1. Introdução

Com o aumento da confiabilidade e praticidade de instalação, as tecnologias de comunicações sem fio (*wireless*) começam a tomar espaço das convencionais redes fixas cabeadas. Isto, combinado com a redução de preços dos componentes, vem aumentando a demanda por redes de acesso sem fio e impulsionando os grandes fabricantes de equipamentos a investir neste novo setor das telecomunicações.

As redes locais sem fio são uma interessante alternativa para ambientes em que obras civis para passagem de cabos são difíceis e caras, muitas vezes exigindo interdição do local durante o prazo de instalação. Estes inconvenientes são decisivos na escolha da opção sem fio, principalmente para empresas que não podem interromper seus trabalhos para implantação de infra-estrutura de comunicações. Este problema é facilmente contornado pelo uso redes sem fio, que em geral, permitem instalações rápidas e simples.

São objetivos deste trabalho discutir as razões que tornam esta opção pelas redes locais *wireless,* vantajosa, apresentar suas características, vantagens, desvantagens e as metodologias de projetos de implantação.

Como principal contribuição do trabalho são apresentados resultados de medidas de propagação em diversos ambientes na faixa de 2,4 GHz. Foram encontrados estudos de propagação baseados em medidas, similares aos propostos neste trabalho em [13], entretanto não são apresentados dados para a faixa de 2,4 GHz. Também são desenvolvidos modelos semi-empíricos, ajustados com base nos resultados das medidas, para previsão da cobertura de redes *wireless* em ambientes fechados (*indoor*) e desenvolvida uma ferramenta de *software* para o planejamento de cobertura utilizando estes modelos.

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

O segundo capítulo aborda alguns aspectos importantes para planejamento de sistemas *wireless*, como interferências, polarização, diversidade de antenas, tráfego e topologia de rede, neste caso, especificamente para as *WLANs*. Este capítulo, como todo o resto do trabalho, 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.

O quarto capítulo apresenta a metodologia e plano de medidas utilizado para o ajuste do modelos de propagação apresentados no capítulo 5.

Finalmente, o sexto e sétimo capítulos abordam, respectivamente, as questões práticas de um projeto de uma *WLAN*, desde o seu planejamento de cobertura e dimensionamento de tráfego até sua implantação (aprofundando mais questões anteriormente comentadas, como interferências intra-sistêmicas e inter-sistêmicas, planejamento de freqüências e capacidade) e um estudo de caso onde foram aplicados todos os pontos abordados neste trabalho.

O Apêndice 1 apresenta um manual de utilização do *software* desenvolvido como parte integrante deste trabalho e o Apêndice 2 apresenta o procedimento básico de captura de níveis de sinal em redes *wireless* e características de equipamentos específicos.

1.1. Histórico

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

Em 1971 surgiu a primeira rede local sem fio (*Wireless LAN ou WLAN*) [1], resultado de um projeto de pesquisa da Universidade do Havaí, chamado ALOHANET, em função do protocolo de acesso utilizado, imaginativamente denominado *ALOHA*. A rede utilizava comunicações via satélite e uma topologia em estrela, tendo 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*) na faixa de 900 MHz, 2,4 GHz e 5 GHz, faixas de espectro 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, o 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. Podemos citar 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

Os alicerces da tecnologia *WLAN* são baseados em portabilidade e praticidade. Estes dois atributos implicam em baixos custos de instalação e operação, pelo fato de permitirem 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 *Wired LANs*, os estudos do IEEE continuaram, resultando em novos avanços na tecnologia 802.11. A tabela a seguir [2] ilustra a evolução desta tecnologia:

Padrão	Data de regulamen.	Banda disponível	Freqüência/ técnica	Taxa de transmissão por canal	Modulação
802.11	Julho de 1997	83,5 MHz	2,4 a 2,4835 GHz DSSS, FHSS	2,1 Mbps	DQPSK (2 Mbps DSSS) DBPSK (1 Mbps DSSS) 4GFSK (2Mbps FHSS) 2GFSK (1Mbps FHSS)
802.11a	Setembro de 1999	300,0 MHz	5,15 a 5,35 GHz OFDM 5,725 a 5,825 GHz OFDM	54, 48, 36, 24, 18, 12, 9, 6 Mbps	BPSK (6, 9 Mbps) QPSK (12, 18 Mbps) 16-QAM (24, 36 Mbps) 64-QAM (48, 54 Mbps)
802.11b	Setembro de 1999	83,5 MHz	2,4 a 2,4835 GHz DSSS	11, 5,5, 2, 1 Mbps	DQPSK/CCK (11, 5,5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)
802.11g	Metade de 2003	83,5 MHz	2,4 a 2,4835 GHz DSSS, OFDM	54, 36, 33, 24, 22, 12, 11, 9, 6, 5,5, 2, 1 Mbps	OFDM/CCK (6, 9, 12, 18, 24, 36, 48, 54 Mbps) OFDM (6, 9, 12, 18, 24, 36, 48, 54 Mbps) DQPSK/CCK (22, 33, 11, 5,5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)

Tabela 1 – Resumo dos padrões IEEE 802.11

Atualmente, 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 *Wireless* atuais ainda são, em geral, um pouco inferiores às redes cabeadas, mas com a rápida popularização dos equipamentos 802.11g, as taxas de transmissão destas redes serão comparáveis às taxas experimentadas nas redes cabeadas tradicionais. 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 *Wireless LANs* sobre as *Wired LANs*

As *WLANs* se tornaram mais populares nos últimos anos em razão da redução dos custos de equipamentos *wireless* no mercado de telecomunicações. Atualmente, 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 a redução de preços dos componentes *wireless*, mas também a 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 w*ireless* sobre redes cabeadas são [3]:

- Portabilidade
- Instalação rápida e fácil
- Instalação de redes temporárias
- Instalação em locais de difícil passagem de cabos
- Baixos custos de instalação

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. Esta questão é discutida no final deste capítulo.

1.4. Componentes de *WLANs*

As *WLANs* são usadas 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 *Wireless LANs e as Wired LANs*, poderíamos dizer que um *AP* tem o mesmo papel em uma *WLAN* que um *Hub* tem em uma rede cabeada.

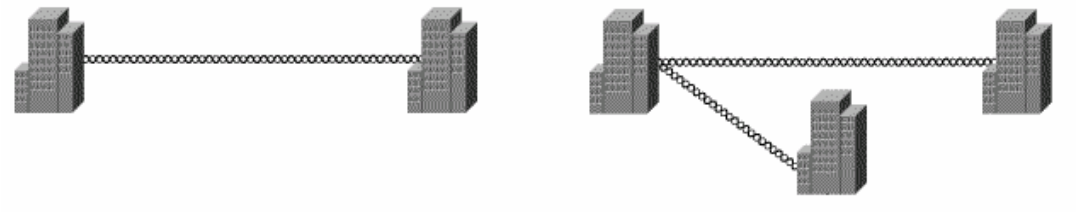
Figura 1 – Exemplo de *Access Point* e antenas externas

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, normalmente isotrópicas, que cobrem 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* [6], 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 mais comuns são: regulagem de potência de transmissão, diversidade de antenas, saídas cabeadas diversas, criptografia (de 40 e 128 bits definidas pelo padrão), entre outras.

1.4.2. Wireless Bridge

Uma *Wireless Bridge* tem a função de estabelecer comunicação entre duas ou mais redes. Esta é uma necessidade comum atualmente, quando se deseja interligar dois edifícios em uma mesma rede (para que possa haver compartilhamento de arquivos, impressoras, 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 ponto-multiponto

Como funcionalidades extras, 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* (ora transmite, ora recebe).

Estas interligações podem muitas vezes ser temporárias para 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 *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*.

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

Figura 4 – Exemplo de *Workgoup Bridge*

1.4.4. Client adapter

O *Wireless Client adapter*, também chamado de *WLAN adapter* ou adaptador de acesso à rede sem fio, é o equipamento chave 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*, 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 e PCI)

1.5. Segurança em redes *wireless*

Em uma rede cabeada, para um indivíduo "entrar" na rede é necessário que o mesmo se conecte a um ponto físico na rede, enquanto em redes sem fio basta estar dentro de sua área de cobertura. Como é muito difícil limitar a área de cobertura a uma área específica, sem que ocorra "vazamento" de sinal, é necessária a implementação de técnicas adicionais de segurança de rede.

O padrão IEEE 802.11 inclui dois métodos de segurança [2]: autenticação e encriptação.

O uso de autenticação significa que cada estação que se deseja conectar a rede deve ter sua autorização avaliada. Esta avaliação se dá entre o *AP* e cada estação. A autenticação pode ser de chave compartilhada (*Shared Key*) ou de sistema Aberto (*Open System*).

No caso de utilização de sistema aberto, uma estação pode obter autenticação conhecendo apenas o nome identificador da rede (*SSID*) e solicitando a autenticação. Num sistema totalmente aberto, os *APs* transmitem seus *SSIDs* em intervalos regulares, permitindo assim a autenticação de qualquer usuário sem qualquer preocupação com a segurança da rede. Uma primeira medida de segurança pode ser implementada inibindo a transmissão aberta dos *SSIDs* o que obriga os usuários a conhecer, pelo menos, o nome da rede. Os *APs* que recebem a solicitação podem autenticar qualquer estação ou apenas um grupo pré-definido de estações, identificadas pelo seu endereço *MAC*. Esta técnica é chamada de *MAC Adress Filtering* e corresponde a uma medida adicional de segurança.

No caso do uso de chave compartilhada, apenas as estações que possuem uma chave secreta podem se autenticar na rede. A chave compartilhada pode ser utilizada em combinação ou não com *MAC Address Filtering.*

Mesmo que esta estratégia seja implementada, não é possível evitar que um *hacker* altere o endereço *MAC* de fábrica por um localmente administrado, escolhendo-o aleatoriamente até que um *MAC* válido seja encontrado. Outra possibilidade é a utilização de um "sniffer" de rede para identificar o tráfego de usuários ativos e seus respectivos *MACs*. Utilizando-se deste endereço, o *hacker* pode participar da rede como se fosse um usuário válido. Conclusão: a estratégia de utilizar o *MAC* como método de autenticação não é aconselhável.

A encriptação tem como objetivo elevar o nível de segurança de uma *WLAN* para que este seja comparável ao de uma rede cabeada. A técnica utilizada no padrão

802.11b, conhecida como *WEP* (*Wired Equivalent Privacy*), utiliza um algoritmo de encriptação chamado de RC4. Este algoritmo foi desenvolvido para prover as seguintes características [4]:

- Ser razoavelmente "forte"
- Auto-sincronia
- Eficiência computacional
- Exportável
- Opcional

A técnica de segurança *WEP* também não fornece um nível de segurança ideal contra invasões à rede por *hackers*. Para tal, o IEEE continua estudando novas medidas de segurança para as redes *wireless*. De fato, existem alguns mecanismos básicos de segurança incluídos na especificação e que podem ser empregados de modo a tornar a rede mais segura, mas mesmo com a adoção desses mecanismos, o potencial risco de invasão continua a ser elevado.

Com o objetivo de melhorar os mecanismos de segurança, o IEEE criou um novo comitê, denominado 802.1X, cuja especificação foi ratificada em abril de 2002. Inicialmente, a intenção era padronizar a segurança em portas de redes *wired*, mas ela se tornou aplicável também às redes *wireless* [5]. No padrão 802.1X, quando um dispositivo solicita acesso a um *AP*, este requisita um conjunto de credenciais. O usuário então fornece esta informação, segundo uma política repassada pelo *AP* para um servidor *RADIUS*, que efetivamente o autenticará e o autorizará. O método utilizado para informar as credenciais chama-se *EAP* (*Extensible Authentication Protocol*), uma base a partir da qual os fabricantes podem desenvolver seus próprios métodos para a troca de credenciais. Existem atualmente cinco tipos diferentes de autenticação: *EAP-MD5*, *EAP-TLS*, *EAP-CISCO* (ou *LEAP*), *EAP-TTLS* e *EAP-PEAP*.

Motivado pelas deficiências de segurança e gerenciamento apresentados pelo WEP desde que foi padronizado pelo comitê 802.11b, o IEEE criou ainda um novo grupo de trabalho identificado pela sigla 802.11i, preocupado principalmente em definir boas práticas de segurança. Apesar de o trabalho ainda estar em andamento, muito já foi feito e alguns novos mecanismos já começam a ser fornecidos pelos fabricantes para as redes *wireless* legadas, como o *PKIP*, *MIC* e "*Broadcast Key Rotation*".

O padrão 802.11i aborda a utilização de um novo mecanismo de cifragem para as novas redes *wireless* 802.11 “a” e “g” de alto desempenho, chamado *AES-OCB* (*Advanced Encryption Standard – Operation Cipher Block*). Esta nova técnica de cifragem foi recentemente adotada pelo governo norte-americano em substituição ao *3DES*. O objetivo é que o *AES-OCB* seja muito mais forte do que a combinação *WEP/PKIP*.