



**MECANISMO DE IDENTIFICAÇÃO
DINÂMICA DA ATENUAÇÃO DE
OBSTÁCULOS PARA LOCALIZAÇÃO DE
ESTAÇÕES EM REDES SEM FIOS IEEE
802.11
TRABALHO DE CONCLUSÃO DE CURSO I**

MILTON ROBERTO MORAES

André Peres
Orientador

Guaíba, Novembro de 2007.

DADOS DE IDENTIFICAÇÃO

Acadêmico: Milton Roberto Moraes

E-mail: milton.moraes@claro.com.br

Professor Orientador: André Peres

E-mail: decoperes@gmail.com

Título do Projeto: Mecanismo de Identificação Dinâmica da Atenuação de Obstáculos para Localização de Estações em Redes Sem Fios IEEE 802.11

Período de realização: Agosto 2007

SUMÁRIO

1 INTRODUÇÃO	5
2 REDES SEM FIO	6
2.1 PADRÕES WIRELESS	7
2.1.1 ENLACES	9
2.1.2 MECANISMOS DE SEGURANÇA	11
2.1.2.1 WEP.....	11
2.1.2.2 Funcionamento do Protocolo WEP.....	12
2.1.2.3 WPA.....	13
2.2 Meios de Transmissão.....	14
2.2.1. <i>Spread Spectrum</i>	14
2.2.2. FHSS.....	15
2.2.3. DSSS.....	15
2.2.4. OFDM.....	15
3 NÍVEL FÍSICO	16
3.1 Microondas	16
3.2 Antenas.....	16
3.2.1 Antenas Direcionais.....	16
3.2.2 Antenas Omnidirecionais.....	17
3.2.3 Antenas Setoriais.....	17
4 LOCALIZAÇÃO DAS ESTAÇÕES SEM FIO	17
4.1 Amplitude de Chegada.....	17
4.1.1 Triangulação	17
4.1.2 <i>Fingerprinting</i>	19
4.2 Tempo de Chegada.....	20
5 PROPAGAÇÃO	21

5.1 Mecanismos de propagação.....	21
5.1.2 Propagação e Atenuação.....	22
5.1.3 Penetração de Sinal em Ambientes Fechados	23
5.1.4 Comportamento de sinal em ambientes fechados.....	24
6 MODELO PROPOSTO	25
7 CENÁRIO	26
8 CONCLUSÃO	26
9 BIBLIOGRAFIA	27

1 INTRODUÇÃO

Atualmente a estrutura de redes sem fios tem-se popularizado, com o principal objetivo de comunicação entre computadores com mobilidade e flexibilidade. A mobilidade garante a movimentação livre na área de abrangência da rede. A flexibilidade gera uma independência de estrutura física, para distribuição de estações, bem como a facilidade de adicionar ou retirar nós da mesma.

Porém estas facilidades têm características que podem ser prejudiciais no ponto de gerência e segurança de rede, uma vez que os limites de abrangência da rede não são delimitados de forma precisa.

Uma das características importantes em relação à segurança é a inexistência no padrão IEEE 802.11 de mecanismos capazes de identificar a localização física de uma determinada estação sem fios na rede.

Este fato, vindo a dificuldade de se definir precisamente a área de abrangência da rede (devido ao comportamento dos sinais de microondas) torna a identificação de uma estação maliciosa uma tarefa complexa ao administrador da rede.

Existem diversas propostas de mecanismos para localização de estações tais como [Bardwell, 2003; Capkun, 2005; Sayed 2005; Taheri, 2004].

Dentre estas propostas, destaca-se o trabalho desenvolvido por [Suris 2007], o qual realiza a localização das estações sem fio através do mapeamento de potências. Este trabalho, no entanto, não considera o impacto da existência de obstáculos dinâmicos.

Este trabalho apresenta uma proposta para o desenvolvimento de uma solução para localização de usuários de rede sem fio IEEE 802.11 (*wireless*) adicionando à solução existente na Ulbra de Guaíba, desenvolvida por [Suris, 2007] mecanismos para obtenção de atenuação causada por obstáculos dinâmicos.

2 Redes Sem Fios

Computadores podem comunicar-se entre si com ou sem o uso de cabos. A utilização de cabos chama-se comunicação é “cabeada” ou *wired*. Já com a não utilização de cabos, diz-se que a comunicação é “sem fio” ou *wireless*. (MAT, 2005)

Uma rede local sem fio, WLAN (*Wireless Lan*), é implementada como extensão ou alternativa para redes convencionais. Além de redes locais, a tecnologia pode ser utilizada para redes de acesso à Internet, que nestes casos são denominadas redes Wi-Fi (*Wireless Fidelity*). No intuito padronizar os equipamentos dói constituído a Wi-Fi Alliance que consiste em uma organização formada pelos principais fabricantes de equipamentos que utilizam a tecnologia 802.11 e se reúnem para organizar um “*bake-off* de interoperabilidade”, onde os fabricantes de hardware trocam informações de seus componentes e se os mesmos se comunicam corretamente com os equipamentos de outros fornecedores (interoperabilidade). Os equipamentos que possuírem a certificação da **Wi-Fi** estão aptos a garantir padrões relevantes, e foram aprovados nesses testes de interoperabilidades. (ROS, 2003).

São utilizados sinais de Radio Frequência (RF) para a transmissão de dados na WLAN, diminuindo assim a necessidade de cabos de conexão dos usuários à rede. Desta forma, uma WLAN integra a comunicação de dados com:

- 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 *wireless* 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 *wireless*;
- e) Praticidade** devido a redução na utilização de cabos, a rede wireless reduz 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 *wireless* 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. (SAN, 2005)

O transporte de dados através de uma rede *wireless* envolve três elementos distintos: os sinais de rádio, o formato dos dados e a estrutura de rede. Em uma rede *wireless*, os adaptadores de rede em cada computador convertem os dados digitais para sinais de rádio, os quais são transmitidos para outros dispositivos na rede, e convertem os sinais de rádios que chegam dos outros elementos da rede de volta para os dados digitais. O IEEE (*Institute of Electrical and Electronics Engineers*) produziu um conjunto de padrões e especificações para redes *wireless*, sob o título “**IEEE 802.11**”, o qual define o formato e a estrutura desses sinais. (ROS, 2003).

Padrões Wireless

Foram criados grupos de estudo pela IEEE para desenvolvimento de padrões, visando de orientar a indústria de equipamentos de aplicações sem fio, a fim de buscar interoperabilidade entre eles. Foram criadas as seguintes especificações:

Wireless Personal Area Network (WPAN)

Utiliza a tecnologia *Bluetooth* (802.15), com o benefício de requerer baixa potência para permitir conectividade dentro de uma pequena área.

Wireless LANs (WLAN)

Utilizada dentro de edificações para prover conectividade entre usuários móveis. Podendo também ser usado para conexão de médias distâncias (da ordem de alguns quilômetros).

IEE 802.11

A norma IEEE 802.11 criada em 18/11/1997, padroniza junto aos fabricantes parâmetros para que possam desenvolver placas de redes e *access points* compatíveis. Essa norma define as taxas de transferência a 1Mbps e 2 Mbps. São determinados dois métodos de transmissão de sinal pela camada física, operando a 2,4 Ghz, a saber:

- *Frequency Hopping Spread Spectrum* FHSS, que utiliza a modulação GFSK;
- *Direct Sequence Spread Spectrum* – DSSS, que utiliza do método de modulação DBPSK e o DQPSK.

IEE 802.11b

Foi publicado o suplemento 802.11b, em setembro de 1999, que trouxe novas especificações de taxas de transmissão para os equipamentos *wireless*. As especificações previam características para camada física operando em DSSS, com 2,4 GHz e taxas de transmissão de 1Mbps, 2 Mbps, 5,5 Mbps e 11Mbps.

São definidas as especificações de modulação BPSK E QPSK com CCK.

IEEE 802.11a

Foi criado um grupo para o desenvolvimento do padrão 802.11a, na mesma época da publicação do padrão 802.11b.

No 802.11a foi criado um novo método de transmissão para a camada física, conhecida como "*Orthogonal Frequency Division Multiplexing*" – OFDM, que utiliza a banda "*Unlicensed National Information Structure*" (U-NII). Nesta banda, o sinal opera em três faixas de frequência: 5.15 – 5.25 GHz, 5.25 – 5.35 GHz e 5.725 – 5.825 GHz

Nessa especificação são constituídas as capacidades de comunicação de dados a 6, 9,12,18,36,48 e 54 Mbps, sendo que as taxas de 6, 12 e 24 Mbps são obrigatórias.

O sistema OFDM utiliza 52 subportadoras moduladas por *binary* ou *quadrature phase keying* – BPSK/QPSK, 16 – *quadrature amplitude modulation* – QAM , ou 64-QAM.

Somente no início de 2002, os primeiros produtos com o padrão 802.11a começaram a aparecer comercialmente. Movendo-se para a frequência de 5 GHz, esse padrão apresenta duas vantagens sobre o 802.11b:

1- Ele aumenta a velocidade máxima por canal a até 54 Mbps contra 11 Mbps do 802.11b;

2- Até 8 canais não sobrepostos estão disponíveis contra 3 canais no 802.11b. Assim, o 802.11a pode suportar um número maior de usuários simultaneamente sem qualquer conflito. Estes benefícios, entretanto, vêm com a desvantagem da incompatibilidade. Uma vez que o 802.11b opera em 2,4 GHz e o 802.11a opera a 5 GHz, a comunicação entre ambos é inviável. A alta frequência da operação do 802.11a equivale a um relativo baixo alcance. Será necessário um número maior de dispositivos 802.11a para cobrir uma mesma área.

IEE 802.11g

O padrão 802.11g foi criado em 2003, e trouxe especificações de taxas de transmissão de até 54 Mbps, operando a 2,4 GHz e usando modulação “*Orthogonal Frequency Division Multiplexing*” – OFDM.

Sua grande vantagem é a total compatibilidade com o padrão 802.11b, aproveitando todas as instalações já feitas naqueles equipamentos 802.11g operam em DSSS quando em taxas de até 11 Mbps. Nas demais velocidades, os produtos 802.11g usam a modulação OFDM.

Apesar de operar com taxas de transferência idênticas (até 54 Mbps), uma desvantagem do 802.11g para servir um grande número de usuários. A modulação OFDM atinge maiores velocidades, mas a largura de banda total disponível em 2,4 GHz permanece a mesma, porque o 802.11g está restrito a 3 canais em 2,4 GHz, diferente dos 8 canais disponíveis na banda de 5 GHz do 802.11a. A tabela 1 apresenta a comparação entre os padrões *wireless*.

Padrões *Wireless* LAN – Comparação

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

Fonte: (SAN, 2005).

Tabela 1- Padrões *wireless* Lan – comparação

***Wireless* World Area Network (WWAN)**

Esse padrão, ainda em proposta, pretende criar a possibilidade de comunicação *wireless* entre cidades.

O 802.16 foi estabelecido, em 1998, com objetivo de criar um padrão de conexão fixa *wireless* ponto-para-multiponto suportando uma ampla área de cobertura. É um sistema *wireless* capaz de alcançar toda uma cidade utilizando links de alta potência para criação de uma rede. O objetivo é proporcionar acesso *wireless* em banda larga para internet e telefonia via internet, utilizando

Voip. Unir diversos links *wireless* ponto a ponto afim de formar uma rede através de uma grande área geográfica é considerado uma WMAN, mas a tecnologia empregada é a mesma da WLAN.

A WMAN utiliza freqüências licenciadas e a WLAN utiliza freqüência não licenciada, tornando este fato o principal diferencial entre as duas.

2.1.1 Enlaces

A forma de conexão e de compartilhamento é estabelecida de acordo com a arquitetura adotada, sendo definidas as seguintes arquiteturas [IEEE Std 802.11b-1999 R2003]:

- 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.

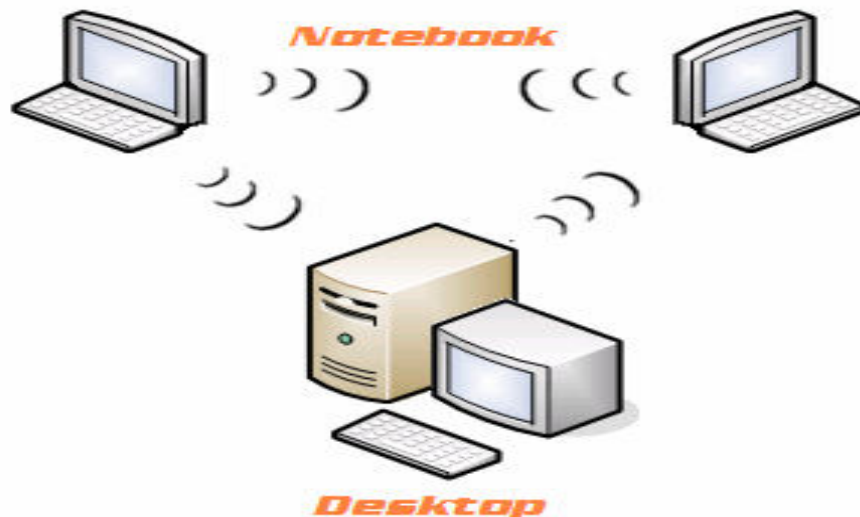


Figura 1. Redes AD Hoc

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*).

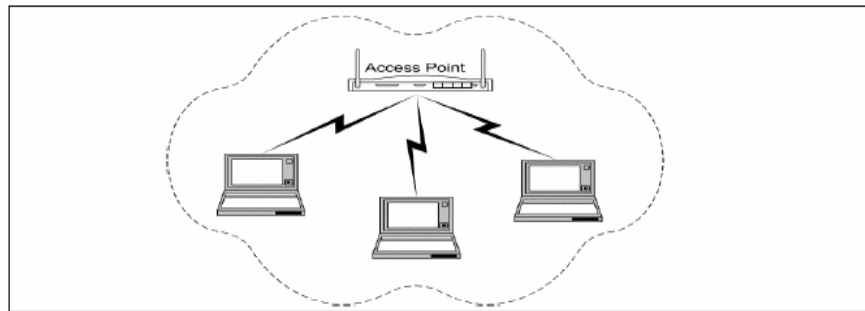


Figura 2. Rede BSS

São denominadas ESS (*Extended Service Set*) as redes de infraestrutura. 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.

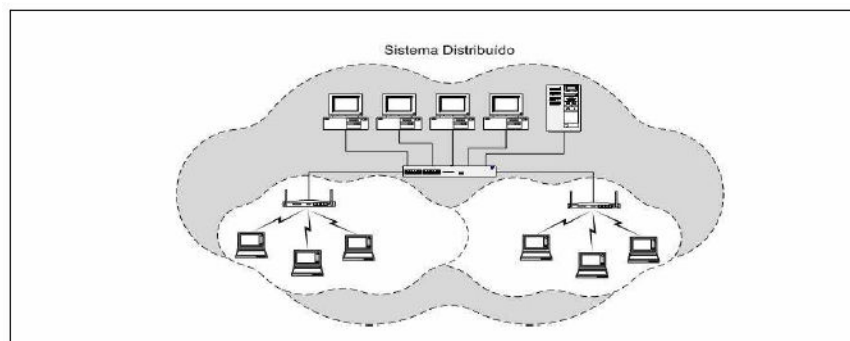


Figura 3. Rede ESS.

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.

2.1.2 Mecanismos de Segurança

Ao se falar em 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 sendo 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, e como pode-se evitar que intrusos localizem nossos sinais, pois como já se sabe o transmissor são omni-direcionais irradiando ondas de rádio e 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 conexão sem fio, esteja imune destes intrusos e que suas informações estejam trafegando em um ambiente preparado para sua maior confiabilidade e maior usabilidade.

Como percebe-se, segurança é o principal problema das redes sem fio e pensando nisso, um grupo de estudo da IEEE, começou a desenvolver técnicas que realmente possam melhorar o tráfego das informações nas redes sem fio, aonde se chegaram primeiramente no protocolo WEP (*Wired Equivalent Privacy*), protocolo este, desenvolvido para suprir todas e qualquer deficiência 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 acabaria os problemas de segurança que rodeiam a redes sem fio, mas em pouco tempo tornou-se um protocolo muito vulnerável e fácil de ser quebrado.

Com estes problemas, a IEEE adiantou algumas cifras e autenticação para um novo protocolo (oriundo do padrão 802.11i) denominado como WPA (*Wi-fi Protected Access*), muitas inovações fazem parte deste protocolo, que busca suprir todas as falhas apresentadas pelo protocolo WEP.

2.1.2.1 WEP (*Wired Equivalent Privacy*)

As redes sem fio ficam expostas a vários riscos tais como; roubo de informações, buscando proporcionar uma rede sem fio com maior segurança, a IEEE buscou melhorias no quesito segurança e o projeto foi denominado protocolo WEP *Wired Equivalent Privacy*, este protocolo traz a utilização de algoritmos simétricos, onde, uma codificação secreta (chave) deverá ser compartilhada entre o concentrador e as estações de trabalho, dando assim liberação para que mecanismos possam cifrar e decifrar fazendo que as informações tenham sempre um tráfego mais confiável, onde de acordo com RUFINO (2005, P.36) alguns critérios foram levados em consideração para o

desenho deste protocolo: "suficientemente forte, auto-sincronismo, requer poucos recursos computacionais, exportável, e de uso opcional".

Quando se fala deste protocolo, logo já vem á prevê-se todas aquelas vulnerabilidades e todos os problemas que já não são novidades a esse protocolo.

O maior problema do WEP, é que a cada vez mais, ele está sendo deixado de ser utilizado pela grande propaganda negativa que vive em torno deste protocolo, mas quando nada mais é possível, o WEP nos permite sair da completa insegurança que nos envolve, para um nível de segurança ainda aceitável.

Em algumas das implementações do WEP, são possíveis as associações a um método de autenticação como o 802.1x, para que se seja aumentado o nível de segurança, acrescentando uma menor vulnerabilidade.

Mas há outras maneiras de autenticação, como o uso de autenticação externa, modelo conhecido como EAP (*Extensible Authorization Protocol*), além da possibilidade de utilização de outras tecnologias, tais como, o RADIUS (Remote Authentication Dial-in User Service), que é um concentrador onde valida o acesso do cliente ao servidor.

Há um grande número de produtos RADIUS no mercado, onde se destacam entre eles, os de código aberto, que são o FreeRADIUS e o GNU RADIUS, onde podemos notar que o primeiro traz mais recursos e maior quantidade de métodos de autenticação.

2.1.2.2 Funcionamento do Protocolo WEP

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.

Na prática 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 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 nenhuma chance da segurança ser

comprometida. 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. Sendo que será utilizado um algoritmo CRC-32 que é utilizado para fazer o controle, onde ele gera um ICV de 4 bytes que deverá ser exatamente igual pelo receptor da mensagem, onde 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 plano.

Em um segundo estágio, é gerada uma seqüência de bits a partir da chave secreta (Bits), 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 um xor entre o resultado do *checksum* (texto plano) e a seqüência do RC4, onde o resultado deste xor constituirá o pacote a ser transmitido ao longo do ar.

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. Onde se tendo este vetor e conhecendo a chave secreta, o receptor utiliza-se do 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 plano (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 plano, onde o resultado do xor de qualquer numero será ele mesmo, desse modo é possível recuperar o pacote original, em seguida o receptor divide a mensagem em dois e em recomputa o CRC-32 e compara os resultados obtidos, onde 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 foram mantida na transmissão.

2.1.2.3 WPA (Wi-fi Protected Access)

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

O WPA inclui várias mudanças que foram feitas a este protocolo para que não haja 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 a certificar-se que apenas o usuário autorizado tenha acesso às informações. O WPA não traz suporte as Redes *Ad-Hoc*, pois o WPA visa segurança a redes que possuam um AP.

O WPA substitui completamente o WEP, com inovações quanto a cifração 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 a outras tecnologias, bem como a utilização do protocolo 802.1x e certificados digitais. Lembra-se, que a maior parte dos recursos disponíveis neste protocolo, não é disponível no modo *Ad-Hoc*.

Neste protocolo a utilização nativa é bastante simples de ser feita, onde poderá ser escolhida a opção por chave compartilhada, ou chave preestabelecida. Esta forma de configuração é bem simples, podendo ser alterada no sistema operacional que utilizamos, ou até mesmo na ferramenta específica disponibilizada pelo fabricante da placa de rede. Com a configuração feita através de chave compartilhada ou mais conhecida como WPA-PSK, tem como objetivo principal a fácil utilização e ao mesmo tempo prover de um bom nível de segurança. Onde a configuração do concentrador e do cliente, se resume em habilitar o uso do recurso (WPA-PSK), e escolher uma chave mestra difícil de ser decifrada.

2.2 Meios de Transmissão

O padrão 802.11 especifica algumas técnicas de transmissão permitidas na camada física. Inicialmente, foram definidos alguns métodos como FHSS (*Frequency Hopping Spread Spectrum*) e DSSS (*Direct Sequence Spread Spectrum*) que utilizam ondas de rádio operando a 2.4Ghz atingindo a taxa de transmissão de 2Mbps.

Em 1999 foram introduzidas novas técnicas de transmissão almejando uma maior largura de banda que são elas; o HR-DSSS (11 Mbps) e OFDM (54 Mbps).

2.2.1. Spread Spectrum

Spread Spectrum é uma forma de codificação para a transmissão digital de sinais. Desenvolvida originalmente pelos militares durante a segunda guerra mundial, com objetivo de camuflar as informações a serem transmitidas num sinal parecido com um ruído radioelétrico, evitando assim a interceptação e decodificação pelas forças inimigas.

A técnica consiste em codificar e modificar o sinal de informação, efetuando o seu espalhamento no espectro de freqüências. Espalhado o sinal ocupa uma banda maior que a informação original, porém possui baixa densidade de

potência, portanto, apresenta uma menor relação sinal/ruído. Em receptores convencionais comunicação poderá até ser imperceptível [SAN, 2005].

2.2.2. FHSS (*Frequency Hopping Spread Spectrum*)

FHSS é uma técnica de espalhamento espectral onde a banda de 2,4 Ghz, é dividida em 75 canais, as informações enviadas utilizarão todos estes 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.

2.2.3. DSSS (*Direct Sequence Spread Spectrum*)

DSSS (*Direct Sequence Spread-Spectrum*) é uma forma de modulação *spread-spectrum* que gera uma redundância padrão de bits para cada bit transmitido. 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. Chips maiores exigem maior largura de banda, porém 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 [SAN 2005].

2.2.4. OFDM (*Orthogonal Frequency Division Multiplexing*)

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, porem 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 à multi-percursos, geradores dos famosos "fantasmas" presenciados nas televisões analógicas [SAN, 2005].

3 Nível Físico

O nível físico trata apenas de transmissões com rádio freqüência (RF), há também outras formas de transmissão que podem ser empregadas com forma de transmissão, como microondas.

3.1 Microondas são ondas eletromagnéticas com comprimentos maiores que os dos raios infravermelhos, mas menores que das ondas de rádio variando, de 10 cm (3 GHz de frequência) até 1 mm (30 GHz de frequência). Também chamada de **SHF** - *Super High Frequency*.

3.2 Antenas pode-se definir antena como qualquer dispositivo que transmite e recebe ondas eletromagnéticas.

Esta atua como um transdutor entre o meio irradiado (espaço) e o meio guiado(cabo coaxial, guia de onda). Por um lado a antena recebe a energia eletromagnética da linha de transmissão e transforma em energia capaz de se propagar no espaço.

Essa energia pode ser direcionada para uma região do espaço. Dependendo dessa distribuição a antena vai ser classificada dentro de uma família (setoriais, direcionais, omnidirecionais...).

Por outro lado, a antena recebe a energia disponível no espaço e a transforma em energia capaz de se propagar numa linha de transmissão.

3.2.1 Antenas Direcionais

A irradiação se propaga em uma direção específica, estas antenas são utilizadas principalmente para enlaces ponto a ponto. Uma característica é de

possuir ganho superior às antenas omnidirecionais, se for utilizado um amplificador a distância máxima fica limitada apenas pela linha de visada.

3.2.2 Antenas Omnidirecionais

Irradiam as ondas em todas as direções, facilitando a instalação, porém possuem uma limitação na potência, não sendo utilizadas para enlaces de longo alcance. São utilizadas principalmente para *broadcast*, por isso é a mais utilizada em ambientes sem fio de baixo ou médio alcance.

3.2.3 Antenas Setoriais

É uma antena composta por um conjunto de dipolos alimentados em fase, e uma chapa refletora. O ganho e o ângulo de abertura de um painel depende do número de dipolos, das dimensões da chapa refletora, da distância entre os dipolos e sua eficiência na alimentação dos mesmos, que na maior parte das vezes se torna complexa.

4 Localização das Estações sem Fio

Os métodos tecnológicos existentes para a determinação da posição de uma estação envolvem medir a potência do sinal, ou a diferença do tempo da chegada do sinal ou ainda o ângulo de chegada do sinal. A eficácia dos sistemas para um ambiente *Indoor* limita-se também pelas reflexões, refrações, atenuação e interferências sofridas pelo sinal da Radiofrequência (RF). As três técnicas são analisadas a seguir.

4.1 AMPLITUDE DE CHEGADA (AMPOA – AMPLITUDE OF ARRIVAL)

Utiliza a amplitude do sinal entre o ponto de acesso e o cliente, onde é possível localizá-lo por meio de duas técnicas. Triangulação e *Fingerprinting*.

4.1.1 Triangulação

No momento em que se sabe qual a potência da recepção de um sinal entre um ponto de referência e um nó sem fios, é possível inferir uma distância entre eles. Esta distância representará o valor do raio de uma circunferência entre o ponto de referência e o elemento que se deseja localizar.

Para localizar fisicamente o nó, deve-se possuir outros pontos de referência, permitindo a determinação do ponto de intersecção entre as

diversas circunferências. Uma situação ideal, seria o mínimo de 3 pontos de referência necessários para que se possa localizar o nodo. A figura 4 representa esta situação. [XIANG, 2004]

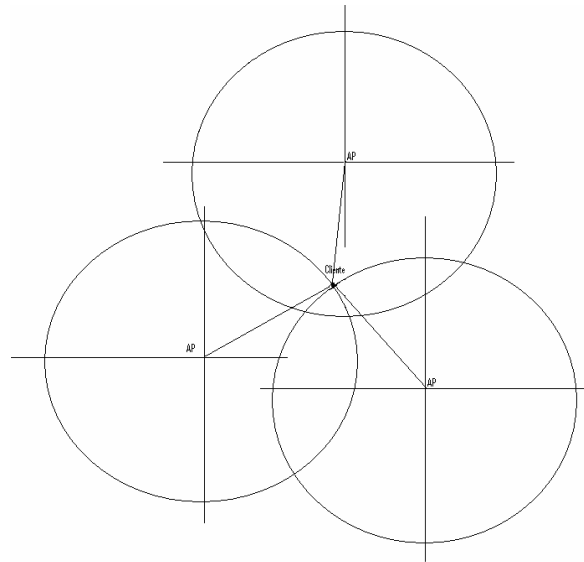


Figura 4: Três pontos de referência

A partir do momento em que se sabe qual a potência da recepção de um sinal entre um ponto de referência e um nodo sem fios, é possível inferir uma distância entre eles. Esta distância representará o valor do raio de uma circunferência entre o ponto de referência e o elemento que se deseja localizar. A figura 5 representa esta situação.

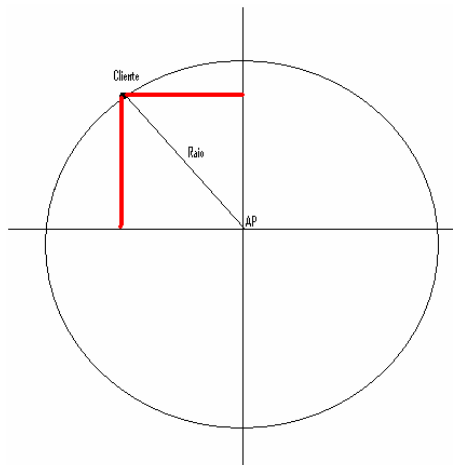


Figura 5: Distância entre ponto de referência e nodo sem fios.

Adiante no documento serão apresentados os conceitos matemáticos necessários para que se implemente o cálculo de intersecção de círculos e a conseqüente triangulação para obtenção da localização de uma estação móvel.

4.1.2 *Fingerprinting*

Também utilizando a potência do sinal recebido, é possível realizar um mapeamento em todo o perímetro físico que se pretende considerar na localização. A área física é dividida em quadrantes e uma amostragem das potências da recepção de sinal dos pontos de acesso é armazenada para cada quadrante, criando uma tabela. Desta forma, quando um cliente informa a potência de sinal entre ele e os pontos de acesso, a tabela é consultada e os valores mais próximos da situação do cliente são utilizados para localizá-lo. Esta técnica chama-se *fingerprinting*. Em [BAHL, 2000] a técnica é utilizada em um ambiente *indoor* e a figura 6 apresenta o mapeamento realizado.

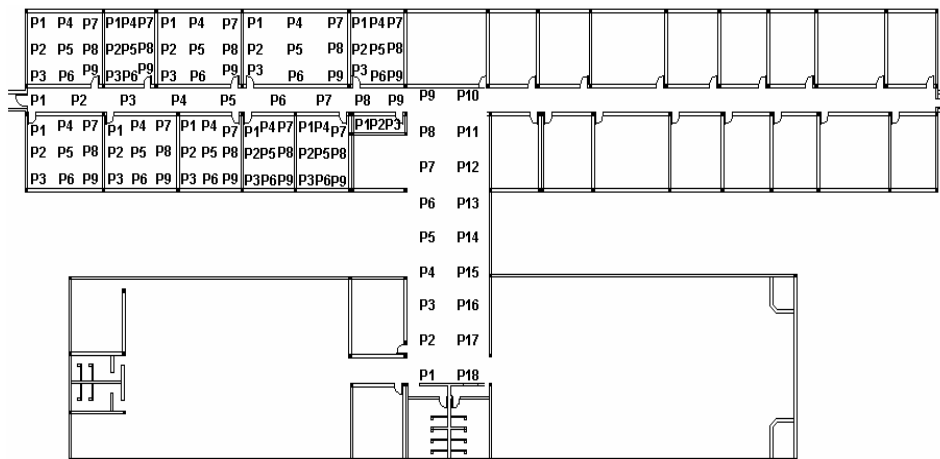


Figura 6: Mapeamento por *fingerprinting* [Suris, 2007].

4.2 TEMPO DE CHEGADA (TOA – TIME OF ARRIVAL)

Caso seja possível medir o tempo entre o envio de um sinal do ponto de referência até o nodo que se deseja localizar, é possível também a determinação de um raio equivalente à distância entre estes pontos. Cabe ressaltar que as microondas utilizadas nas redes IEEE 802.11, viajam a uma velocidade constante (velocidade da luz). [TAHERI, 2004]

Pelo fato da velocidade de propagação dos sinais de microondas ser alta, a precisão do relógio presente no computador não será capaz de identificar a distância com a mesma confiabilidade da potência (o erro de cálculo será elevado).

4.3 ÂNGULO DE CHEGADA (AOA – ANGLE OF ARRIVAL)

A técnica de medida de ângulo de chegada exige que o ambiente em estudo possua um conjunto de antenas direcionais em cada ponto de acesso. Ao receber um sinal proveniente da estação móvel, o ponto de acesso determina qual das antenas recebe o sinal com a maior amplitude, conseguindo assim identificar a direção de onde o sinal foi gerado. Com esta informação é possível determinar uma linha reta entre o ponto de acesso e a estação móvel. Ao realizar o mesmo procedimento com outro ponto de acesso, têm-se duas linhas e é possível identificar a localização da estação através da intersecção das linhas. [TAHERI, 2004]

A figura 7 apresenta um exemplo de localização através de AOA.

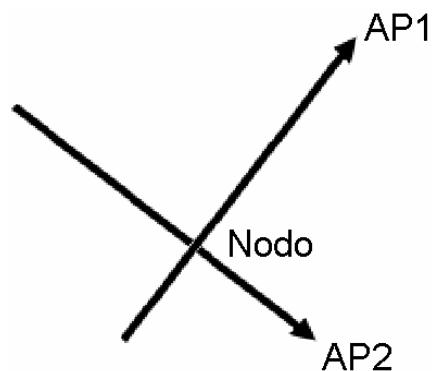


Figura 7: Exemplo de localização através de AOA

As duas técnicas citadas em seções anteriores, TOA - *Time of Arrival*, e o AOA - *Angle Of Arrival*, adicionam uma maior complexidade aos mecanismos de localização de estações, quando comparados com o AmpOA - *Amplitude of Arrival*. O TOA necessita de relógio precisos e sincronizados, especialmente ao se trabalhar em ambientes *indoor*, onde a precisão da localização torna-se importante.

O AOA necessita da adição de antenas direcionais nos pontos de acesso, o que não é uma prática comum em soluções comerciais.

5 Propagação

A propagação é um modo de transmissão de energia ao longo do meio.

5.1 Mecanismos de Propagação

Há três tipos básicos de mecanismos de propagação, são eles: 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, móveis, portas entre outros e no caso de ambientes abertos, podem ser montanhas, carros, prédios, casas, etc.

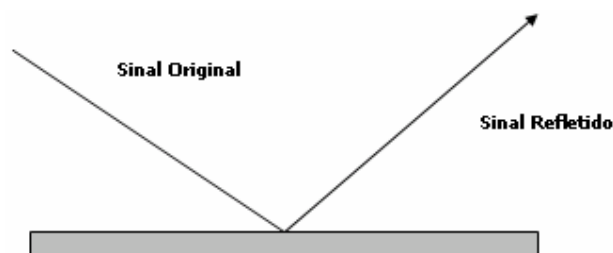


Figura 8: Reflexão de sinal

- Difração: Existe quando uma barreira obstrui a passagem do sinal entre o transmissor e receptor. De acordo com o princípio 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.

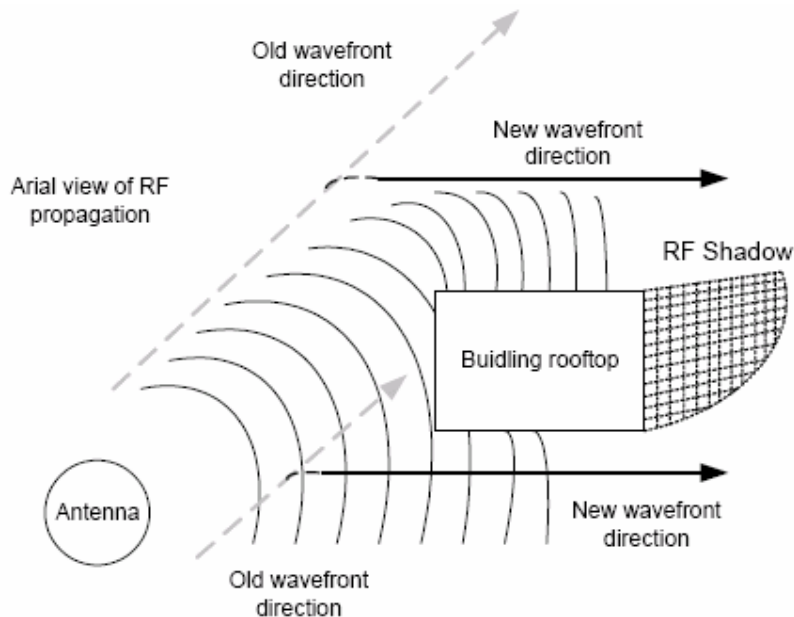


Figura 9: Como ocorre a difração do sinal

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

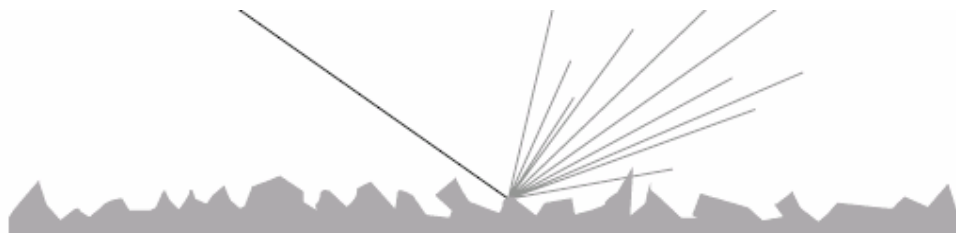


Figura 10: Espalhamento do sinal

5.1.2 Propagação e atenuação

O conceito de visibilidade é um conceito importante para propagação, visto que um enlace de rádio é dito em visibilidade se não houver difração. Para determinar se há ou não refração em um enlace é necessário calcular os limites da primeira zona de *Fresnel*.

A zona de *fresnel* é uma elipsóide, criada entre as antenas de transmissão e recepção.

Para que se possa identificar o raio da elipsóide da zona de *Fresnel*, utiliza-se a seguinte fórmula:

$$r = 547 \sqrt{\frac{D1 + D2}{f \times d}}$$

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 frequência 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 é criada através da fórmula de atenuação da microondas no ar:

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

onde A_w 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.

5.1.3 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, 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 frequência. 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.[AND96]

Em relação à frequência, a perda por penetração diminui com o aumento da frequência.

5.1.4 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 ao ambiente de propagação. A quantidade de interferência 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. [AND96]

O ambiente de propagação é diretamente relacionado com o tipo de construção e com o mobiliário onde se localiza a rede, se em uma sala há divisão por paredes de alvenaria, se são compostas por divisórias, se possuem muitas janelas, se nos móveis há composição de superfície metálica, existem muitas outras redes sem fio. Prédios que tem menos metal e que são constituídos por superfícies mais rígidas tipicamente oferecem menores atrasos médios da ordem de 30 a 60ms entre os diferentes raios em multipercurso. Esse tipo de ambiente pode suportar maiores taxas sem a necessidade de equalizadores da ordem de Mbps. Entretanto, ambientes com grande quantidade de metal, que pode ser o caso de indústrias, podem ter suas o atraso médio entre os diferentes raios da ordem de 300ms, o que limita as taxas à ordem de algumas centenas de kbps sem equalização.[AND96]

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.

Num 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 [ADE87], esse resultado pode ser estendido para frequências superiores, que é o caso das utilizadas no padrão 802.11.

Tabela 1 – Atenuação de Obstáculos em Microondas de 2.4 GHz [3COM 2005]

<i>obstáculo</i>	<i>atenuação</i>
parede de madeira sólida	6 dB
divisória de escritório com janela de vidro	4 dB
tijolo 3,5"	6 dB
parede de concreto 18"	18 dB
corpo humano	3 dB

6 Modelo Proposto

No primeiro semestre de 2007, o aluno Henrique Suris, desenvolveu um trabalho que consiste na localização de estações padrão 802.11. No trabalho foram criadas tabelas com o mapeamento das potências obtidas em cada posição baseando-se na técnica de *fingerprinting*. Este mapeamento foi obtido utilizando os comandos oriundos do sistema operacional *Linux*. As estações móveis enviam dados de potência ao servidor, e neste há um software desenvolvido em PHP que compara o valor informado com a tabela de *fingerprinting*, com isso determina a posição da estação móvel. Porém não é considerado as alterações das amostras de potência devido a eventuais obstáculos, podendo gerar uma informação incorreta da posição, então torna-se necessário aumentar a precisão.

Para efetuar o aumento de precisão haverá uma distribuição de equipamentos (Figura 11), no cenário proposto, visando mensurar a potência entre os mesmos, com isso poderemos identificar os obstáculos.



Figura 11 : Distribuição de equipamentos no ambiente.

Será utilizado o mesmo comando no *Linux*, e o software instalado no servidor fará a atualização das informações das tabelas do *fingerprinting* dinamicamente, conforme as mudanças na intensidade do sinal. Assim qualquer alteração levará em conta as medições dos demais equipamentos, atualizando as tabelas de *fingerprinting*.

7 Cenário

O cenário será a distribuição de equipamentos no laboratório de informática da ULBRA Campus Guaíba e suas dependências. Abaixo segue a figura 12 que demonstra as disposições das salas e dependências do 2º pavimento da Ulbra Guaíba.

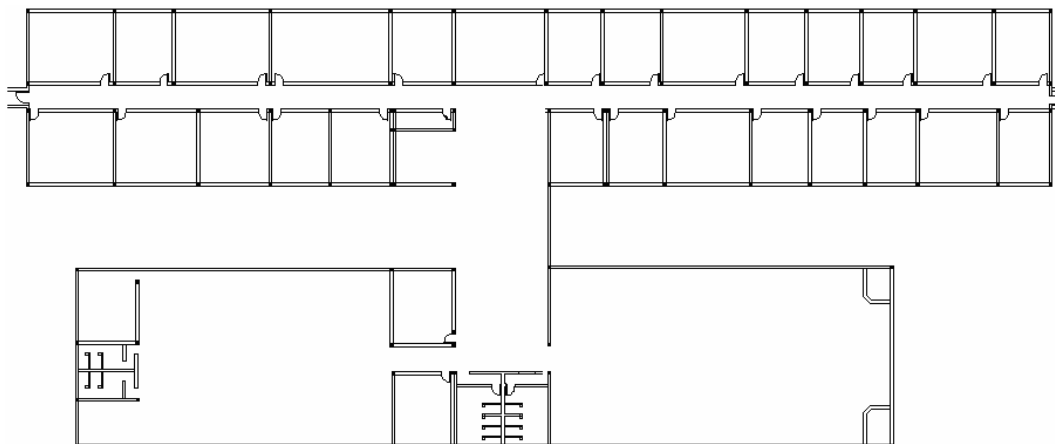


Figura 12: Planta baixa do 2ª andar da Ulbra Guaíba

8 Conclusão

Esta pesquisa visa atingir uma melhor precisão na localização de estações trabalho inicialmente desenvolvido por (Suris, 2007) que será utilizado como base. Inicialmente o trabalho de localização de estações não contempla os obstáculos que podem interferir na atenuação do sinal. Um obstáculo pode gerar uma alteração na informação de atenuação, se não for tratado, entende-se que a estação mudou sua posição geográfica, sendo que esta informação é falsa. Será utilizado o protótipo desenvolvido pelo Henrique Suris, e será inserida alterações que contemplem a existência de obstáculos. Serão ainda construídos dispositivos para análise de atenuação e uma das tarefas será identificar a quantidade e a posição que os mesmos deverão ser distribuídos pelo cenário. Serão realizados testes com o protótipo, visando obter resultados e eventuais ajustes no mesmo.. Será ainda verificado o impacto de atenuação em ambientes que possuem fluxo de pessoas em determinados horários, visando obter a informação de como esta movimentação incide na atenuação do sinal. Após todos os testes e ajustes será elaborado um relatório com o resultado final da pesquisa

Abaixo segue o cronograma das atividades a serem desenvolvidas:

Atividade / Mes	Mar	Abr	Mai	Jun	Jul
Construção de dispositivos	X	X			
Distribuição de dispositivos	X	X			
Alteração do prototipo		X	X		
Testes com prototipo		X	X		
Obtenção de Resultados				X	X
Escrita TCC II	X	X	X	X	X

9 Bibliografia

3COM (2005) “3Com Wireless Antennas Product Guide”, http://www.3com.com/other/pdfs/products/en_US/101900.pdf, Maio 2007.

Bahl, P.; Padmanabhan, V.N. e Balachandran, A. (2000) “Enhancements to the RADAR User Location and Tracking System,” Microsoft Research Technical Report, February 2000.

Battisti Julio, disponível em <http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless003.asp>
Acesso em 11/2007.

Matos, Luis – Guia Profissional de redes Wireless. São Paulo, SP, Digerati Books 2005. (MAT 2005)

Peres, A. ; Weber, R. F. . Mecanismo de Identificação Dinâmica da Atenuação de Obstáculos para Localização de Estações em Redes Sem Fios IEEE 802.11. In: V ERRC - Escola Regional de Redes de Computadores, 2007, Santa Maria. V ERRC - Escola Regional de Redes de Computadores, 2007.

Ross, John. O livro de Wi -Fi instale, configure, e use redes wireless (semfio). Rio de Janeiro, Alta Books -2003.

Suris, Henrique. Localização de Estações Sem Fio Padrão 802.11 In ULBRA – Campus Guaíba, 2007. Curso de Sistemas de Informação.

Santos Júnior, Arthur Roberto. Projetos de redes locais sem fio Wireless Lan Belo Horizonte MG, InstitutoOnline 2005. (SAN, 2005)

Taheri, A.; Singh, A.; Emmanuel, A. (2004). “Location fingerprinting on infrastructure 802.11 wireless local area networks (WLANs) using Locus”. Local Computer Networks, 2004. 29th Annual IEEE International Conference on 16-18 Nov. 2004