fios modelo PCI/PCMCIA. A Figura 20 mostra as disposições dos AP´s onde estão instalados e as devidas dependências onde foram realizadas as medições.

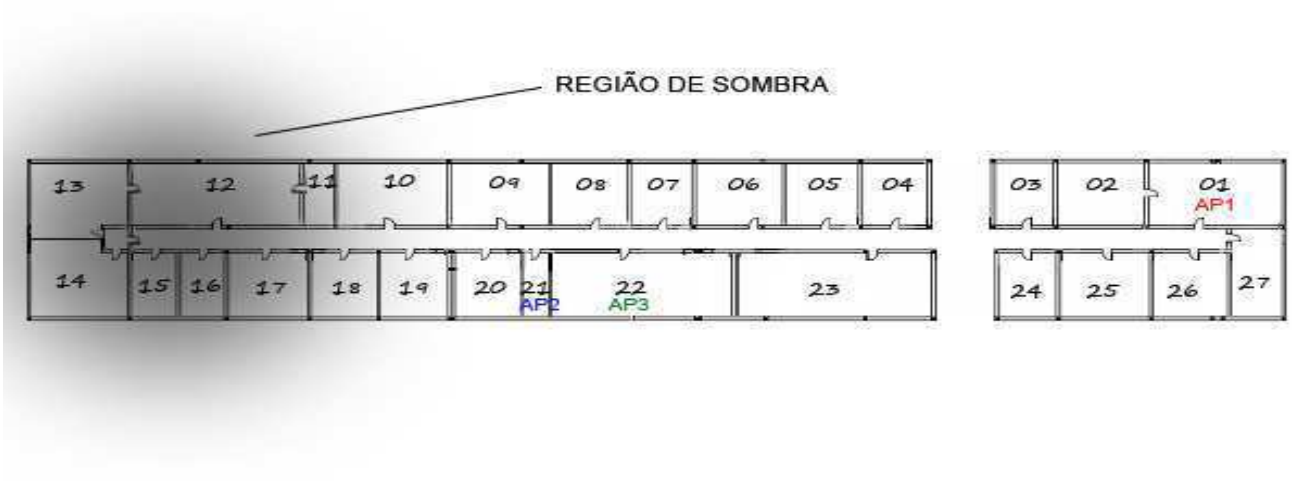


Figura 20– Planta baixa do bloco CJ da Universidade federal de Campina Grande.

Sala 01 - LAPS (Laboratório de Processamento de Sinais)
Sala 21 – Sala do mestrado
Sala 22 – Sala do professor Benedito Aguiar
AP1 - *Access Point* 1
AP2 - *Access Point* 2
AP3 - *Access Point* 3

4.3.Testes realizados

Inicialmente, foram designados alguns pontos estratégicos (pontos vermelhos) para se avaliar a melhor localização do AP2 para que a cobertura *wireless* em todo o bloco seja satisfatória. Para cada ponto estabelecido, foram feitas todas as análises em tempo real até a sala 14 (Laboratório de Comunicações), onde todo o percurso foi realizado com um *notebook* em mãos, em velocidade constante.

Todas as medições foram feitas com um software , chamado Netstumbler. A Figura 21 mostra os pontos onde foram feitas todas as medidas.

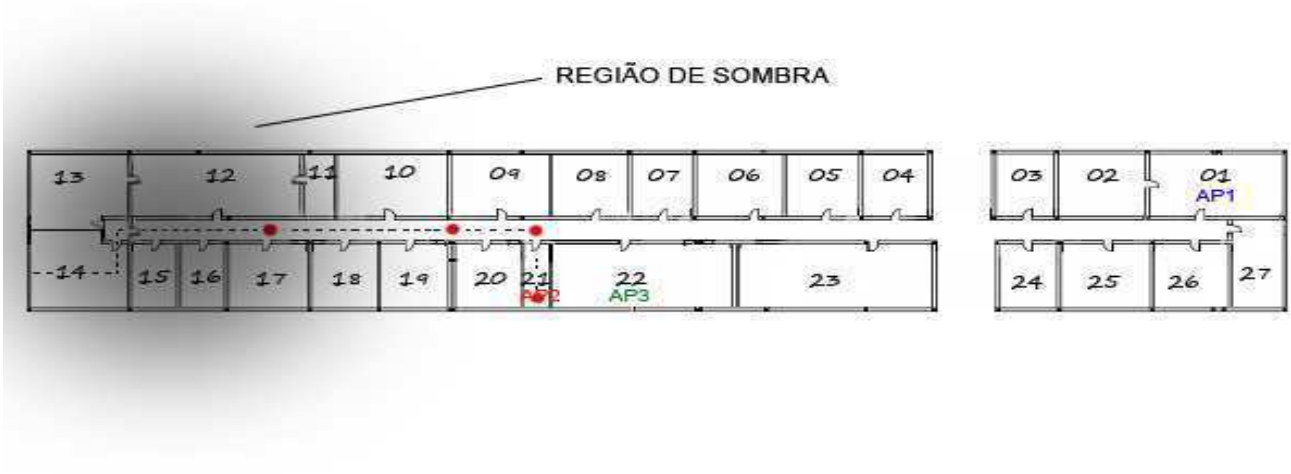


Figura 21 – Pontos estratégicos pra melhor localização do AP.

Sala 2- Sala de mestrado
Sala 19 - Sala do professor Francisco Marcos
Sala 20 - Sala do professor José Ewerton
Sala 17 - Porta da sala do professor Rômulo do Valle
Sala 14 – Laboratório de Comunicações (LABCOM)
Ponto 1 - Interno a sala 21
Ponto 2 - Porta da sala 21
Ponto 3 - Entre a sala 19 e 20
Ponto 4 - Frente da sala do professor Rômulo do Valle

4.4. Análise dos resultados

Após realizar todas as medidas, verifica-se, quando se desloca o AP2 em direção a sala 14 existe uma variação mais significativa, sendo que o sinal passa a ter períodos de maior atenuação (ganho). Nas Figuras 22 e 23, mostra-se as distribuições de potência referente ao AP1, quando está localizado nos pontos 1 e 4:

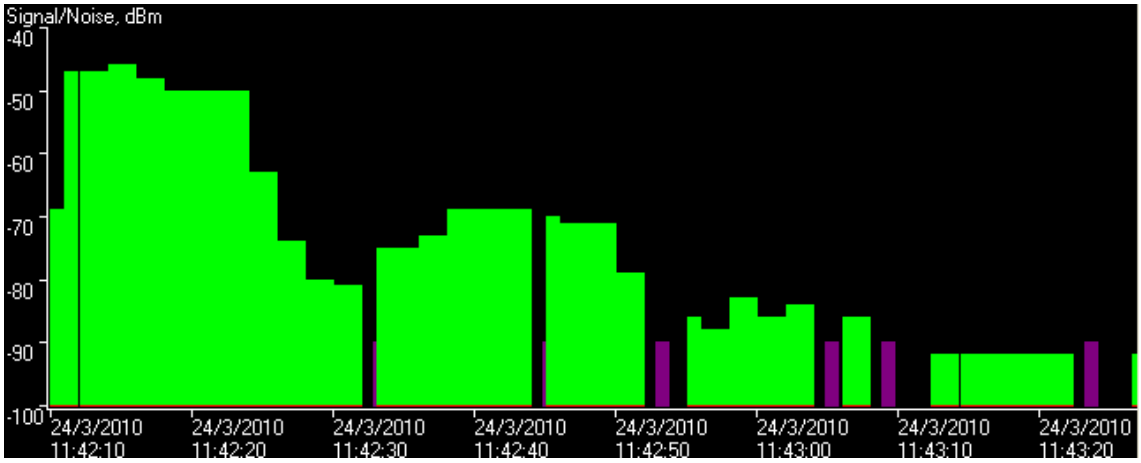


Figura 22 – Espectro referente a distribuição de potência no ponto 1.

Pode-se observar na figura 22 que o sinal se comporta de maneira uniforme, ou seja, entre 11:42:10 e 11:42:25, tendo o sinal sempre entre – 46 dBm (com poucas amostras extrapolando este intervalo). A partir de 11:42:25 o gráfico apresenta variações até as 11:43:10 horas, ou seja, é neste período que há uma degradação do sinal. Depois das 11:43:10 passa-se a ter períodos de menor atenuação em torno de – 89 dBm e o sinal volta a se comporta de maneira constante.

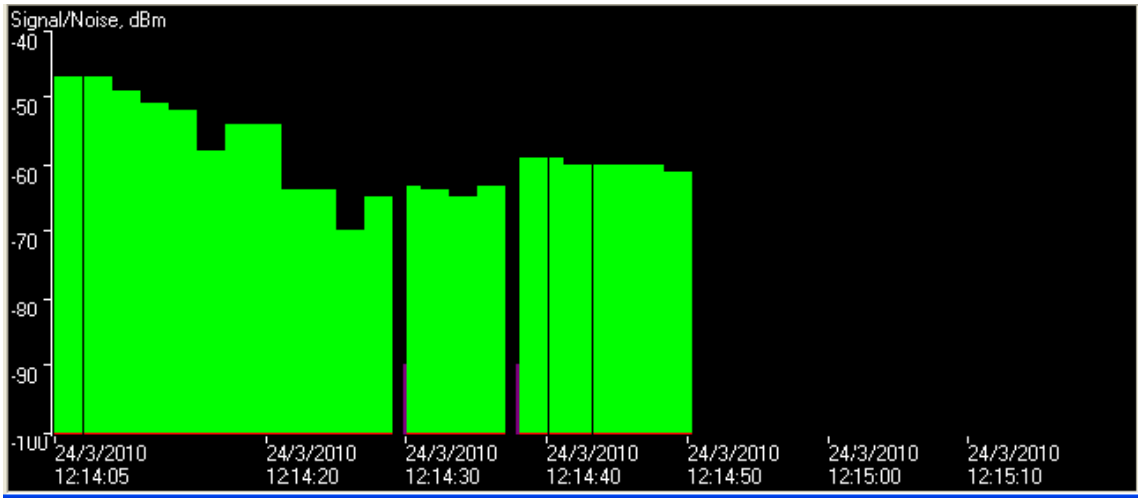


Figura 23 – Espectro referente a distribuição de potência no ponto 4.

Na figura 23, entre 12:14:05 e 12:14:30, o gráfico apresenta variações apresentando degradação do sinal. Deve-se notar que a partir de 12:14:30 há uma notável variação no ganho do sinal, passando a ter períodos de maior atenuação em torno de – 55 dBm. Fazendo um comparativo entre os pontos 1 e 4, verifica-se que o nível de potência na sala 14 em relação ao ponto 2 teve um ganho aproximadamente de – 34 dBm.

Em relação as análises referentes aos pontos 2 e 3, os gráficos referentes estão em ANEXOS no final deste relatório.

CONSIDERAÇÕES FINAIS

Este trabalho motivou-se em uma tecnologia que está em crescente utilização, às redes sem fio. Com a utilização dessa tecnologia, a segurança torna-se primordial e as formas de controle de acesso à essas redes tende a serem primordiais. Em conjunto com as ferramentas de segurança ,como WEP, WPA e WPA2, o sistema de localização que utiliza os mecanismos de detecção de obstáculos dinâmicos é mais uma forma de preservar a integridade da rede.

A respeito ao planejamento de cobertura é essencial dispor de um modelo adequado para os cálculos de perda de propagação. Em ambientes fechados a utilização de modelos determinísticos, como o traçado de raios, é limitada pela necessidade de uma descrição muito detalhada dos obstáculos existentes no ambiente. Modelos semi-empíricos apresentam menor complexidade e menor tempo de processamento, mas exigem o conhecimento de uma série de parâmetros que apresentam variabilidade significativa dependendo da geometria do ambiente e do tipo e material de construção.

Este trabalho teve como objetivo estudar a instalação e o desempenho do servidor internet sem fio DI-524 localizado nas dependências do bloco CJ do Departamento de Engenharia Elétrica da UFCG. A análise eletromagnética,feito com o software NETSTUMBLER, buscou avaliar a melhor localização do AP ,de modo se tenha uma cobertura bastante satisfatória De acordo com as análises dos resultados,conclui-se que a localização do AP deve está próxima a sala 17,onde se pode verificar que o sinal na sala 14 passou a ter períodos de maior atenuação.

Com trabalhos futuros, indica-se uma maior análise no sistema, de forma a efetivamente propor modificações na implantação do sistema ou ajustes de forma a otimizar seu desempenho e sua adequação às normas.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] **Vagner Sacramento**, "WLAN-802.11.pdf", Departamento de Informática – PUC-Rio. (www-di.inf.puc-rio.br/~endler/courses/Mobile/transp/WLAN-80211.pdf)

[2] **Eduardo Prado**, Apresentação do Seminário WLAN - Wireless Local Area Network, 21 de maio de 2003 - RIOSOFT.

[3] **Jim Zyren e Al Petrick**, "IEEE 802.11 Tutorial", 1999

[4] Acces Point Cisco 350 Series Datasheet. (www.cisco.com)

[5] **Theodore S. Rappaport**, "Wireless Communications-Principles & Practice", Pretince Hall Inc, 1996

[6] **Marcio Eduardo da Costa Rodrigues**, "Técnicas de Traçado de Raios em Três Dimensões para Cálculo de Campos em Ambientes Interiores e Exteriores", Dissertação de Mestrado – Pontifícia Universidade Católica de Rio de Janeiro, 2000

[7] **R. F. Rudd**, "Indoor Coverage Considerations for High-elevation Angle Systems", Aegis Systems Limited, 2002

[8] Recommendation ITU-R P.1238-1, "Propagation data and prediction models for the planning of indoor radiocommunication systems and radio local area networks in the range 900 MHz to 100 GHz", 1997 – 1999 – 2001

[9] **Steve Shellhammer**, "Overview of ITU-R P.1238-1 Propagation Data and Prediction Methods for Planning of Indoor Radiocommunication Systems and Radio LAN in the Frequency Band 900 MHz to 100 GHz", Symbol Technologies, 2000

[10] **Michael Döhler**, "An Outdoor-Indoor Interface Model for Radio Wave Propagation for 2.4, 5.2 and 60 GHz", Msc Thesis – King's College London, 1999

[11] **Keenan J.M. and Motley A.J.**, "Radio Coverage in Buildings", British Telecom Technology Journal, 1990

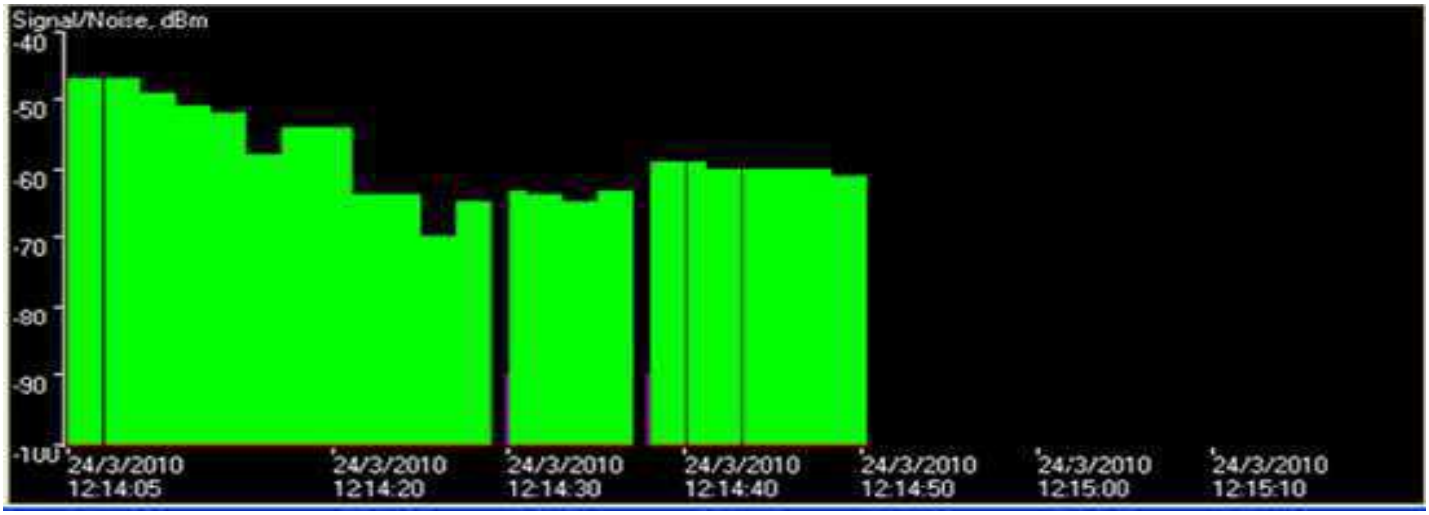
[12] COST 231, "Digital Mobile Radio Towards Future Generation Systems", Final Report – European Commission, 1999

[13] **Daniela Laselva**, "WLAN Indoor Radio Network Planning", HUT Communications Laboratory, 2003

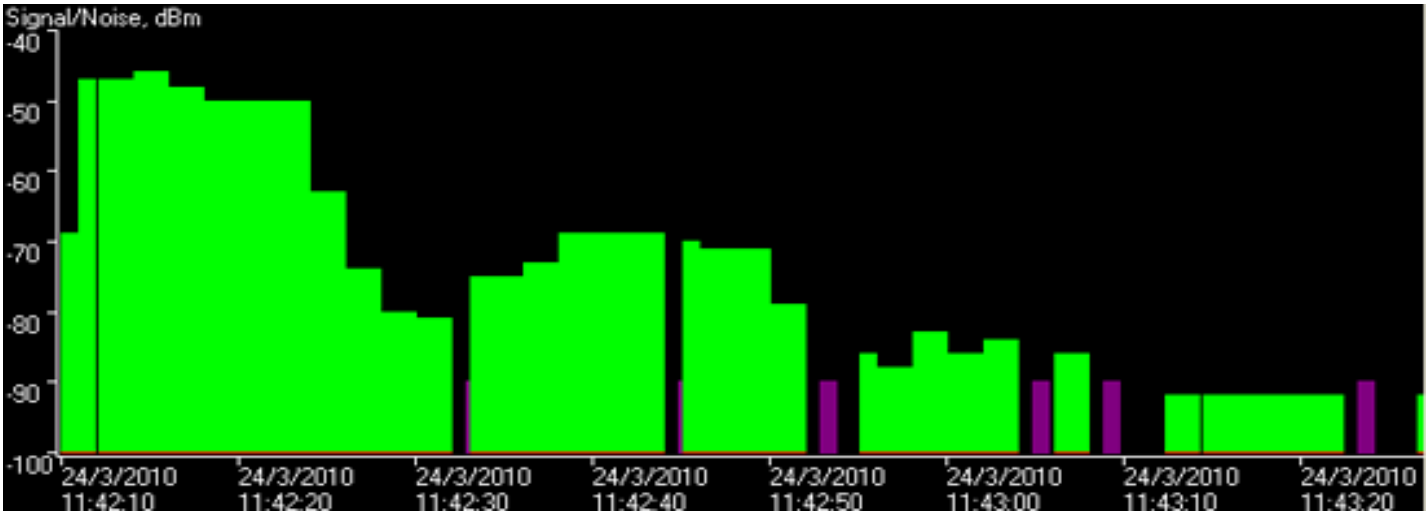
[14] **N. Amitay**, "Modeling and computer simulation of wave propagation in lineal line-of sight microcell," IEEE Trans. Vehic. Technol., Vol VT-41, No. 4, pp 337-342, Nov. 1992

ANEXOS

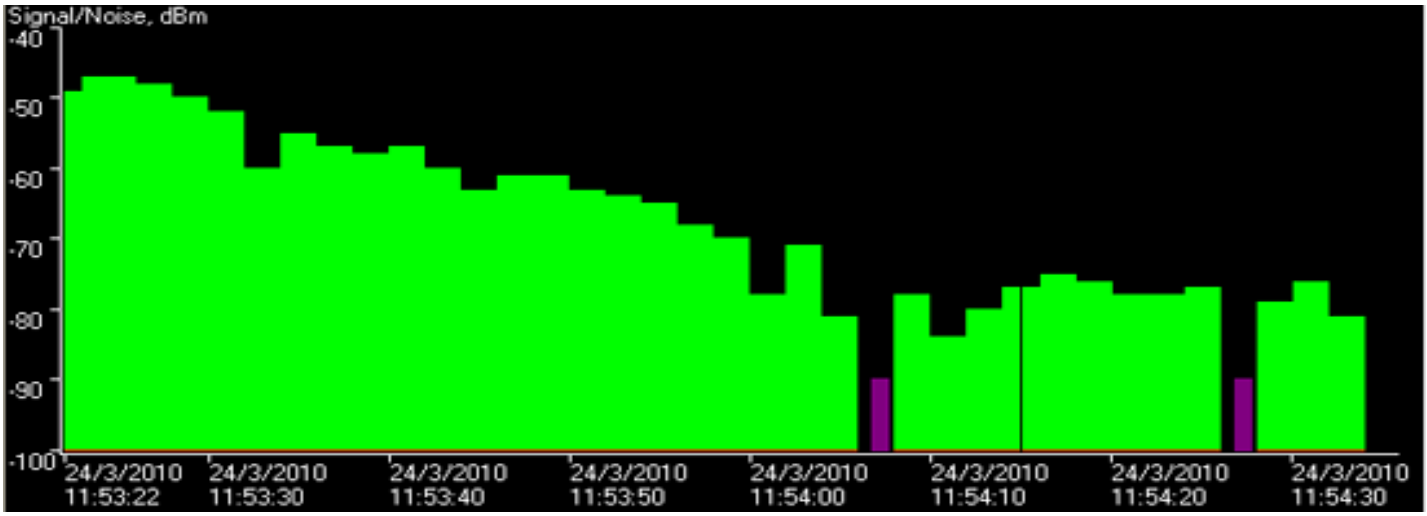

REGIÃO DE SOMBRA
13
12
11
10
09
08
07
06
05
04
03
02
01
AP1
14
15
16
17
18
19
20
21
AP2
22
AP3
23
24
25
26
27



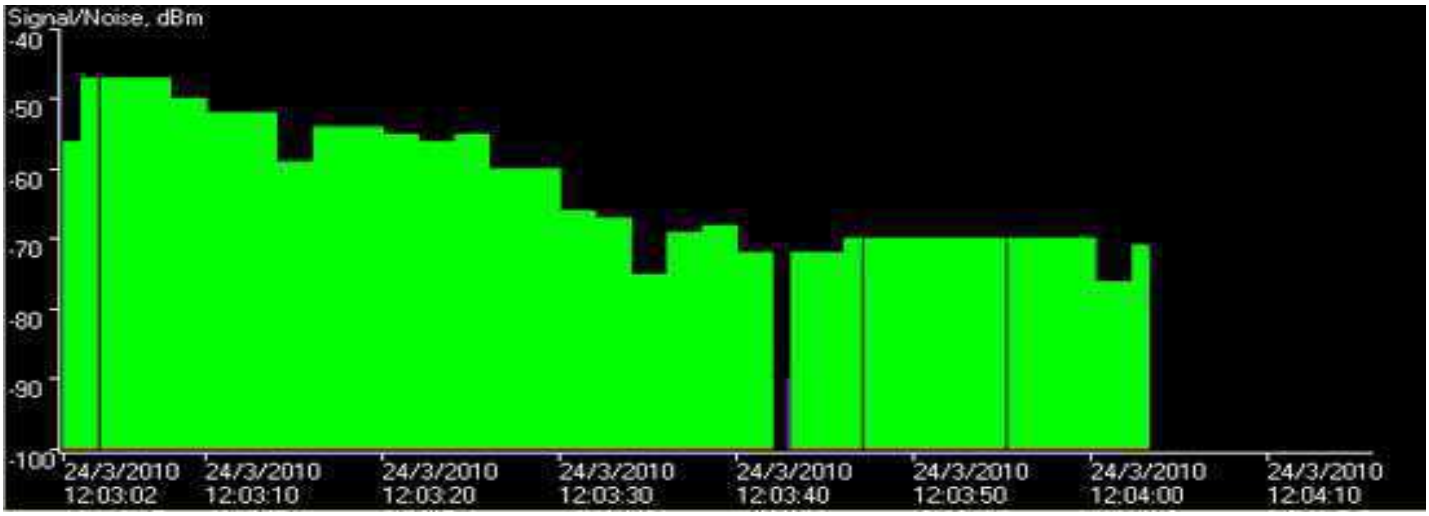
- Espectro referente a distribuição de potência no ponto 4.



- Espectro referente a distribuição de potência no ponto 1.



- Espectro referente a distribuição de potência no ponto 2.



- Espectro referente a distribuição de potência no ponto 3