

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL  
INSTITUTO DE INFORMÁTICA  
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

ANDRÉ PERES

**Mecanismo de Autenticação Baseado na  
Localização de Estações Sem Fios Padrão  
IEEE 802.11**

Tese apresentada como requisito parcial  
para a obtenção do grau de  
Doutor em Ciência da Computação

Prof. Dr. Raul Fernando Weber  
Orientador

Porto Alegre, janeiro de 2010

## CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Peres, André

Mecanismo de Autenticação Baseado na Localização de Estações Sem Fios Padrão IEEE 802.11 / André Peres. – Porto Alegre: PPGC da UFRGS, 2010.

87 f.: il.

Tese (doutorado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR-RS, 2010. Orientador: Raul Fernando Weber.

1. Redes sem fios IEEE 802.11. 2. Localização de estações sem fios. 3. Segurança de sistemas. 4. Autenticação de redes. I. Weber, Raul Fernando. II. Título.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

Reitor: Prof. Carlos Alexandre Netto

Vice-Reitor: Prof. Rui Vicente Oppermann

Pró-Reitor de Pós-Graduação: Prof. Aldo Bolten Lucion

Diretor do Instituto de Informática: Prof. Flávio Rech Wagner

Coordenador do PPGC: Prof. Álvaro Freitas Moreira

Bibliotecária-chefe do Instituto de Informática: Beatriz Regina Bastos Haro

## **AGRADECIMENTOS**

Dedico este trabalho à Fabi, minha esposa, que sempre me incentivou, inspirou e mostrou que era possível conquistar esta batalha. Agradeço à minha família pela forma com a qual sempre me apoiou e acreditou no meu trabalho. Agradeço também ao meu orientador, Raul Weber, por todo seu apoio, paciência e sabedoria como pesquisador e amigo.

# SUMÁRIO

<b>LISTA DE ABREVIATURAS E SIGLAS</b> . . . . .	6
<b>LISTA DE SÍMBOLOS</b> . . . . .	8
<b>LISTA DE FIGURAS</b> . . . . .	9
<b>LISTA DE TABELAS</b> . . . . .	11
<b>RESUMO</b> . . . . .	12
<b>ABSTRACT</b> . . . . .	13
<b>1 INTRODUÇÃO</b> . . . . .	14
<b>2 PROPAGAÇÃO DE MICROONDAS</b> . . . . .	17
<b>2.1 Antenas</b> . . . . .	17
<b>2.2 Características da Propagação das Microondas e Obstáculos</b> . . . . .	19
2.2.1 Atenuação . . . . .	20
2.2.2 Reflexão . . . . .	22
2.2.3 Refração . . . . .	24
2.2.4 Difração . . . . .	24
2.2.5 Dispersão . . . . .	24
2.2.6 Ruídos e Interferências . . . . .	25
<b>2.3 Zona de Fresnel</b> . . . . .	25
<b>3 REDES IEEE 802.11</b> . . . . .	27
<b>3.1 Espalhamento Espectral</b> . . . . .	28
3.1.1 FHSS - <i>Frequency Hopping Spread Spectrum</i> . . . . .	28
3.1.2 DSSS - <i>Direct Sequence Spread Spectrum</i> . . . . .	29
3.1.3 HR-DSSS - <i>High-Rate DSSS</i> . . . . .	30
3.1.4 OFDM - <i>Orthogonal Frequency Division Multiplexing</i> . . . . .	32
<b>3.2 Tipos de Enlace IEEE 802.11</b> . . . . .	33
3.2.1 Arquitetura Ad-Hoc . . . . .	33
3.2.2 Arquitetura BSS - <i>Basic Service Set</i> . . . . .	33
3.2.3 Arquitetura ESS - <i>Extended Service Set</i> . . . . .	34
3.2.4 Redes MANET - <i>Mobile Ad-Hoc Networks</i> . . . . .	34
<b>3.3 Controle de Acesso ao Meio</b> . . . . .	35
<b>3.4 Mecanismos de Segurança IEEE 802.11</b> . . . . .	37
3.4.1 Confidencialidade . . . . .	37

3.4.2	Autenticidade . . . . .	43
3.4.3	<i>Manutenção da Confidencialidade e Autenticidade em Redes 802.11</i> . . . . .	44
<b>4</b>	<b>ESTADO ATUAL NA LOCALIZAÇÃO DE ESTAÇÕES</b> . . . . .	<b>45</b>
4.1	Localização por Análise de Tempo de Sinal . . . . .	46
4.2	Localização por Análise de Ângulo de Sinal . . . . .	46
4.3	Localização por Análise de Amplitude de Sinal . . . . .	46
4.4	Localização em Ambientes Internos Utilizando Amplitude . . . . .	47
4.5	Trabalhos Correlatos . . . . .	48
4.5.1	Trabalhos em Amplitude . . . . .	49
<b>5</b>	<b>MECANISMO IMPLEMENTADO</b> . . . . .	<b>54</b>
5.1	Protocolo de Associação Definido . . . . .	54
5.2	Localização das Estações . . . . .	57
5.2.1	Técnica de <i>Fingerprint</i> . . . . .	58
5.2.2	Identificação de Obstáculos Dinâmicos . . . . .	61
5.3	Aplicação da Política de Segurança . . . . .	64
5.4	Relação da Técnica desenvolvida com o Estado da Arte . . . . .	65
<b>6</b>	<b>TESTES E RESULTADOS OBTIDOS</b> . . . . .	<b>68</b>
6.1	Cenário de Testes . . . . .	68
6.2	Análise Realizada . . . . .	70
6.3	Situação 1 - Cenário livre de Obstáculos . . . . .	72
6.4	Situação 2 - Cenário Com Obstáculo Inserido . . . . .	74
6.5	Situação 3 - Cenário Com Obstáculo Dinâmicos em Período de Aula . . . . .	77
6.6	Compilação dos Resultados Obtidos . . . . .	78
<b>7</b>	<b>CONCLUSÕES</b> . . . . .	<b>80</b>
7.1	Em relação à Localização das Estações Móveis . . . . .	80
7.2	Em relação à Autenticação das Estações . . . . .	81
7.3	Trabalhos Futuros . . . . .	82
	<b>REFERÊNCIAS</b> . . . . .	<b>83</b>

## LISTA DE ABREVIATURAS E SIGLAS

AES	<i>Advanced Encryption Standard</i>
AmpoA	<i>Amplitude of Arrival</i>
AoA	<i>Angle of Arrival</i>
AP	<i>Access Point</i>
BPSK	<i>Binary Phase Shift Keying</i>
BSS	<i>Basic Service Set</i>
CCK	<i>Complementary Code Keying</i>
CSMA/CA	<i>Carrier Sense Multiple Access with Collision Avoidance</i>
CSMA/CD	<i>Carrier Sense Multiple Access with Collision Detection</i>
CTS	<i>Clear to Send</i>
DSSS	<i>Direct Sequence Spread Spectrum</i>
DPSK	<i>Differential Phase Shift Keying</i>
EAP	<i>Extensible Authentication Protocol</i>
ERP	<i>Effective Radiated Power</i>
ESS	<i>Extended Service Set</i>
FFT	<i>Fast Fourier Transform</i>
FSPL	<i>Free Space Path Loss</i>
FHSS	<i>Frequency Hopping Spread Spectrum</i>
GFSK	<i>Gaussian Frequency Shift Keying</i>
GPS	<i>Global Positioning System</i>
HR-DSSS	<i>High Rate Direct Sequence Spread Spectrum</i>
ICV	<i>Integrity Check Value</i>
IBSS	<i>Independent Basic Service Set</i>
IEEE	<i>Institute of Electric and Electronic Engeneers</i>
IFFT	<i>Inverse Fast Fourier Transform</i>
ISM	<i>Industrial Scientific and Medical</i>

IV	<i>Initialization Vector</i>
LLC	<i>Logical Link Control</i>
LOS	<i>Line of Sight</i>
MANET	<i>Mobile Ad-Hoc Network</i>
MS	<i>Mobile Station</i>
NAV	<i>Network Allocation Vector</i>
NLOS	<i>Non Line of Sight</i>
OFDM	<i>Orthogonal Frequency Division Multiplexing</i>
OSI	<i>Open System Interconnection</i>
OLSR	<i>Optimized Link State Routing Protocol</i>
PSK	<i>Pre-Shared Key</i>
QAM	<i>Quadrature Amplitude Modulation</i>
QPSK	<i>Quadrature Phase Shifting Keying</i>
RAS	<i>Remote Access Server</i>
PRNG	<i>Pseudo-Random Number Generator</i>
RADIUS	<i>Remote Authentication Dial In User Service</i>
RSSI	<i>Received Signal Strength Indicator</i>
RTS	<i>Request to Send</i>
TKIP	<i>Temporal Key Integrity Protocol</i>
ToA	<i>Time of Arrival</i>
ToF	<i>Time of Flight</i>
WDS	<i>Wireless Distribution System</i>
WEP	<i>Wired Equivalent Privacy</i>
WPA	<i>Wi-Fi Protected Access</i>
WPAN	<i>Wireless Personal Area Network</i>
WLAN	<i>Wireless Local Area Network</i>
WWAN	<i>Wireless Wide Area Network</i>

## LISTA DE SÍMBOLOS

$\lambda$	tamanho do período da onda em $m$
$P_{mw}$	potência de transmissão em $mw$
$P_t$	potência de transmissão na estação remetente em $dBm$
$A_{CaboT}$	a atenuação sofrida pelo sinal no cabo do transmissor em $dBm$
$P_{AT}$	potência da antena do transmissor em $dB_i$
$P_{AR}$	potência da antena do receptor em $dB_i$
$A_{CaboR}$	atenuação sofrida pelo sinal no cabo do receptor em $dBm$
$R_x$	potência do sinal recebido pelo destinatário em $dBm$
$r$	raio da elipsóide da zona de Fresnel em $m$
$D1$	distância entre a primeira antena e o ponto no centro da elipsóide da zona de Fresnel em $m$
$D2$	distância entre a segunda antena e o ponto no centro da elipsóide da zona de Fresnel em $m$
$d$	distância entre antenas em $m$
$R_M$	distância entre duas estações em $m$
$T_R$	tempo de recebimento do quadro ACK após envio de quadro de dados
$T_T$	é o tempo de transmissão do quadro de dados
$T_D$	é o tempo para o processamento e geração do quadro ACK pelo receptor
$Pr(d)$	é a atenuação na distância $d$
$\alpha$	fator de atenuação dependendo do tipo de ambiente
$X_\sigma$	variável randômica gaussiana com distribuição $\sigma$



## LISTA DE FIGURAS

Figura 2.1:	Relação entre sinal elétrico e potência de sinal de microondas de saída	18
Figura 2.2:	Tipos de antenas em relação ao ângulo de atuação . . . . .	19
Figura 2.3:	Atenuação por metro para 2.4GHz e 5.7GHz . . . . .	21
Figura 2.4:	Atenuação com Obstáculo . . . . .	23
Figura 2.5:	Reflexão do Sinal . . . . .	23
Figura 2.6:	Reflexão do Sinal em Antenas Direcionais . . . . .	23
Figura 2.7:	Refração do Sinal . . . . .	24
Figura 2.8:	Difração do Sinal . . . . .	24
Figura 2.9:	Dispersão do Sinal . . . . .	25
Figura 2.10:	Zona de Fresnel . . . . .	26
Figura 2.11:	Raio no centro da zona de Fresnel . . . . .	26
Figura 3.1:	Padrão IEEE 802.11 no OSI (IEEE, 1999a) . . . . .	27
Figura 3.2:	<i>Frequency Hopping Spread Spectrum</i> . . . . .	29
Figura 3.3:	<i>Direct Sequence Spread Spectrum</i> . . . . .	29
Figura 3.4:	Seqüência de Barker . . . . .	30
Figura 3.5:	<i>Orthogonal Frequency Division Multiplexing</i> . . . . .	32
Figura 3.6:	Enlace <i>Ad-Hoc</i> . . . . .	33
Figura 3.7:	Enlace <i>BSS</i> . . . . .	34
Figura 3.8:	Enlace <i>ESS</i> . . . . .	34
Figura 3.9:	Enlace <i>MANET</i> . . . . .	34
Figura 3.10:	Nodo Escondido Com CSMA ou CSMA/CD . . . . .	35
Figura 3.11:	Protocolo CSMA/CA . . . . .	36
Figura 3.12:	Possíveis estados de uma estação sem fios (IEEE, 1999a) . . . . .	38
Figura 3.13:	Funcionamento da Cifragem no Protocolo RC4 . . . . .	39
Figura 3.14:	Funcionamento da Decifragem Protocolo RC4 . . . . .	39
Figura 3.15:	Problema de Sincronismo em Transmissões Wireless . . . . .	40
Figura 3.16:	Funcionamento da Cifragem no Protocolo WEP . . . . .	40
Figura 3.17:	Funcionamento da Decifragem no Protocolo WEP . . . . .	40
Figura 3.18:	Autenticação 802.1x . . . . .	42
Figura 3.19:	Autenticação <i>Open System</i> . . . . .	43
Figura 3.20:	Autenticação <i>Shared Key</i> . . . . .	43
Figura 4.1:	Triangulação de distâncias . . . . .	45
Figura 4.2:	Exemplo de AoA. . . . .	47
Figura 4.3:	Resultados Obtidos em Ambiente Interno por (FARIA, 2005) . . . . .	50
Figura 4.4:	Resultados Obtidos em Ambiente Externo por (FARIA, 2005) . . . . .	50

Figura 5.1:	Protocolo Definido . . . . .	56
Figura 5.2:	Relação de Potência em Uma Comunicação AP-Estação . . . . .	57
Figura 5.3:	Linhas de Identificação de Obstáculos Dinâmicos . . . . .	62
Figura 5.4:	Definição de $\alpha$ entre dois APs . . . . .	64
Figura 5.5:	Processo de Autenticação com Localização de Estação . . . . .	65
Figura 6.1:	Planta Baixa do Cenário de Testes . . . . .	69
Figura 6.2:	Pontos de Amostragem de <i>Fingerprint</i> . . . . .	69
Figura 6.3:	Distribuição da Potência de um AP (dB) . . . . .	70
Figura 6.4:	Obtenção de Variações de Potência por Obstáculos Dinâmicos . . . . .	71
Figura 6.5:	Obstáculos Dinâmicos - Compilação de 48 horas . . . . .	71
Figura 6.6:	Obstáculos Dinâmicos - Período de Aula . . . . .	71
Figura 6.7:	Obstáculos Dinâmicos - AP1 - AP2 . . . . .	72
Figura 6.8:	Obstáculos Dinâmicos - AP1 - AP3 . . . . .	72
Figura 6.9:	Situação 1 - Comparativo entre as Técnicas de <i>Fingerprint</i> . . . . .	73
Figura 6.10:	Situação 1 - Precisão das Técnicas . . . . .	74
Figura 6.11:	Situação 2a - Comparativo entre as Técnicas de <i>Fingerprint</i> Sem Adição de Obstáculo . . . . .	75
Figura 6.12:	Situação 2a - Precisão das Técnicas . . . . .	75
Figura 6.13:	Situação 2a - Comparativo de Localização (sala) . . . . .	76
Figura 6.14:	Situação 2b - Comparativo entre as Técnicas de <i>Fingerprint</i> Com Adição de Obstáculo . . . . .	76
Figura 6.15:	Situação 2b - Precisão das Técnicas . . . . .	76
Figura 6.16:	Situação 2b - Comparativo de Localização (sala) . . . . .	77
Figura 6.17:	Situação 3 - Comparativo entre as Técnicas de <i>Fingerprint</i> . . . . .	78
Figura 6.18:	Situação 3 - Precisão das Técnicas . . . . .	78
Figura 6.19:	Situação 3 - Comparativo de Localização (sala) . . . . .	78

## LISTA DE TABELAS

Tabela 2.1:	Atenuação de Obstáculos para ondas de 2,4 GHz (3COM, 2005) . . . . .	22
Tabela 3.1:	Padrões de Nível Físico WLAN . . . . .	27
Tabela 3.2:	DSSS com DPSK . . . . .	30
Tabela 3.3:	DSSS com QPSK . . . . .	30
Tabela 3.4:	Codificação da primeira dupla de bits $b_0; b_1$ . . . . .	31
Tabela 3.5:	Codificação da segunda dupla de bits $b_2; b_3$ e <i>chips</i> $c_0-c_7$ correspondentes . . . . .	31
Tabela 3.6:	Codificação dos bits (2,3) (4,5) (6,7) . . . . .	31
Tabela 3.7:	Taxas de transmissão IEEE 802.11a e IEEE 802.11g (GAST, 2002) . . . . .	32
Tabela 4.1:	Resumo Comparativo dos Trabalhos Correlatos . . . . .	53
Tabela 5.1:	Comparativo Entre Técnicas de Localização . . . . .	58
Tabela 5.2:	Matriz de <i>Fingerprint</i> do AP1 . . . . .	59
Tabela 5.3:	Matriz de <i>Fingerprint</i> do AP2 . . . . .	59
Tabela 5.4:	Matriz de <i>Fingerprint</i> do AP3 . . . . .	60
Tabela 5.5:	Matriz $D_{AP1}$ . . . . .	60
Tabela 5.6:	Matriz $D_{AP2}$ . . . . .	61
Tabela 5.7:	Matriz $D_{AP3}$ . . . . .	61
Tabela 5.8:	Somatório das Matrizes de Diferença de Potência $P$ . . . . .	62
Tabela 5.9:	Resumo Comparativo dos Trabalhos Correlatos e Técnica Desenvolvida . . . . .	66
Tabela 6.1:	Compilação dos Resultados Obtidos . . . . .	79

## RESUMO

A vantagem das redes locais sem fios, as quais permitem que uma estação móvel possa deslocar-se livremente dentro da área de abrangência da rede, possui uma contrapartida em termos de segurança. A possibilidade dos sinais de microondas atravessarem paredes e sofrerem atenuação, reflexão, refração, difração e dispersão, dependendo dos obstáculos, torna a definição dos limites da área de abrangência da rede sem fios uma tarefa difícil. Sem o conhecimento dos limites de abrangência, o administrador não tem como delimitar fisicamente o acesso à rede. Além disso, o padrão IEEE 802.11 não define um mecanismo capaz de localizar a posição física de estações móveis. Sem a possibilidade de localização de estações, é impossível restringir o acesso à rede baseando-se em limitações físicas definidas pelo administrador. Quando a rede sem fios é utilizada em ambientes internos, os diversos obstáculos e seu comportamento dinâmico (como pessoas em movimento, por exemplo), fazem com que os sinais de microondas alterem as características da área de abrangência da rede. Este trabalho propõe uma nova abordagem para localização de estações sem fios em ambientes internos, baseada no comportamento dinâmico dos obstáculos e conseqüentes alterações na rede, e, de acordo com este comportamento, tenta ampliar a eficiência da localização de estações. Por fim, é proposto um novo sistema de autenticação de estações baseado na sua localização.

**Palavras-chave:** Redes sem fios IEEE 802.11, localização de estações sem fios, segurança de sistemas, autenticação de redes.

## IEEE 802.11 Authentication Mechanism Based on Wireless Station Location

### ABSTRACT

The advantage of wireless local area networks, giving the mobile stations the possibility of moving free inside the network access range comes with a security drawback. The fact that microwave signals can cross walls and behave with attenuation, reflections, refraction, diffraction and dispersion, depending of the obstacles, makes very difficult to define the network access range. Without the knowledge of the network boundaries, the network administrator cannot define a physical delimiter to network access. Besides this issue, there is no default user-location mechanism in the IEEE 802.11 standard. Without the user-location, it is impossible to restrict the network access based on the physical access boundaries defined by the administrator. When the wireless network operates indoor the many obstacles and the dynamic behavior of these obstacles (some people moving around, for instance) make the microwave signal behavior change the range and aspect of the network. This work proposes a new approach to indoor user-location mechanism, based on the dynamic behavior of the obstacles and consequent changes on network range. This approach focus on the dynamic obstacles behavior analysis and according to this behavior tries to increase the user-location system efficiency. Finally a new authentication system based on the user location is proposed.

**Keywords:** *wireless local area networks IEEE 802.11, wireless location, network security, network authentication.*

# 1 INTRODUÇÃO

A utilização de comunicação sem fios representa hoje uma grande porcentagem da troca de dados tanto em ambientes comerciais, quanto domésticos. Quando se utiliza uma estrutura de redes sem fios, têm-se normalmente como objetivo ampliar os serviços de conexão à rede com a disponibilização de mobilidade e flexibilidade de acesso. A mobilidade garante que uma estação estará conectada, podendo movimentar-se livremente em qualquer momento, desde que permaneça dentro da área de abrangência da rede (definida pelos pontos de acesso sem fios).

A flexibilidade provê a independência de estrutura física de cabeamento para distribuir as diversas estações dentro da rede, além da simplicidade na adição e retirada de estações da mesma. É possível então que as estações estejam em qualquer parte da abrangência da rede, concentradas em uma mesma sala ou dispersas, sem que seja necessário qualquer intervenção física.

Apesar destas facilidades, quando compara-se uma rede com fios com uma rede sem fios, nota-se que esta última adiciona algumas características que podem ser consideradas prejudiciais à gerência e segurança da rede. Em uma rede sem fios, os limites físicos da área de abrangência são de difícil definição, tendo em vista o comportamento dos sinais utilizados para a comunicação. Situações de atenuação de sinal, reflexão, refração, difração e dispersão, acabam por distribuir o alcance da rede de forma irregular, de acordo com os obstáculos presentes no ambiente. Não é possível confinar o sinal em uma área restrita de acesso, nem ter conhecimento preciso de até onde vai a abrangência da rede.

Ainda, comparando-se as duas tecnologias de enlace com e sem fios, nota-se que em uma rede com fios, a comutação de pacotes é de fácil implementação, ou seja, em um mesmo ambiente é possível a coexistência de diversas redes separadas por um equipamento de *switch* gerenciável, roteador ou *firewall*, controlando o acesso e troca de dados entre elas. Apesar de possibilitar a coexistência de redes diferentes através de multiplexação de canais (as redes IEEE 802.11, por exemplo, permitem até 11 redes em canais de frequência diferentes), não existe um mecanismo capaz de restringir fisicamente o acesso de uma estação a qualquer rede, bastando que o cliente defina o canal ao qual deseja associar-se.

Durante o desenvolvimento do padrão de redes locais sem fios IEEE 802.11 (IEEE, 1999a) (IEEE, 1999b) (IEEE, 2003), foram considerados os impactos da mobilidade e flexibilidade na segurança da rede e conseqüentemente adicionados mecanismos de segurança visando a garantia de confidencialidade e autenticação de estações. Atualmente o padrão IEEE 802.11i (IEEE, 2004) define a utilização de criptografia através do algoritmo AES (*Advanced Encryption Standard*) fornecendo a confidencialidade dos dados e o padrão 802.1x que garante a autenticação de clientes através de negociação entre o cliente e um servidor específico (como um servidor RADIUS). Um estudo mais detalhado dos

mecanismos de segurança é apresentado na seção 3.4.

Outra característica prejudicial à gerência e segurança (e não prevista pelos padrões IEEE 802.11) é a falta de mecanismos precisos para localizar os diversos dispositivos distribuídos pela rede. Este fato impede a localização física de uma estação maliciosa e a definição e restrição de acesso à rede de acordo com um perímetro pré-determinado. No caso das redes locais sem fios, é possível por exemplo, que um usuário malicioso acesse a rede de uma empresa a partir do exterior do prédio, sem que sua localização seja identificada. O mesmo não ocorre em redes com fios, onde as restrições físicas de acesso à rede permitem que, com uma boa gerência, seja possível localizar o ponto de rede do qual parte um determinado pacote de dados. Da mesma forma, a inexistência da possibilidade da localização física das estações não permite que se defina uma política baseada nesta informação. Não é possível, por exemplo, definir uma política de acesso distinta em um enlace sem fios de acordo com a sala na qual o usuário se encontra.

Vários tipos de enlaces sem fios apresentam as características mencionadas, podendo-se citar as redes de telefonia celular (voz e dados); redes pessoais WPAN (*Wireless Personal Area Network*), redes de grande abrangência WWAN (*Wireless Wide Area Network*), e as redes locais sem fios WLAN (*Wireless Local Area Network*). As redes celulares possuem, atualmente mecanismos capazes de realizar a localização de estações móveis através da triangulação de potências entre as torres envolvidas na comunicação. As redes WPAN possuem uma área de abrangência de aproximadamente 10 metros, o que torna de pouca relevância a localização de dispositivos. As redes WWAN possuem as mesmas características das redes de telefonia móvel, tornando possível a triangulação de potência entre torres e dispositivo móvel. O foco deste trabalho fica, então, restrito a mecanismos de localização de estações em redes WLAN com o objetivo de possibilitar o desenvolvimento de um método de autenticação de clientes baseado nesta localização física.

Para que este objetivo seja alcançado, é necessário que se considere o ambiente no qual a rede se encontra. Nota-se que as redes locais sem fios são, na maioria das implementações, utilizadas em ambientes internos (*indoor*), com a presença de diversos obstáculos entre o transmissor e receptor dos sinais. Este fato impede que a localização de dispositivos seja feita da mesma forma que nos sistemas de localização para redes de telefonia móvel ou WWAN. Ressalta-se também que em ambientes externos, a precisão da localização pode possuir um erro maior (vários metros), em comparação a ambientes internos, sem que se perca o foco primordial da localização (determinar a região à qual a estação se encontra).

Mesmo com a garantia de confidencialidade através de criptografia e autenticidade através do padrão 802.1x, nenhum mecanismo de localização das estações sem fios foi proposto como padrão pelo IEEE. Desta feita, o trabalho aqui proposto tem por objetivo apresentar um mecanismo capaz de ampliar os mecanismos de segurança existentes, fornecendo à rede uma forma de identificar fisicamente a localização de uma estação que deseja associar-se à rede, verificando se a mesma encontra-se dentro dos perímetros permitidos para tal ação. Desta forma, torna-se possível ao administrador ampliar o controle de acesso a uma determinada rede através de segurança física de perímetro, ou seja, através da definição de limites físicos para permitir a associação.

A principal questão abordada por este trabalho é:

**Criação de um mecanismo para realizar a localização de estações sem fios IEEE 802.11 em um ambiente *indoor* permitindo que a infra-estrutura da rede possa controlar o acesso de estações e aplicar uma política de segurança baseada em perímetros físicos de localização.**

O restante do volume está organizado da seguinte forma: no próximo capítulo são descritas as características de propagação das microondas no ar, e seu comportamento frente à obstáculos (devido à importância deste tema em ambientes *indoor*). No capítulo 3, são descritas as características definidas no padrão IEEE 802.11, referentes aos diferentes tipos de enlaces e mecanismos de segurança existentes no padrão. No capítulo 4 são apresentados os diferentes modelos existentes atualmente para realizar a localização de estações sem fios e os aspectos referentes à utilização destes mecanismos em ambientes *indoor*. No capítulo 5 é apresentada a técnica de localização implementada e o cenário de testes utilizado para validação do protótipo. O capítulo 6 apresenta os resultados obtidos durante os testes do protótipo implementado. O capítulo 7 apresenta as conclusões do trabalho realizado e propostas para trabalhos futuros.



## 2 PROPAGAÇÃO DE MICROONDAS

Os equipamentos em uma rede local sem fios realizam a comunicação através de sinais de microondas. Para que se compreenda a forma com a qual os sinais utilizados para representar os bits são transmitidos, é necessário que se apresente os conceitos básicos sobre criação de radiofrequências e propagação de microondas no ar.

### 2.1 Antenas

As antenas são os elementos básicos para a comunicação sem fios. O objetivo de uma antena é possibilitar a conversão de uma corrente elétrica em uma onda de radiofrequência e vice-versa. Ao aplicar-se uma corrente variante em um condutor, os elétrons livres são acelerados e se deslocam através dos espaços livres existentes entre os átomos (FUSCO, 2006). Quando a corrente é alternada, os elétrons de uma determinada região do condutor se movem para frente e para trás no mesmo ritmo, definido pela frequência da tensão aplicada. A aceleração ou desaceleração destes elétrons faz com que ocorra a radiação, formada por um campo elétrico e um campo magnético, dando origem a uma onda eletromagnética, ou seja, uma onda de radiofrequência.

Quando uma onda eletromagnética atinge uma antena, ela realiza a ação inversa, fazendo com que esta onda crie a aceleração e desaceleração dos elétrons, gerando uma corrente elétrica de mesmas características da corrente original.

A potência do sinal elétrico é medida em miliwatts (*mw*), sendo que o sinal de radiofrequência propagado, tem sua potência expressa em decibéis (*dB*). O *dB* é uma unidade que representa a relação entre duas potências expressas em miliwatts, tendo esta relação definida na fórmula 2.1, conforme (GAST, 2002).

$$dB = 10 \log\left(\frac{P_{entrada}mw}{P_{saida}mw}\right) \quad (2.1)$$

Um sistema amplificador possui um valor *dB* positivo, pois a potência de entrada no sistema é inferior à potência de saída. Já um sistema que causa atenuação do sinal possui um valor *dB* negativo, pois a potência de entrada será superior à potência de saída.

Para criar-se uma relação absoluta (de referência) entre *mw* e potência de transmissão, utiliza-se a unidade de medida *dBm*. A unidade *dBm* é a relação *dB* entre a potência de transmissão em *mw* e o valor de *1mw* (THOMPSON; TAYLOR, 2008). A fórmula 2.2 expressa esta relação, a qual é representada graficamente na figura 2.1.

$$dBm = 10 \log\left(\frac{Pmw}{1mw}\right) \quad (2.2)$$

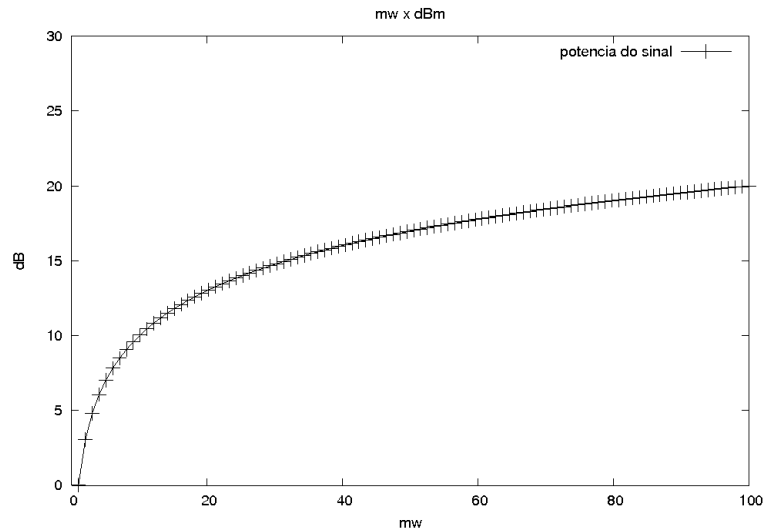


Figura 2.1: Relação entre sinal elétrico e potência de sinal de microondas de saída

Ou seja, uma placa de rede sem fios que possui uma potência de  $50mw$  irá transmitir aproximadamente  $17dBm$  de potência, conforme expresso na equação 2.3.

$$dBm = 10 \log\left(\frac{50mw}{1mw}\right) = 16,989dBm \quad (2.3)$$

O sinal transmitido pela placa de rede é levado para a antena através de um meio de transmissão (ligação entre a placa e a antena). Conforme o meio de transmissão existente entre a placa e a antena, têm-se maior ou menor atenuação do sinal. As medidas de atenuação são expressas em dB (conforme a equação 2.1).

Ao atingir a antena, será adicionado o ganho da antena à potência do sinal. As antenas possuem seu ganho expresso em  $dB_i$ . A unidade  $dB_i$  é uma unidade relativa entre a antena utilizada e uma antena teórica isotrópica (KRAUS, 1950). A antena isotrópica é uma antena capaz de irradiar energia uniformemente em todas as direções. Esta antena não é fisicamente factível, sendo utilizada apenas como referência (FUSCO, 2006).

A utilização das unidades  $dB$ ,  $dBm$  e  $dB_i$  permite que se calcule de maneira simples a potência irradiada por um sistema de radiofrequência através de cálculos de soma e subtração. Para que se calcule a potência efetivamente irradiada (*Effective Radiated Power*, ou ERP), ou seja, a potência de sinal que será transmitido na extremidade da antena de transmissão de um sistema, utiliza-se a equação 2.4, conforme (SMITH; GERVELIS, 2003).

$$ERPdB = P_t dBm - A_{CaboT} dB + G_{AT} dB_i \quad (2.4)$$

onde  $P_t$  representa a potência em  $dBm$  da placa de rede,  $A_{CaboT}$  a atenuação sofrida pelo sinal no cabo entre a placa de rede e a antena em  $dB$ , e  $G_{AT}$  é o ganho em  $dB_i$  da antena utilizada para a transmissão. No exemplo apresentado na equação 2.3, caso se utilize uma placa de rede que transmite com a potência de  $17dBm$ , com um cabo entre a placa de rede e a antena aplicando uma atenuação de  $2dB$  e fosse utilizada uma antena com ganho de  $8dB_i$ , teria-se a ERP expressa na equação 2.5.

$$ERP = 17dBm - 2dB + 8dB_i = 23dB \quad (2.5)$$

Como visto, as antenas possuem diferentes ganhos, sendo classificadas de acordo este valor (expresso em *dBi*) ou de acordo com o seu ângulo de irradiação. Em relação ao ângulo, têm-se antenas omnidirecionais, direcionais e setoriais.

As antenas omnidirecionais irradiam as ondas eletromagnética em todas as direções em torno da antena, criando uma área de abrangência de 360 graus em torno da mesma. São normalmente utilizadas em ambientes internos, ou em áreas em que se busca distribuir a potência de irradiação em torno da antena.

As antenas direcionais são utilizadas normalmente para enlaces ponto-a-ponto e possuem um ângulo de irradiação estreito. O seu objetivo é o de concentrar a potência de irradiação em uma única direção, aumentando a distância abrangida dentro deste ângulo.

As antenas setoriais possuem um ângulo de abrangência maior que as direcionais, porém não compreendem 360 graus. Existem diversos tipos de antenas setoriais, com ângulos de 45, 90, 120 graus, entre outros. Normalmente são utilizadas para criar ligações ponto-multiponto, ou utilizadas em conjunto ampliando a área de abrangência (três antenas setoriais de 120 graus utilizadas em conjunto para dar abrangência de 360 graus).

A figura 2.2 representa os três tipos de antenas, de acordo com o ângulo de irradiação.

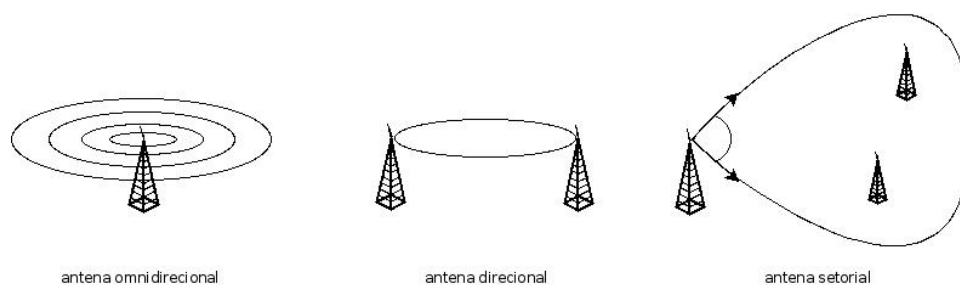


Figura 2.2: Tipos de antenas em relação ao ângulo de atuação

Independente do tipo de antena, a propagação das microondas sempre é considerada comparando-se com a irradiação de uma antena isotrópica. Desta forma, é possível a utilização das mesmas fórmulas de propagação para qualquer tipo de antena, mantendo-se esta referência.

## 2.2 Características da Propagação das Microondas e Obstáculos

Durante a propagação dos sinais de microondas, existem diversos fatores capazes de causar alterações no seu comportamento. Estas alterações dizem respeito a atenuação, reflexão, refração, difração e dispersão do sinal propagado, além da adição de ruídos causados pelo meio de transmissão ou por interferências.

O grau de interferência e características de propagação estão diretamente relacionados com a frequência utilizada pelo sinal propagado. Por este motivo, as próximas seções irão abordar as interferências ocasionadas em sinais de 2,4 GHz e 5,7 GHz, faixas ISM (*Industrial Scientific and Medical*) utilizadas pelas placas de rede IEEE 802.11, conforme será apresentado posteriormente na tabela 3.1.

A escolha destas frequências se deve ao fato de que as faixas ISM são definidas como públicas para uso por qualquer indivíduo, independente de concessões do governo. Isto torna os componentes que utilizam a tecnologia IEEE 802.11 exportáveis e compatíveis em qualquer país (ITU, 2002).

### 2.2.1 Atenuação

Como qualquer sinal enviado em um meio de comunicação, os sinais de microondas sofrem atenuação, ou seja, perda de potência do sinal devido à transmissão. No caso da propagação de microondas, dois fatores influenciam na perda desta potência: a distribuição do sinal no espaço durante a transmissão; e a capacidade da antena de recepção de captar o sinal.

Sempre que o sinal é propagado, espalha-se no espaço conforme o ângulo de abertura da antena de transmissão. A potência do sinal é distribuída na área de propagação até atingir a antena de recepção.

Para criação de uma referência ao modelo de atenuação, utiliza-se o ângulo de abertura de antenas isotrópicas. Uma antena isotrópica é capaz de propagar os sinais em todas as direções, formando uma esfera em torno da antena. A potência do sinal transmitido é distribuída uniformemente nesta esfera. A área  $A$  de uma esfera de raio  $r$  pode ser determinada conforme a fórmula 2.6 (KRAUS, 1950).

$$A = 4\pi r^2 \quad (2.6)$$

Isto significa que para que se possa identificar a distribuição  $S$  de potência em uma antena isotrópica, divide-se esta potência pela área da esfera, conforme a fórmula 2.7 (WALKE; MANGOLD; BERLEMANN, 2006).

$$S = \frac{P_t}{4\pi d^2} \quad (2.7)$$

Onde  $S$  é a potência do sinal distribuído por área expressa em *watts* por  $m^2$ , na distância (raio da esfera)  $d$ , e  $P_t$  é a potência de transmissão em *watts*. A partir desta fórmula, identifica-se que a potência de um sinal em um determinado ponto é proporcional ao quadrado da distância entre este ponto e a antena de transmissão, e à distribuição de potência na esfera de propagação, conforme a fórmula 2.8.

$$P_t = S4\pi d^2 \quad (2.8)$$

O segundo fator diz respeito à capacidade da antena de captar o sinal de acordo com sua abertura, ou seja, qual a área de sinal que será captado pela antena. Para uma antena isotrópica, este valor é definido pela equação 2.9 (KRAUS, 1950).

$$P_r = S \frac{\lambda^2}{4\pi} \quad (2.9)$$

Onde  $P_r$  é a potência recebida em *watts*,  $\lambda$  é o comprimento da onda (ou seja, esta relação depende da frequência da onda utilizada). Para que se obtenha, então a perda de potência durante a transmissão, utiliza-se a relação em *dB*, conforme a equação 2.1, com  $P_{entrada} = P_t$  e  $P_{saida} = P_r$ .

$$10 \log\left(\frac{P_t}{P_r}\right) = 10 \log\left(\frac{S4\pi d^2}{S \frac{\lambda^2}{4\pi}}\right) = 10 \log\left(\frac{(4\pi d)^2}{\lambda^2}\right) \quad (2.10)$$

Têm-se então que, quando da transmissão de microondas no vácuo, o fator de atenuação é representado pela equação 2.11 de FSPL (*Free Space Path Loss*).

$$FSPL = 20 \log\left(\frac{4\pi d}{\lambda}\right) \quad (2.11)$$

onde  $FSPL$  é a atenuação em dB,  $d$  é a distância em metros e  $\lambda$  é o comprimento da onda em metros.

Os sinais de microondas propagam-se em velocidade próxima à velocidade da luz, ou seja  $3 \times 10^8 m/s$ . Isto significa que para uma onda de 2,4 GHz (802.11b e 802.11g), têm-se  $\lambda$  com o valor de aproximadamente 0,125m e para ondas de 5,7 GHz (802.11a) de aproximadamente 0,06m, conforme as equações 2.12 e 2.13.

$$\lambda = \frac{1}{2,4 \times 10^9} \times (3 \times 10^8) \simeq 0,125m \quad (2.12)$$

$$\lambda = \frac{1}{5,7 \times 10^9} \times (3 \times 10^8) \simeq 0,06m \quad (2.13)$$

A atenuação pode ser analisada na figura 2.3, a qual apresenta o índice de atenuação em dB por metro para microondas a 2.4GHz e 5.7GHz.

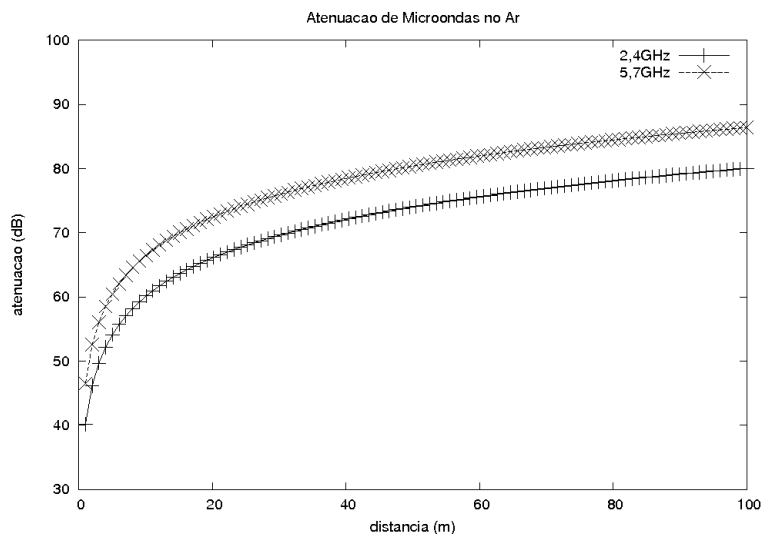


Figura 2.3: Atenuação por metro para 2.4GHz e 5.7GHz

Pode-se então concluir, utilizando a equação 2.4, que o sinal transmitido por uma placa IEEE 802.11 operando a 2,4 GHz, será recebido com a potência definida na fórmula 2.14 e 2.15:

$$R = ERP - FSPL + G_{AR} - A_{CaboR} \quad (2.14)$$

onde  $R$  é a potência do sinal recebido na placa de rede de recepção em dB,  $FSPL$  a atenuação no espaço em dB,  $G_{AR}$  o ganho da antena do receptor em dBi, e  $A_{CaboR}$  a atenuação em dB sofrida no cabo entre a antena e a placa do receptor.

Para ilustrar esta situação, considerando:

$$R = P_t - A_{CaboT} + G_{AT} - 20 \log\left(\frac{4\pi d}{\lambda}\right) + G_{AR} - A_{CaboR} \quad (2.15)$$

- uma placa capaz de enviar sinais com aproximadamente 17 dBm;
- utilização de 10m de cabo padrão RG213, que causa uma atenuação de 0,6 dB por metro, totalizando 6 dB;

- utilização de uma antena direcional com ganho de 24 dBi;
- enlace ponto a ponto, com 10 Km de distância entre um ponto e outro, o que ocasiona uma atenuação de aproximadamente 120dB;
- utilização de uma antena direcional com ganho de 24 dBi no receptor;
- utilização de 10m de cabo RG213 no receptor, com atenuação de 0,6 dB por metro, totalizando 6 dB.

Têm-se então que o sinal recebido pela placa de rede destino será de:

$$R = 17dBm - 6dB + 24dBi - 120dB + 24dBi - 6dB = -67dB \quad (2.16)$$

A equação 2.16, não leva em consideração nenhuma outra interferência além da atenuação. Salienta-se que em uma transmissão real, deve-se adicionar uma margem de atenuação de acordo com o nível de ruído entre os pontos de transmissão e recepção.

A diferença entre a potência de recepção  $R$  e a potência do ruído no meio de comunicação definem a relação sinal/ruído SNR (*Signal Noise Rate*). O valor do SNR define a qualidade do sinal recebido, permitindo que o nível físico das placas de transmissão e recepção definam o tipo de modulação e espalhamento espectral a ser utilizado (conseqüentemente definem a capacidade de bits por segundo da comunicação).

Além da atenuação causada pelo meio de propagação, quando um sinal de microondas encontrar um obstáculo, poderá também sofrer diferentes graus de atenuação. A atenuação causada por alguns tipos de obstáculos pode ser obtida através da tabela 2.1.

Tabela 2.1: Atenuação de Obstáculos para ondas de 2,4 GHz (3COM, 2005)

Obstáculo	Atenuação
parede de madeira sólida	6 dB
divisória de escritório com janela de vidro	4 dB
porta corta-fogo 25"	19 dB
tijolo 3,5"	6 dB
parede de concreto 18"	18 dB
divisória de vidro 0,5"	12 dB
corpo humano	3 dB

Na figura 2.4 nota-se o comportamento da atenuação de um sinal de microondas de 2,4 GHz ao encontrar uma parede com índice de atenuação de 6 dB à 40m do transmissor.

### 2.2.2 Reflexão

Sempre que um sinal de microondas encontra um obstáculo com superfície reflexiva (normalmente metal ou água), será refletido, não sendo capaz de atravessá-lo (ANDERSON, 2006), (FETTE et al., 2008). O ângulo de reflexão depende do ângulo do sinal ao incidir na superfície (sendo que o ângulo de incidência será sempre igual ao ângulo de reflexão em relação à normal  $N$ ). A figura 2.5 representa uma situação de reflexão de um sinal.

A ocorrência de reflexões podem ocasionar na criação de multi-caminho, ou seja, o receptor irá receber o mesmo sinal pelo caminho direto entre as antenas e, de forma

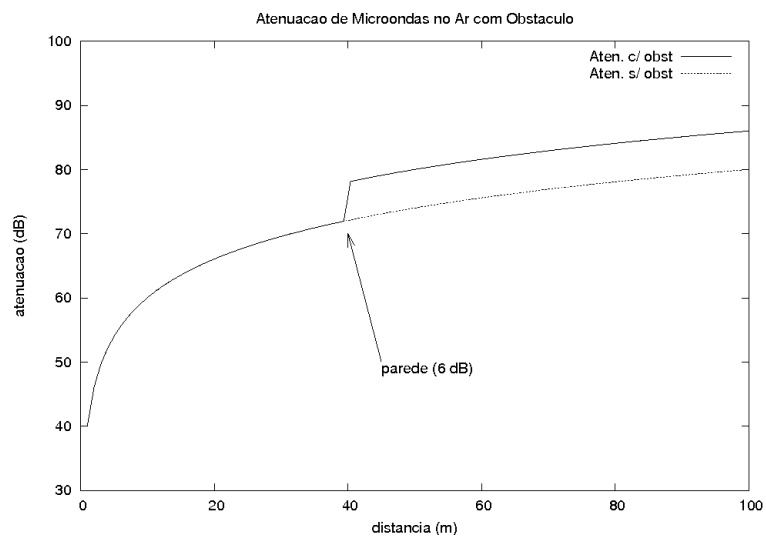


Figura 2.4: Atenuação com Obstáculo

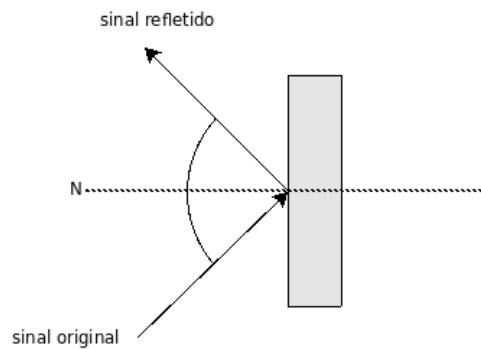


Figura 2.5: Reflexão do Sinal

defasada, o sinal que sofreu reflexão em um obstáculo. Isto significa que um único sinal transmitido pode ocasionar interferência nele próprio.

A reflexão também é utilizada para a criação de antenas direcionais e setoriais. Todas as antenas são compostas por um material condutor capaz de criar ondas eletromagnéticas omnidirecionais. Para que se possa concentrar esta onda de maneira direcional, são utilizados materiais reflexivos, conforme a figura 2.6.

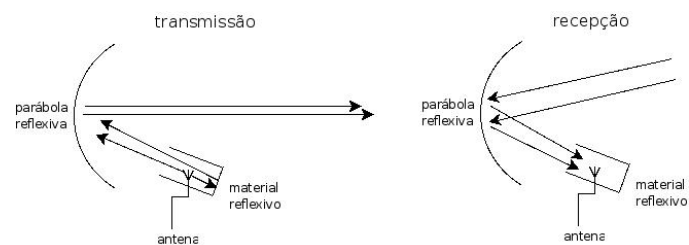


Figura 2.6: Reflexão do Sinal em Antenas Direcionais

O mesmo processo é utilizado para que se consiga ângulos de abrangência diferenciados nas antenas setoriais, porém neste caso, o material reflexivo é especialmente confeccionado em ângulos de ação específicos.

### 2.2.3 Refração

Quando o sinal passa de um meio físico com uma determinada densidade para outro meio com densidade diferente ao qual está, sofre alteração na sua direção. Isto significa que assim como na reflexão, podem existir interferências entre o sinal que sofreu refração e o sinal que não a sofreu (OPPENHEIMER; BARDWELL, 2002). A alteração da direção depende do material existente no meio original do sinal e do material no novo meio de propagação. Este fenômeno está representado na figura 2.7.

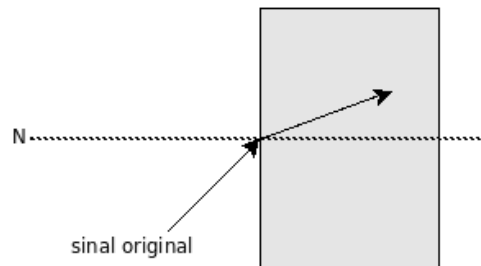


Figura 2.7: Refração do Sinal

### 2.2.4 Difração

A difração é um fenômeno de propagação que permite a comunicação de sinais de rádio frequência entre dois pontos, mesmo sem visada direta (a visada direta é identificada pela inexistência de obstáculos entre as antenas). É também a difração que preenche os espaços entre os obstáculos em um ambiente interno (FETTE et al., 2008).

A difração ocorre em consequência da formação das ondas durante a propagação dos sinais de rádio frequência. Cada ponto de uma onda é a fonte de energia para a criação da onda subsequente. Conseqüentemente, quando um sinal de microondas encontra um obstáculo de tamanho superior ao tamanho de sua onda (tamanho de um período da onda), ele irá contornar este obstáculo, alterando a direção de sua propagação original. A energia que possibilita que o sinal se propague para a área de sombra (atrás do obstáculo) é proveniente das ondas que não o atingiram (FETTE et al., 2008). Na figura 2.8 nota-se que o ângulo de propagação do sinal é alterado devido ao tamanho do obstáculo.

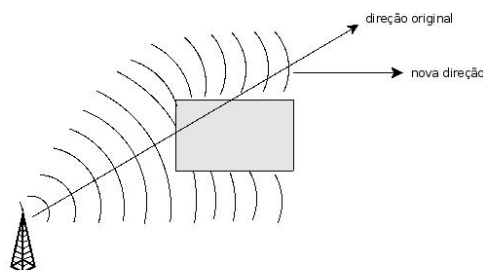


Figura 2.8: Difração do Sinal

### 2.2.5 Dispersão

Durante a propagação do sinal, caso encontre um obstáculo com a superfície irregular, o sinal de microondas pode sofrer reflexões em diversas direções, de acordo com esta



superfície. Este efeito é denominado dispersão e está relacionado com a profundidade das irregularidades na superfície (FETTE et al., 2008). A figura 2.9 representa esta situação.

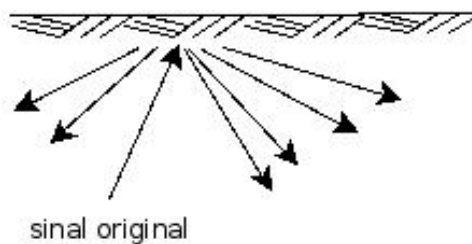


Figura 2.9: Dispersão do Sinal

### 2.2.6 Ruídos e Interferências

Em qualquer transmissão de dados existe um nível de ruído entre transmissor e receptor. O nível de ruído depende de diversos fatores como temperatura, meio de transmissão, qualidade de conectores, entre outros. Existem dois tipos de ruídos: ruídos brancos e ruídos impulsivos.

O ruído branco caracteriza-se pela alta frequência e baixa amplitude. Está sempre presente em qualquer comunicação e não pode ser eliminado do meio. O sucesso de uma comunicação depende da relação entre a potência (amplitude) do sinal transmitido e do ruído existente no meio.

O ruído impulsivo possui frequência e amplitude variadas. Este tipo de ruído ocorre devido a interferências externas como raios ou fontes eletromagnéticas de alta potência. Não pode ser previsto e normalmente acarreta na destruição do sinal transmitido.

Em redes WLAN, o nível de interferência suportado depende do tipo de espalhamento espectral e da modulação utilizada. Quanto menor for a diferença entre potência de sinal e ruído, menor será a capacidade de transmissão de dados do enlace.

## 2.3 Zona de Fresnel

Levando em consideração todas as interferências descritas anteriormente, é importante que seja definida a área de propagação das microondas em um enlace sem fios, na qual a existência de obstáculos irá interferir na comunicação. Esta área é denominada zona de fresnel.

A zona de fresnel é definida como uma elipsóide onde se encontram as áreas de propagação da antena de transmissão e recepção. A figura 2.10 representa as duas áreas de propagação e, entre as antenas, a zona de fresnel na qual o sinal será propagado.

Sempre que possível, deve-se manter a zona de fresnel livre de qualquer tipo de obstáculo, o que impede que as reflexões, refrações, difrações e dispersões ocorram. Sempre que a zona de fresnel estiver livre, as únicas alterações na transmissão serão a atenuação do sinal, e os ruídos existentes no ambiente.

Para que se possa identificar o raio da elipsóide em qualquer ponto entre as antenas, utiliza-se a fórmula 2.17 (SAYRE, 2001):

$$r = 17,3 \sqrt{\frac{D1 \times D2}{f \times d}} \quad (2.17)$$

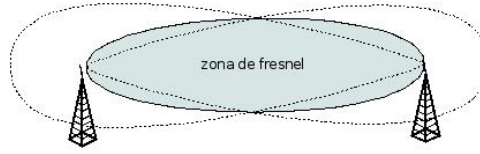


Figura 2.10: Zona de Fresnel

sendo  $r$  o raio da elipsóide no ponto medido em metros,  $D1$  a distância em quilômetros entre a primeira antena e o ponto a ser medido com a elipsóide do qual se deseja obter o raio,  $D2$  a distância entre o ponto a ser medido e a segunda antena em quilômetros,  $f$  a frequência da onda em GHz (2,45 GHz é utilizado para redes 802.11b e 802.11g) e  $d$  a distância total entre as duas antenas em metros. A distribuição do raio da zona de fresnel pode ser observada na figura 2.11.

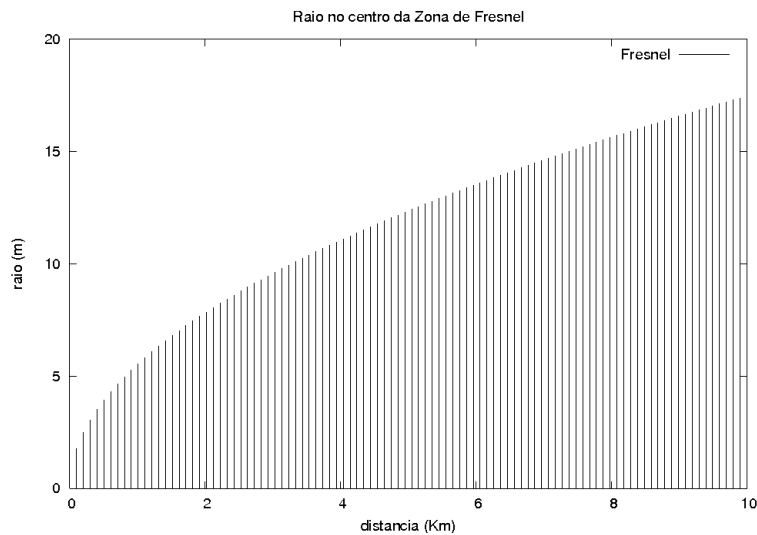


Figura 2.11: Raio no centro da zona de Fresnel

O cálculo da zona de fresnel é muito utilizado para definição da altura das torres que abrigarão as antenas em enlaces ponto-a-ponto. Ao obter-se o raio no centro da elipsóide, sabe-se qual a altura que as antenas devem ficar para que não exista interferência de obstáculos existentes entre elas. Conforme o tipo de obstáculo, até 20% da área da elipsóide pode estar ocupado sem comprometer o sinal (SAYRE, 2001).

### 3 REDES IEEE 802.11

O padrão IEEE 802.11 foi inicialmente definido em 1999 (IEEE, 1999a), como uma especificação de nível físico e de enlace do modelo OSI para redes locais sem fio WLAN. A figura 3.1 representa a posição do padrão IEEE 802.11 na arquitetura OSI.

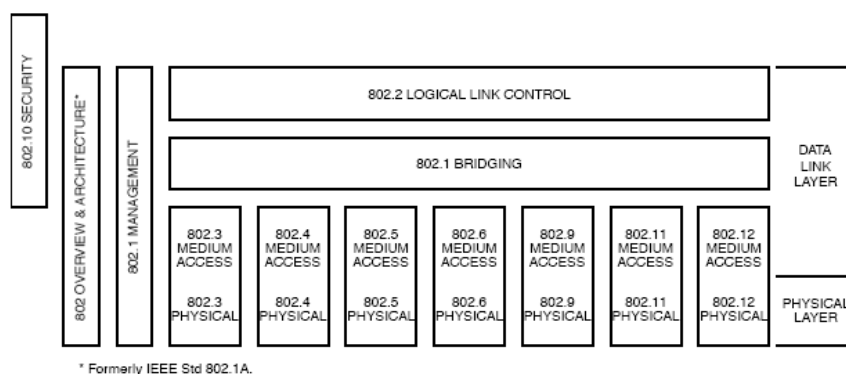


Figura 3.1: Padrão IEEE 802.11 no OSI (IEEE, 1999a)

A especificação do padrão define as características de controle de acesso ao meio, definição de quadros e controle de erros de enlace, além da forma de representação dos sinais para representação de dados no nível físico.

Até o presente momento, quatro padrões de nível físico foram definidos e estão descritos na tabela 3.1.

Tabela 3.1: Padrões de Nível Físico WLAN

Padrão	Freq. de operação	Taxa máxima de transm.	Espalhamento espectral
801.11	2,4 GHz	2 Mbps	FHSS / DSSS
802.11b	2,4 GHz	11 Mbps	HR-DSSS
802.11a	5,7 GHz	54 Mbps	OFDM
802.11g	2,4 GHz	54 Mbps	OFDM

A tabela 3.1 apresenta a evolução dos padrões físicos em ordem cronológica. Nota-se que as frequências utilizadas pelas redes WLAN são faixas ISM (*Industrial Scientific and Medical*), ou seja, sua utilização é livre, sem que seja necessária a obtenção de licenças junto aos órgãos governamentais. As faixas ISM são frequentemente utilizadas por diversos equipamentos eletrônicos, como forno de microondas, telefones sem fios, controles remotos de alarmes de carros, entre outros. A utilização destes equipamentos no mesmo ambiente acarreta em interferência mútua, ou seja, para que possam continuar operando

é necessário que a forma de sinalização do nível físico suporte o máximo possível as interferências.

A forma de garantir esta interoperabilidade é através da utilização de técnicas de espalhamento espectral, os quais permitem que dispositivos operando simultaneamente na mesma faixa de frequência "ignorem", dentro de certos limites, uns aos outros, como será descrito na seção 3.1.

### 3.1 Espalhamento Espectral

As técnicas de espalhamento espectral possuem como objetivo o aumento da robustez dos sinais transmitidos e a redução de interferências através da distribuição do sinal em uma grande faixa de frequências. Esta técnica permite, como já mencionado anteriormente, que diversos dispositivos operem na mesma faixa de frequência simultaneamente. A primeira técnica de espalhamento espectral foi patenteada no ano de 1942 pela atriz austríaca Hedy Lamarr e seu marido George Antheil. A idéia surgiu durante o casamento anterior de Lamarr com um comerciante de armas também austríaco, que comercializava armamentos para a Alemanha nazista. Durante esta época, ela tomou conhecimento dos esforços na criação de um mecanismo de controle remoto para torpedos que fosse resistente a tentativas de *jamming* (interferências na mesma faixa de frequência causada por inimigos). Lamarr teve a idéia de criar um mecanismo que fosse capaz de realizar a troca de frequência de maneira síncrona entre o torpedo e o controle remoto, em uma seqüência complexa o suficiente para não ser prevista pelo inimigo. Na época não existia nenhum mecanismo capaz de realizar tal sincronismo. Quando chegou nos Estados Unidos conheceu Geroge Antheil, um músico que criara um mecanismo capaz de sincronizar 16 pianos automaticamente. Ao unir sua idéia com a técnica de seu novo marido, foi criado o FHSS (*Frequency Hopping Spread Spectrum*) (GAST, 2002).

A técnica de FHSS deu origem, então, aos estudos em novas técnicas de espalhamento espectral, as quais são utilizadas atualmente em diversos equipamentos sem fios. As redes IEEE 802.11, conforme apresentado na tabela 3.1 utilizam diversas destas técnicas.

#### 3.1.1 FHSS - *Frequency Hopping Spread Spectrum*

Conforme descrito anteriormente, a técnica de FHSS diz respeito a alterações rápidas de frequência de maneira síncrona entre transmissor e receptor. Os saltos são pré-determinados e acarretam na divisão da informação transmitida em fatias de tempo. Nesta técnica de espalhamento espectral, a portadora é alterada em frequências pré-determinadas, fazendo com que a informação seja modulada em diferentes canais de frequência, um por vez (FETTE et al., 2008).

O FHSS é utilizado nas redes de nível físico padrão IEEE 802.11 e possuem as seguintes características (GAST, 2002):

- o canal principal é dividido em 95 microcanais de 1 MHz cada, sendo o primeiro canal 2,401 GHz, o segundo 2,402 GHz e assim por diante;
- cada canal é utilizado por um período de tempo de aproximadamente 0,4 segundos (denominado *dwel time*);
- a troca entre dois canais (o salto) não pode durar mais que 224 microssegundos;
- o ponto de acesso envia o padrão referente à seqüência de saltos sendo utilizada

nos quadros de *beacon* (os *beacon frames* são quadros especiais de anúncio de pontos de acesso para as estações);

- para a modulação dos dados, é utilizada GFSK - *Gaussian Frequency Shift Keying*.

A figura 3.2 apresenta uma representação da realização dos saltos de frequência realizados pelo FHSS.

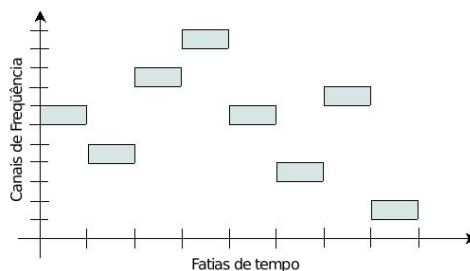


Figura 3.2: *Frequency Hopping Spread Spectrum*

Nesta técnica nota-se que caso exista interferência em apenas um dos canais de frequência, a informação transmitida não será totalmente perdida (apenas uma fatia de tempo é corrompida).

Operando com um *clock* de 1 MHz e realizando uma modulação de GFSK com 2 níveis, o 802.11 com FHSS obtém a taxa de transferência de 1 Mbps. Já com GFSK de 4 níveis, obtém a taxa de 2 Mbps. Ao utilizar o FHSS, é possível que duas ou mais redes operem simultaneamente sem interferência. Para isso, basta que utilizem canais de frequência diferentes no mesmo instante de tempo.

### 3.1.2 DSSS - *Direct Sequence Spread Spectrum*

Apresentado como uma evolução das técnicas de espalhamento espectral, o DSSS - *Direct Sequence Spread Spectrum* não realiza saltos de frequência, mas realiza a divisão da potência do sinal em uma grande faixa de frequência. A onda modulada terá sua amplitude distribuída no meio de acordo com a figura 3.3 (GAST, 2002).

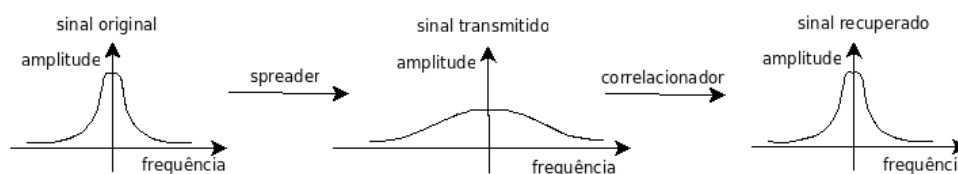


Figura 3.3: *Direct Sequence Spread Spectrum*

O receptor busca um sinal homogêneo em toda a faixa de frequência. Caso exista outro dispositivo não DSSS operando na mesma faixa de frequências, este irá identificar a transmissão DSSS como ruído (pois possui baixa amplitude). Já o equipamento DSSS irá ignorar a transmissão do outro equipamento por não se portar como uma transmissão DSSS (pois ocupa uma faixa de frequência menor)(GAST, 2002).

Para representação dos sinais, o DSSS utiliza informações denominadas *chips*. Um conjunto de 11 *chips* representam 1 bit. A seqüência de *chips* padrão para representação de bits em dispositivos 802.11 é denominada seqüência de Barker. A figura 3.4 apresenta esta seqüência.

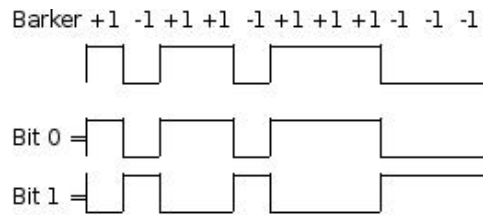


Figura 3.4: Seqüência de Barker

A seqüência de 11 *chips* representando um único bit permite que parte do sinal seja comprometida sem afetar a comunicação. Com um *clock* de 11 MHz, representando 11 *Mchips/s*, e utilizando modulação DPSK *Differential Phase Shift Keying* (2 fases discretas), obtém-se a taxa de transferência de 1 Mbps. Ao utilizar-se QPSK *Quadrature Phase Shift Keying* (4 fases discretas), obtém-se a taxa de 2 Mbps (GAST, 2002).

Para 1 Mbps, as alterações de fase são as descritas na tabela 3.2. Já para 2 Mbps, as alterações de fase são de acordo com a tabela 3.3

Tabela 3.2: DSSS com DPSK

Bit	Fase
0	0
1	$\pi$

Tabela 3.3: DSSS com QPSK

Bits	Fase
00	0
01	$\frac{\pi}{2}$
11	$\pi$
10	$\frac{3\pi}{2}$

Tanto a modulação FHSS, quanto a DSSS são definidas para utilização nas redes WLAN no padrão IEEE 802.11 original de 1997 (IEEE, 1999a).

### 3.1.3 HR-DSSS - *High-Rate DSSS*

O padrão IEEE 802.11b (IEEE, 1999b) define uma nova forma de espalhamento espectral para as redes WLAN. Com a adoção do HR-DSSS (*High-Rate DSSS*), as redes podem atingir as taxas de 1, 2, 5.5 ou 11 Mbps. Conforme a potência do sinal recebido e do ruído na comunicação, o espalhamento espectral é alterado para manter a comunicação. A compatibilidade com os dispositivos anteriores DSSS também foi mantida, ou seja, para 1 e 2 Mbps se utiliza DSSS e para 5.5 e 11 Mbps se utiliza HR-DSSS.

O HR-DSSS mantém a mesma estrutura de *chips* e *clock* de 11 MHz. Para atingir as taxas mais elevadas, o grupo de trabalho do IEEE optou pela utilização de um método de codificação alternativo à modulação simples de fase, o CCK (*Complementary Code Keying*).

O CCK divide o conjunto de *chips* em séries de 8 símbolos, capazes de representar 4 ou 8 bits por série. Com um *clock* de 11 MHz, ou seja 11 *Mchips/s*, e codificando 4 bits para cada 8 *chips*, têm-se a taxa de 5.5 Mbps. Ao codificar 8 bits em 8 *chips*, têm-se 11 Mbps (GAST, 2002).

A seção 3.1.3.1 descreve a obtenção da taxa de 5.5 Mbps com HR-DSSS e a seção 3.1.3.2 descreve como se obter a taxa de 11 Mbps.

### 3.1.3.1 HR-DSSS com 5.5 Mbps

Para se obter a taxa de 5.5 Mbps, o HR-DSSS divide a seqüência de bits a ser transmitida em blocos de 4 bits. Conforme a posição do bloco na seqüência, ele é classificado como *par* ou *ímpar* (o primeiro bloco é sempre considerado *par*). Cada bloco de 4 bits é subdividido em grupos de 2 bits. O primeiro grupo de 2 bits define o valor de uma variável  $i$ , conforme a tabela 3.4.

Tabela 3.4: Codificação da primeira dupla de bits  $b_0; b_1$

Bits $b_0$ e $b_1$	Valor de $i$ - bloco par	Valor de $i$ - bloco ímpar
00	0	$\pi$
01	$\frac{\pi}{2}$	$\frac{3\pi}{2}$
11	$\pi$	0
10	$\frac{3\pi}{2}$	$\frac{\pi}{2}$

Ou seja, se for um bloco *ímpar* e o valor dos dois primeiros bits for  $00$ , o valor de  $i$  passa a ser  $\pi$ . O segundo grupo de 2 bits, é utilizado para escolher um entre quatro conjuntos de 8 *chips*. Estes conjuntos utilizam o valor  $i$  definido anteriormente, conforme a tabela 3.5.

Tabela 3.5: Codificação da segunda dupla de bits  $b_2; b_3$  e *chips*  $c_0-c_7$  correspondentes

Bits $b_2$ e $b_3$	$c_0$	$c_1$	$c_2$	$c_3$	$c_4$	$c_5$	$c_6$	$c_7$
00	$i$	1	$i$	-1	$i$	1	- $i$	1
01	- $i$	-1	- $i$	1	1	1	- $i$	1
10	- $i$	1	- $i$	-1	- $i$	1	$i$	1
11	$i$	-1	$i$	1	- $i$	1	$i$	1

Com *clock* de 11M*chips/s*, transmitindo 4 bits em 8 *chips*, têm-se a capacidade de transmissão de 5.5 Mbps.

### 3.1.3.2 HR-DSSS com 11 Mbps

Para se obter a taxa de 11 Mbps, o conjunto de 8 *chips* deve representar 8 bits. Para isso, inicialmente a seqüência de bits a ser transmitida é dividida em blocos de 8 bits, também classificados como *par* ou *ímpar*. Cada bloco é subdividido em 4 grupos de 2 bits. O primeiro grupo de 2 bits é codificado de acordo com a tabela 3.4 já apresentada. Os outros grupos são codificados de acordo com a tabela 3.6 (IEEE, 1999b).

Tabela 3.6: Codificação dos bits (2,3) (4,5) (6,7)

Bits	codificação
00	0
01	$\frac{\pi}{2}$
10	$\pi$
11	$\frac{3\pi}{2}$

### 3.1.4 OFDM - *Orthogonal Frequency Division Multiplexing*

A técnica de OFDM foi incorporada nas redes WLAN no padrão IEEE 802.11a (IEEE, 1999c) e IEEE 802.11g (IEEE, 2003). É uma evolução da multiplexação por frequência FDM (*Frequency Division Multiplexing*) na qual diversos canais de frequência são criados para uma única comunicação. No OFDM, as informações são transmitidas em paralelo nos diversos canais. A figura 3.5 apresenta uma representação do FDM e OFDM.

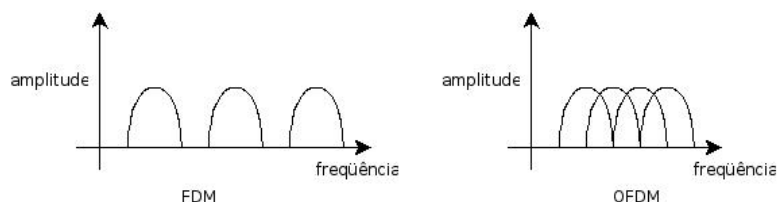


Figura 3.5: *Orthogonal Frequency Division Multiplexing*

O FDM utiliza uma banda de resguardo entre os canais para evitar que um canal cause interferências nos canais próximos. Esta banda de resguardo acarreta em desperdício de largura de banda. O OFDM, ao contrário, força os canais a ficarem sobrepostos, sem a banda de resguardo, porém evitando a interferência. Para que funcione, cada canal deve ser facilmente distinguido dos demais. Como é apresentado na figura 3.5, cada canal possui amplitude 0 no pico de amplitude dos canais vizinhos. E é justamente no pico de cada canal que é feita a transmissão dos dados, utilizando na transmissão a técnica de IFFT (*Inverse Fast Fourier Transform*), e na recepção, para recuperar os dados transmitidos, a FFT (*Fast Fourier Transform*) (GAST, 2002).

Nas redes IEEE 802.11a e IEEE 802.11g, é definido um canal de 20 MHz, o qual é dividido em 52 subcanais, sendo 48 para transmissão dos dados e 4 para controle de comunicação. Os dados modulados são divididos nestes canais e transmitidos em paralelo. Conforme a modulação realizada antes do espalhamento espectral, têm-se uma taxa de transmissão diferente. A tabela 3.7 apresenta as possíveis taxas de transmissão das redes IEEE 802.11a e IEEE 802.11g.

Tabela 3.7: Taxas de transmissão IEEE 802.11a e IEEE 802.11g (GAST, 2002)

Velocidade (Mbps)	Modulação	taxa de codificação	Bits por símbolo	Bits por subportadora	Bits de dados por subportadora
6	BPSK	$R=1/2$	1	48	24
9	BPSK	$R=3/4$	1	48	36
12	QPSK	$R=1/2$	2	96	48
18	QPSK	$R=3/4$	2	96	72
24	16-QAM	$R=1/2$	4	192	96
36	16-QAM	$R=3/4$	4	192	144
48	64-QAM	$R=2/3$	6	288	192
54	64-QAM	$R=3/4$	6	288	216

Observando a tabela, nota-se que para atingir a taxa de 54 Mbps, utiliza-se em cada sub-canal a modulação de 64-QAM, ou seja, codifica-se 6 bits por símbolo. Com 6 bits por símbolo em 48 sub-canais de dados, obtêm-se 288 bits por subportadora. Destes 288 bits, 216 são bits de dados, devido à taxa de codificação  $R = 3/4$ . A



taxa de sinalização nestas redes é de 250000 símbolos por segundo (BAUD), ou seja  $250000 \times 216 = 54Mbps$ .

## 3.2 Tipos de Enlace IEEE 802.11

As redes WLAN operam em diferentes arquiteturas de enlace. Estas arquiteturas dizem respeito à forma com a qual os dispositivos móveis irão trocar informações, sendo definidas arquiteturas: *Ad-Hoc* ou IBSS (*Independent Basic Service Set*), BSS (*Basic Service Set*), ESS (*Extended Service Set*) e uma arquitetura não definida nos padrões da IEEE denominada MANET (*Mobile Ad-hoc Network*). Estas arquiteturas serão descritas nas seções a seguir.

### 3.2.1 Arquitetura Ad-Hoc

As redes *Ad-Hoc* são redes formadas apenas por estações móveis que se comunicam diretamente, sem a existência de um elemento de comunicação central. Para que exista a comunicação entre um par de estações é necessário que ambas estejam na área de abrangência uma da outra. A comunicação sempre ocorre de maneira direta. A figura 3.6 apresenta um exemplo deste tipo de arquitetura de enlace.

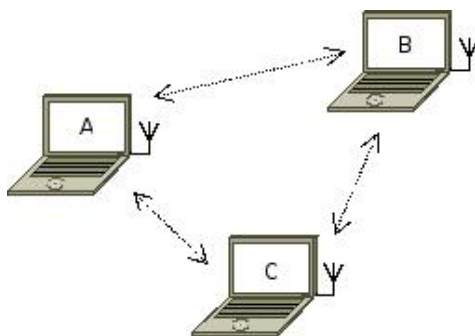


Figura 3.6: Enlace *Ad-Hoc*

### 3.2.2 Arquitetura BSS - *Basic Service Set*

As redes BSS são redes que possuem um elemento central de comunicação denominado ponto de acesso ou AP (*Access Point*). Para que exista a comunicação neste tipo de enlace, a estação móvel envia os dados ao AP que os retransmite para a estação destino. Todas as estações devem estar dentro da área de abrangência do AP, sendo que toda comunicação dos dados é interceptada por todos os clientes, de maneira semelhante ao modo de operação de um concentrador (*hub*) em uma rede cabeada.

Os APs também permitem a interligação entre a rede sem fios e uma rede com fios. Neste caso, o ponto de acesso opera como uma *bridge* entre as duas redes, ou como um roteador (dependendo do modelo do AP). No modo *bridge*, o AP possui uma tabela de endereços MAC associada a cada uma das suas interfaces de rede. Todas as estações com ou sem fio encontram-se no mesmo enlace lógico (mesma sub-rede). Em modo roteador, são criadas duas sub-redes, uma do enlace com fios e outra do enlace sem fios.

A figura 3.7 possui uma representação de rede BSS.

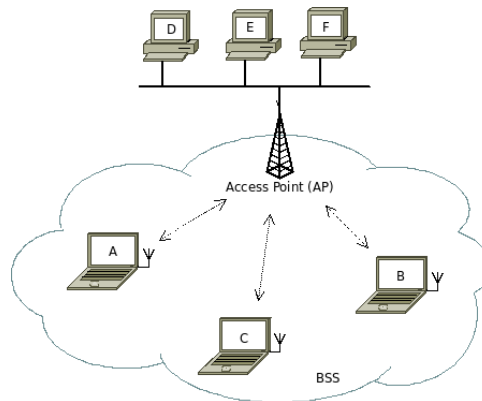


Figura 3.7: Enlace BSS

### 3.2.3 Arquitetura ESS - *Extended Service Set*

As redes ESS são formadas por um conjunto de redes BSSs, onde os pontos de acesso compartilham informações através de um protocolo WDS (*Wireless Distribution System*). O objetivo deste tipo de rede é o de que as estações móveis possam trocar de ponto de acesso sem perder a conexão com a rede. Forma-se então um conjunto de células de abrangência da rede, cada qual com seu ponto de acesso, e as estações ficam com a mobilidade garantida entre as células (realização de *handoff*). A figura 3.8 representa uma rede ESS formada por duas BSSs.

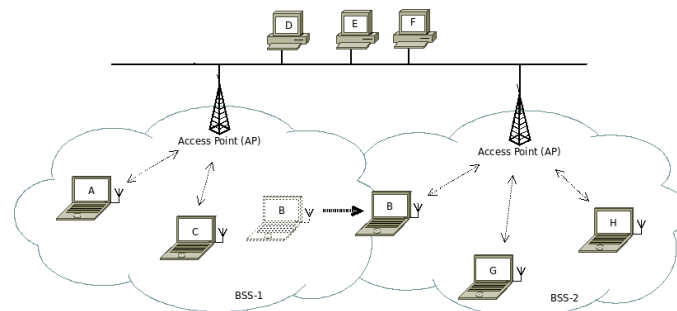


Figura 3.8: Enlace ESS

### 3.2.4 Redes MANET - *Mobile Ad-Hoc Networks*

As redes MANET são um tipo especial de rede Ad-Hoc. Nestas redes, cada nodo pode ser utilizado como intermediário de uma comunicação, ou seja, se um nodo *C* não está na área de abrangência de um nodo *A*, o nodo *B* pode ser utilizado como intermediário, desde que *A* e *C* estejam em sua área de abrangência. A figura 3.9 representa esta situação.



Figura 3.9: Enlace MANET

As redes MANET não são especificadas no padrão IEEE 802.11, portanto para que seja possível a criação deste tipo de enlace, é necessário a adição de um mecanismo de

roteamento específico para este fim. O protocolo OLSR (*Optimized Link State Routing Protocol*) é um exemplo de protocolo para implementação de redes MANET. Este protocolo realiza a troca de informações de nodos vizinhos periodicamente, em busca da melhor rota para qualquer destino na rede. Com este procedimento é montada uma tabela do tipo vetor-distância de rotas (OLSR.ORG, 2004).

A utilização deste tipo de rede é adequada em situações onde não existe a possibilidade de utilização de um AP, e as estações encontram-se distribuídas de maneira a não possuírem abrangência mútua.

### 3.3 Controle de Acesso ao Meio

Um enlace 802.11 tem suas funções baseadas no padrão 802.3 (ethernet). Semelhante às redes ethernet, existe a forma de endereçamento de dispositivos de rede através de um endereço MAC compatível com ambos os protocolos. Também pode-se utilizar como controle de acesso ao meio a técnica de CSMA (*Carrier Sense Multiple Access*).

Ao se utilizar a técnica de CSMA, os dispositivos que desejam transmitir realizam a leitura do meio de comunicação para certificarem-se de que não existe nenhuma comunicação já em andamento (com o objetivo de evitar colisões com estas transmissões). Caso o meio esteja livre, a estação inicia a transmissão.

Nas redes ethernet utiliza-se o CSMA/CD (*CSMA with Collision Detection*), no qual durante o processo de transmissão a estação continua lendo o meio. Caso o sinal recebido seja diferente do sinal sendo transmitido, é identificada uma colisão. Neste tipo de rede as colisões ocorrem apenas quando duas estações identificam o meio livre e iniciam a transmissão concomitantemente.

O CSMA/CD é eficiente em redes ethernet e permite que seja garantida a detecção de colisões durante a transmissão de dados. Com isto, nestas redes o envio de quadros de reconhecimento (ACK - *Acknowledgement*) torna-se dispensável. Em um ambiente sem fios, entretanto, a leitura do meio de comunicação e não detecção de transmissão de dados, não garante a inexistência de uma transmissão em curso. A situação de "nodos escondidos", por exemplo, acarreta em possíveis colisões não detectáveis via CSMA/CD.

Além disso, a não garantia de entrega de quadros de enlace devido aos problemas de propagação de microondas já apresentados neste documento torna imprescindível o envio de quadros de reconhecimento ACK para a garantia de entrega correta dos dados transmitidos. A figura 3.10 apresenta uma situação de colisão não detectável pelo CSMA ou CSMA/CD em um ambiente sem fios.

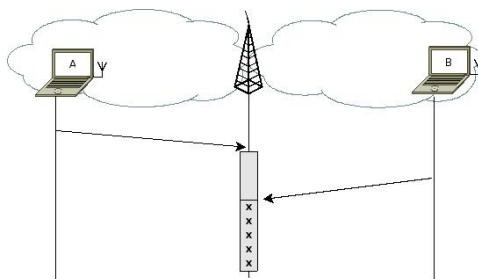


Figura 3.10: Nó Escondido Com CSMA ou CSMA/CD

Na figura 3.10 a estação A possui capacidade de transmissão e recepção de dados com o AP, assim como a estação B. A não possui capacidade de detectar sinais provenientes

de *B* (está fora de sua área de abrangência). Conseqüentemente, *A* não identifica transmissões de *B* e vice-versa. A comunicação entre *A* e *B* é possível pois ambas as estações estão na área de abrangência do AP.

A estação *A* acessa o meio de comunicação (não identifica nenhuma transmissão em andamento) e transmite seu quadro. Durante a transmissão, a estação *B* acessa o meio e não identifica a transmissão de *A* em andamento, pois está fora da área de abrangência da transmissão de *A*. *B* inicia a sua transmissão colidindo com a transmissão de *A*. O AP identifica a colisão, porém as estações não. Como nenhuma estação receberá confirmação de envio (ACK) irão retransmitir os quadros.

Este tipo de situação tem maior probabilidade de ocorrência quanto maior for o tamanho dos quadros transmitidos. Para minimizar as colisões, as redes sem fios utilizam como protocolos de acesso ao meio o CSMA para quadros considerados pequenos pelo administrador, ou CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) para quadros maiores, evitando as colisões nestes quadros.

O protocolo CSMA/CA define os seguintes procedimentos:

1. a estação verifica se existe alguma transmissão ocorrendo;
2. caso o meio esteja livre, a estação envia um quadro de RTS (*Request to Send*) para o ponto de acesso contendo o valor de NAV (*Network Allocation Vector*), o qual define o tempo necessário para que o quadro de dados seja enviado;
3. o AP envia um quadro de CTS (*Clear to Send*) contendo o NAV atualizado;
4. as estações na área de abrangência do AP que não identificaram o RTS, identificam o CTS e o valor de NAV, ou seja, identificam que não podem iniciar nenhuma transmissão pelo período de tempo definido no NAV;
5. a estação transmite o quadro de dados;
6. o AP envia o quadro de confirmação de recebimento sem erros ACK;
7. as estações retornam ao estado de disputa do meio de comunicação.

A figura 3.11 representa a troca de quadros durante a utilização do CSMA/CA.

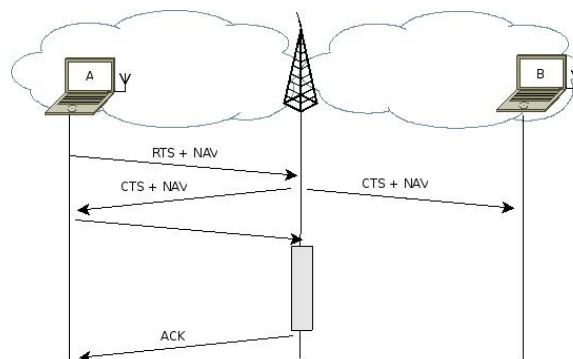


Figura 3.11: Protocolo CSMA/CA

Nota-se que o processo necessário para o CSMA/CA possui um peso (*overhead*) no desempenho da transmissão de dados na rede superior ao CSMA e que apresenta uma solução para uma situação específica (porém importante) de distribuição de nodos na

rede. Devido ao peso extra, os APs possuem em sua configuração a possibilidade de se ativar o CSMA/CA para pacotes com tamanho superior a um limite especificado pelo administrador. Para a transmissão de pacotes menores que o limiar definido, se utiliza o CSMA com probabilidade de colisões baixa. Para pacotes maiores que o limiar, utiliza-se o CSMA/CA e se mantém a estabilidade da rede.

Caso identifique-se a ocorrência de um número elevado de colisões na rede, o administrador deve diminuir o valor do limiar, forçando o uso do CSMA/CA para quadros menores.

### 3.4 Mecanismos de Segurança IEEE 802.11

As redes sem fios abrangem os níveis físico e de enlace de dados. Isto significa que todos os protocolos de níveis superiores que foram desenvolvidos anteriormente ao padrão IEEE 802.11 consideravam as características de segurança de um enlace com fios permanecem inalterados. Foi necessário então que se garantisse alguns aspectos de confidencialidade de dados e autenticidade de estações, sem sobrecarregar o dispositivo de rede. Ainda, a aplicação dos dispositivos sem fios estende-se a aparelhos móveis de baixa capacidade de processamento e que utilizam baterias, ou seja, a aplicação de protocolos criptográficos complexos acarreta numa sobrecarga neste tipo de equipamento.

Para que se possa manter os níveis superiores sem alterações e garantir a segurança da comunicação é necessário que exista:

1. a garantia do acesso aos dados da rede somente às estações associadas através de criptografia de dados;
2. a garantia de autenticidade das estações associadas à rede através de protocolos de autenticação.

Para que uma estação sem fios possa conectar-se à rede, é necessário então que passe por dois processos iniciais: autenticação e associação.

No processo de autenticação, a estação comprova que possui os privilégios necessários para o acesso à rede. Enquanto a estação estiver realizando este processo, não terá capacidade de enviar quadros aos demais dispositivos da rede, e não receberá nenhum quadro que não seja relacionado à autenticação. A comunicação fica restrita entre a estação e o AP.

O processo de associação representa a conexão da estação à rede. Somente após esta etapa, a estação terá permissão de trocar dados com os demais dispositivos da rede. A figura 3.12 apresenta a máquina de estados de uma estação sem fios em relação ao acesso à rede. Nota-se que em qualquer momento, o AP pode desautenticar uma estação.

#### 3.4.1 Confidencialidade

As redes com fios garantem que as informações da rede só são acessíveis aos dispositivos conectados fisicamente aos equipamentos de rede. Quando se utiliza uma rede sem fios, os dados são propagados sem controle no ar, ou seja, qualquer equipamento que esteja dentro da área de propagação do sinal pode capturar os dados transmitidos. Ainda, as placas de rede sem fios possuem um modo de operação especial denominado "modo monitor", o qual permite que uma estação sem fios capture os dados de qualquer canal de frequência, mesmo não estando associado à rede, ou seja, sem a necessidade de passar por nenhum mecanismo de autenticação.

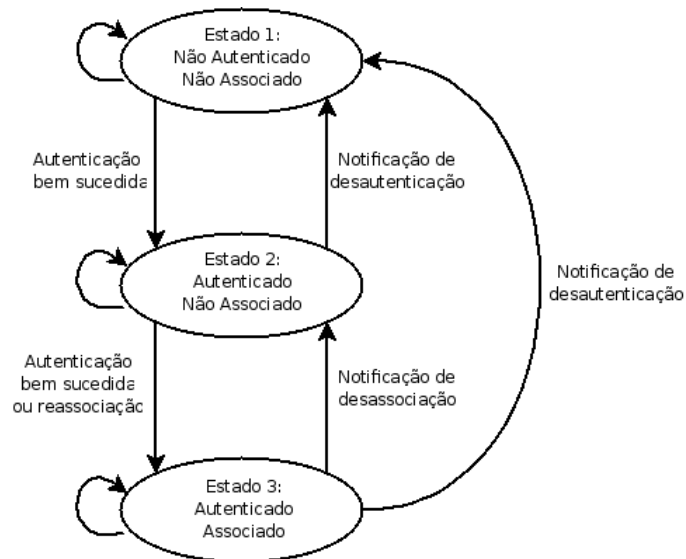


Figura 3.12: Possíveis estados de uma estação sem fio (IEEE, 1999a)

Para contornar este tipo de acesso, alguns protocolos criptográficos foram adotados desde a criação do primeiro padrão IEEE 802.11. O *Wired Equivalent Privacy* (WEP) foi o primeiro padrão, e posteriormente foi aperfeiçoado por um grupo de fabricantes através do novo protocolo WPA (*Wi-Fi Protected Access*). Ambos apresentam problemas de segurança, o que levou o grupo IEEE 802.11i a desenvolver um novo mecanismo denominado WPA-2.

#### 3.4.1.1 WEP

O WEP foi desenvolvido pelo IEEE já no primeiro padrão 802.11. É um mecanismo de confidencialidade de dados baseado no algoritmo criptográfico RC4. Assim como o RC4, o WEP é um protocolo criptográfico de chave simétrica, ou seja, existe uma única chave para cifrar e decifrar os dados e tanto a origem dos dados, quanto o destino devem conhecer esta chave. O algoritmo de cifragem é uma operação lógica XOR.

Como exemplo, caso deseje-se transmitir o byte 00011011 com a chave 01010101, têm-se:

$$00011011 \oplus 01010101 = 01001110$$

Ao analisar-se o resultado (que é o texto cifrado), nota-se que caso um atacante capture estes dados, não conseguirá identificar nem a chave utilizada, nem o texto original pois para cada bit do texto cifrado o atacante tem 50% de probabilidade para cada bit possível da chave ou do texto original. Por exemplo, analisando os dois últimos bits do texto cifrado: 10. O texto original e chave poderiam ser:

$$00 \oplus 10 = 10 \text{ ou } 01 \oplus 11 = 10 \text{ ou } 10 \oplus 00 = 10 \text{ ou } 11 \oplus 01 = 10$$

Desta forma, garante-se que o atacante não conseguirá obter o texto original, nem a chave de criptografia através da análise dos dados cifrados. Para realizar a decifragem, o destinatário dos dados, de posse da mesma chave criptográfica utilizada para a cifragem, realiza novamente a operação de XOR entre texto cifrado e a chave, obtendo o texto original.

$$01001110 \oplus 01010101 = 00011011$$

Nota-se que a chave a ser utilizada no processo de cifragem deve possuir o mesmo tamanho do texto a ser cifrado. Isto torna-se um problema na comunicação, tendo em vista

que todas as estações devem possuir esta mesma chave. A repetição da mesma chave não é adequada, pois caso o atacante insira dados na rede, ou obtenha o texto original de uma mensagem, poderá realizar a operação de XOR entre o texto original e o texto cifrado, resultando na chave criptográfica, pois:

$$01001110 \oplus 00011011 = 01010101$$

Se um atacante enviar qualquer dado para a rede (um comando ICMP, por exemplo) e capturar este dado cifrado, facilmente obtém a chave criptográfica utilizada naquele pacote.

Para evitar a necessidade de repetição da chave, o algoritmo criptográfico RC4 utiliza-se de um gerador de números pseudo-aleatórios PRNG (*Pseudo Random Number Generator*), o qual, a partir de uma semente, gera uma seqüência de números pseudo-aleatórios de qualquer tamanho. O RC4 possui também um verificador de integridade de dados ICV (*Integrity Check Value*), utilizando o cálculo de CRC-32. Este valor garante que a integridade dos dados trafegados não foi violada.

Desta forma, basta que as estações possuam a mesma semente para o PRNG e criem uma chave do tamanho dos dados a serem enviados. A pseudo-randomicidade é explicada pelo fato que a mesma semente gera sempre a mesma seqüência de números. O funcionamento da cifragem de dados no protocolo RC4 é apresentado na figura 3.13 e a decifragem na figura 3.14.

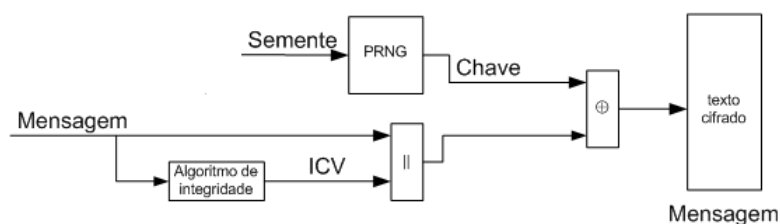


Figura 3.13: Funcionamento da Cifragem no Protocolo RC4

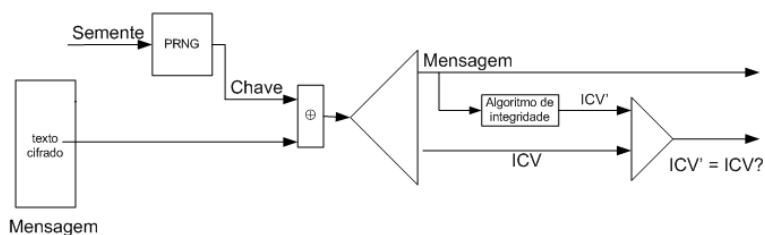


Figura 3.14: Funcionamento da Decifragem Protocolo RC4

O RC4 é um protocolo de criptografia de fluxo, ou seja, a chave de criptografia é gerada enquanto os dados são transmitidos. Este tipo de algoritmo possui um alto desempenho e flexibilidade. Porém, ao utilizar este mecanismo no nível de enlace têm-se um problema de sincronismo entre transmissor e receptor que acabou forçando o IEEE a alterar características do RC4 e criar o WEP. O nível de enlace das redes 802.11 não realiza controle de seqüência dos quadros transmitidos. Isto significa que ao utilizar-se o RC4 no nível de enlace, criando-se uma chave única para todos os dados, a perda de um quadro de enlace ocasiona a tentativa de decifragem do quadro subsequente com a porção errada da chave, destruindo completamente o sincronismo e comunicação entre as estações. Já foi

apresentado neste documento os diversos problemas existentes na comunicação sem fios, e nota-se que a perda de um quadro de enlace é um evento bastante provável (inclusive gerando a necessidade de confirmação ACK para cada quadro enviado). A figura 3.15 representa o problema de quebra de sincronismo no caso de perda de um único quadro, utilizando o RC4 como algoritmo.

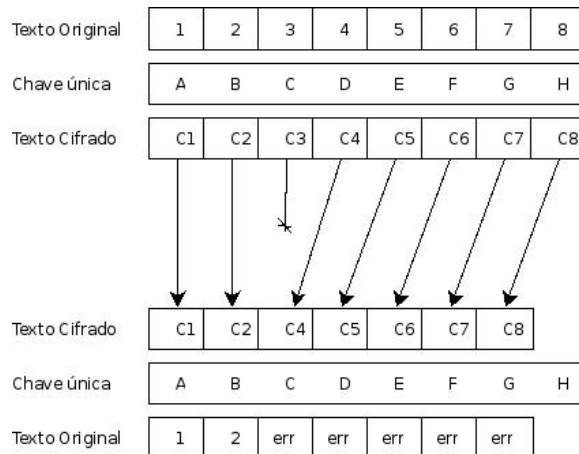


Figura 3.15: Problema de Sincronismo em Transmissões Wireless

Para contornar o problema de sincronismo e ao mesmo tempo não utilizar a mesma chave em todos os quadros de enlace, o WEP deve trocar de chave sempre que for transmitir um quadro. Também deve existir algum mecanismo capaz de garantir que tanto o transmissor, quanto o receptor utilizem a mesma semente para o PRNG.

A solução encontrada foi a criação de um vetor de inicialização IV (*Initialization Vector*), contendo 24 bits e que, concatenado com um segredo compartilhado, formam a semente do PRNG. O IV deve ser trocado a cada quadro transmitido e enviado ao receptor sem criptografia. O processo de cifragem do protocolo WEP é representado na figura 3.16, e a decifragem na figura 3.17.

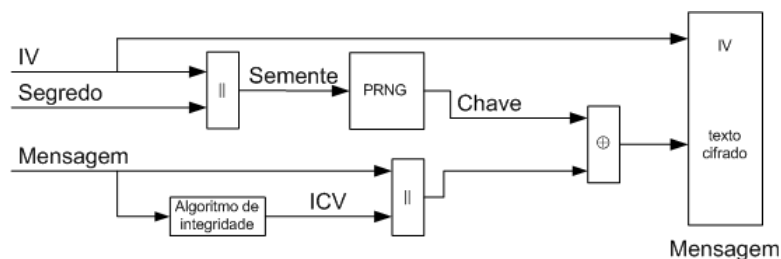


Figura 3.16: Funcionamento da Cifragem no Protocolo WEP

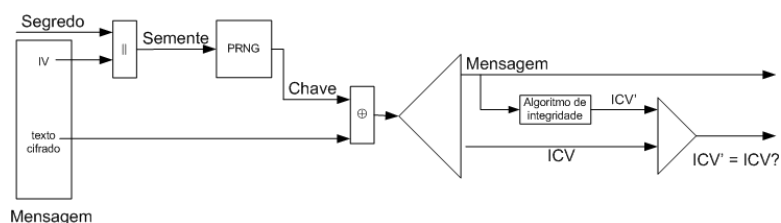


Figura 3.17: Funcionamento da Decifragem no Protocolo WEP



A cada transmissão de um quadro um novo IV é gerado aleatoriamente e enviado para o destinatário. Caso um atacante capture o tráfego, irá identificar o IV, porém não terá o segredo compartilhado entre as estações.

O padrão IEEE 802.11 define dois tamanhos de chave sendo:

1. WEP64 - 24 bits de IV + 40 bits de segredo compartilhado;
2. WEP128 - 24 bits de IV + 104 bits de segredo compartilhado.

O WEP possui uma série de problemas pela inclusão do IV e a incapacidade de garantir a confidencialidade dos dados neste protocolo foi comprovada em (FLUHRER; MANTIN; SHAMIR, 2001). Neste artigo, os autores apresentam a possibilidade da obtenção da semente a partir da geração de chaves fracas no protocolo RC4. No caso do WEP, pelo fato da criação de uma chave para cada quadro de enlace, o problema de geração de chaves fracas é acentuado. Além disso, parte da semente já é entregue ao atacante através do IV.

Outro detalhe importante, é que todos os quadros de uma rede 802.11 possuem o primeiro byte definido pela camada de adaptação LLC (*Logical Link Control*), equivalente a: *10101010*. Ou seja, o atacante possui também a capacidade de obter o primeiro byte de cada chave gerada pelo PRNG.

O WEP pode ser quebrado através de ataques probabilísticos que foram otimizados em diversos programas específicos para isso (como o software *WEPCrack* e *Airsnort*). O atacante necessita capturar alguns milhares de pacotes e executar a análise via software para obter o segredo compartilhado.

#### 3.4.1.2 WPA *Wi-Fi Protected Access*

Após a descoberta das fragilidades do WEP, o IEEE iniciou as pesquisas na alteração do modelo de confidencialidade a ser utilizado nas redes 802.11. Foi criado então o grupo IEEE802.11i especificamente para tratar desta pesquisa.

Os fabricantes de equipamentos, organizados através da *Wi-Fi Alliance*, no entanto, decidiram buscar uma solução alternativa para ampliar a segurança nos dispositivos já comercializados. O resultado deste grupo de fabricantes foi a definição, no ano de 2003, do protocolo WPA (*Wi-Fi Protected Access*) (ALLIANCE, 2003). O objetivo deste mecanismo de segurança é o de manter a compatibilidade com o WEP, ampliando suas características de segurança.

A principal alteração no protocolo, foi a adição de um mecanismo de troca dinâmica de segredo compartilhado entre as estações, o TKIP (*Temporal Key Integrity Protocol*). O objetivo é o de substituir o segredo estático do WEP, por um segredo que dinamicamente é alterado pela rede. Isto significa que o mesmo algoritmo criptográfico baseado no RC4 continua sendo utilizado pelas estações.

Para que se consiga realizar esta mudança dinâmica de segredo, é necessário que o serviço de autenticação de estações realize a identificação de um dispositivo como legítimo, para que possa ser fornecido o segredo atualmente em uso. Duas alternativas são fornecidas para este mecanismo de autenticação: 802.1x/EAP, e PSK (*Pre-Shared Key*).

O 802.1x/EAP utiliza uma negociação entre a estação que deseja se autenticar e um servidor de autenticação (RADIUS), através de um protocolo EAP (*Extensible Authentication Protocol*). O 802.1x é um mecanismo de autenticação baseado em portas de acesso. Um servidor de acesso remoto RAS *Remote Access Server* realiza o controle de tipos de acesso entre a estação requisitante da autenticação e a rede. Inicialmente apenas

uma “porta” de comunicação entre o requisitante e o servidor de autenticação é liberada pelo RAS. Caso a autenticação seja garantida pelo servidor de autenticação, o RAS libera a porta de acesso à rede. Em ambientes sem fios, o AP é visto como o RAS, que permite inicialmente apenas a comunicação entre cliente e servidor de autenticação. Após a negociação da autenticação (que pode ser realizada através de certificados digitais, usuário/senha, *smart-card*, entre outros), o servidor de autenticação informa ao AP se o cliente pode ou não acessar a rede. Após a autenticação o segredo é repassado ao cliente, o qual pode acessar a rede a partir de então. A figura 3.18 representa um modelo de autenticação 802.1x

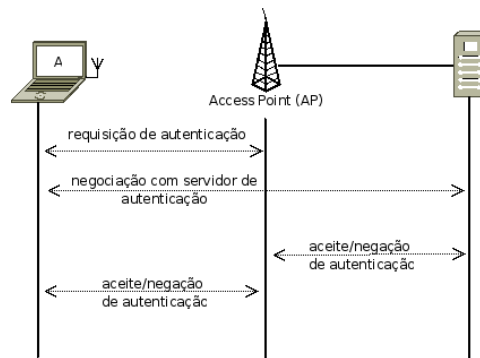


Figura 3.18: Autenticação 802.1x

O modelo de PSK tem por objetivo atender a demanda de ambientes sem servidor de autenticação (basicamente ambientes domésticos e de pequenas empresas). Neste modelo, um segredo “mestre” é inserido em todas as estações clientes e no AP. Este segredo é utilizado para o processo de autenticação e, após este processo, o segredo do TKIP é informado à estação cliente autenticada. O modelo PSK não é tão robusto quanto o 802.1x, principalmente devido à existência deste segredo pré compartilhado.

Mesmo com estas melhorias, no caso do PSK, se um atacante obtiver os quadros trocados durante o processo de autenticação, é possível que realize um ataque de dicionário (força bruta) em busca do segredo, como apresentado em (MOSKOWITZ; FLEISHMAN, 2003).

### 3.4.1.3 WPA-2 Wi-Fi Protected Access 2

No ano de 2004, o IEEE ratificou o padrão IEEE 802.11i (IEEE, 2004), o qual serviu como base para a padronização do WPA-2 (ALLIANCE, 2005).

O WPA-2 utiliza o algoritmo de criptografia AES (*Advanced Encryption Standard*) (NIST, 2001) no lugar do TKIP e WEP. Assim como o WPA, o WPA-2 permite o processo de autenticação via 802.1x/EAP ou PSK.

Ao contrário do WEP, o AES não realiza a cifragem de dados em fluxo, ou seja, conforme os dados são gerados, existe o processo de cifragem. O AES é um algoritmo de criptografia simétrico, que trabalha com blocos de dados. Os dados são cifrados em grupos de 128 bits independentes, com chaves de 128, 192 e 256 bits. No 802.11i, são utilizadas chaves de 128 bits.

O AES não possui nenhum ataque conhecido até a escrita deste trabalho, e as possíveis vulnerabilidades são consideradas especulações, não existindo nenhuma ferramenta capaz de realizar a quebra do algoritmo. Alguns trabalhos, como (SMITH, 2007) tentam apresentar possíveis fraquezas no AES, porém sem nenhum resultado prático.

### 3.4.2 Autenticidade

Em conjunto com os mecanismos de confidencialidade de dados em redes sem fios, é necessário que exista um processo de autenticação de estações na rede, capaz de comprovar que um determinado dispositivo ou usuário pode ter acesso à mesma. Nos primeiros padrões 802.11, dois mecanismos foram previstos: *Open System* e *Shared Key*. A partir da criação do WPA, foi adicionado um mecanismo adicional para autenticação através da utilização do protocolo 802.1x, já descrito na seção 3.4.1.2.

#### 3.4.2.1 *Open System*

A autenticação *Open System* baseia-se na troca simples de quadros de associação, sem necessidade de comprovação por parte da estação que deseja associar-se de identificação ou posse de privilégios especiais. É considerado como um processo de autenticação nulo, ou seja, não possui nenhum mecanismo de segurança.

A figura 3.19 possui uma descrição do processo de autenticação *Open System*.

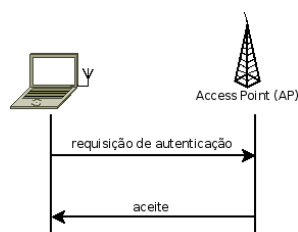


Figura 3.19: Autenticação *Open System*

#### 3.4.2.2 *Shared Key*

A autenticação *Shared Key* utiliza-se do algoritmo criptográfico WEP para realizar o processo de autenticação. Neste mecanismo, para que possa associar-se à rede, um cliente deve possuir conhecimento do segredo WEP compartilhado entre os dispositivos da rede.

Para comprovar que um cliente é autêntico, o ponto de acesso realiza um processo de desafio-resposta, ou seja, gera uma seqüência de bytes aleatórios e a envia para o cliente. O cliente deve, então comprovar que conhece o segredo cifrando esta seqüência de bytes e enviando o resultado para o ponto de acesso. O ponto de acesso pode, então, verificar se os bytes enviados foram cifrados com o segredo compartilhado, e comprovar a autenticação da estação. A figura 3.20 possui uma descrição do processo de autenticação *Shared Key*.

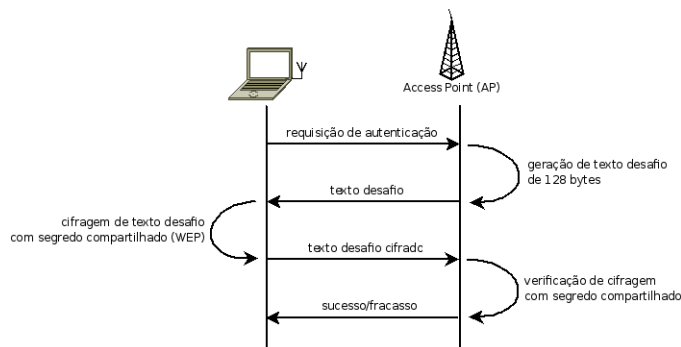


Figura 3.20: Autenticação *Shared Key*

### **3.4.3 *Manutenção da Confidencialidade e Autenticidade em Redes 802.11***

Têm-se então que atualmente é possível a configuração de uma rede 802.11 de forma a garantir a confidencialidade dos dados de forma considerada segura (até o presente momento) através da utilização do protocolo WPA-2.

O uso do algoritmo criptográfico AES pelo WPA-2 representa um avanço no nível de confidencialidade das redes sem fios, quando comparado com os demais algoritmos. As interfaces de redes comercializadas anteriormente à definição do padrão tornam-se, no entanto, incompatíveis com este novo mecanismo de segurança. Isto se deve à necessidade de alterações nos componentes das placas para que suportem a utilização do AES como algoritmo criptográfico.

Quanto à autenticidade das estações, o protocolo 802.1x permite que se utilize a verificação de dados de usuário, ao invés de garantir a autenticação apenas da estação. Este processo permite um maior controle sobre, por exemplo, o cancelamento de acesso a determinados usuários. Ao se utilizar o WEP, WPA/PSK e WPA-2/PSK, caso deseje-se cancelar o acesso de uma estação, é necessário que se realize a troca de segredo compartilhado em todas as demais estações.

Considera-se então que a utilização do conjunto de protocolos WPA-2 e 802.1x torna o controle de confidencialidade e de autenticação de usuários da rede adequados à grande maioria dos ambientes computacionais atuais. Resta então a complementação da segurança das redes com mecanismos adicionais, capazes de ampliar o nível de confiabilidade do uso das mesmas, e incrementar as possibilidades de controle sobre as estações móveis.

Neste aspecto, a possibilidade de localização da posição física das estações móveis permite a implementação de políticas de segurança de acesso baseadas nesta informação, contribuindo para a implementação de novas funcionalidades e controles para a rede.

## 4 ESTADO ATUAL NA LOCALIZAÇÃO DE ESTAÇÕES

Para que se possa localizar estações em um ambiente sem fios é necessário que existam pontos de referência conhecidos, e que se consiga obter informações de distância, potência de sinal ou ângulo entre estes pontos e a estação que se deseja localizar. Com a obtenção destas informações, é possível inferir a possível localização, com precisão que varia de acordo com a técnica utilizada. Existem dois modelos para que se possa realizar a localização de uma estação móvel (SAYED; TARIGHAT; KHAJEHNOURI, 2005):

- *Mobile Based* - onde o cliente (estação móvel) obtém sua localização através da obtenção de dados provenientes da infra-estrutura de rede (pontos de acesso que possuem a localização conhecida), e;
- *Network Based* - onde a infra-estrutura da rede (serviço de localização) obtém informações de distância de cada cliente e pontos de referência para que possa localizá-los.

Com a obtenção da distância entre o dispositivo móvel e pontos de referência, é possível realizar-se a triangulação das distâncias e obtenção da localização do dispositivo cliente, conforme a figura 4.1. As técnicas utilizadas para obter a distância normalmente são o Tempo de Recepção, Tempo de Vôo ou a Amplitude de Recepção de um sinal.

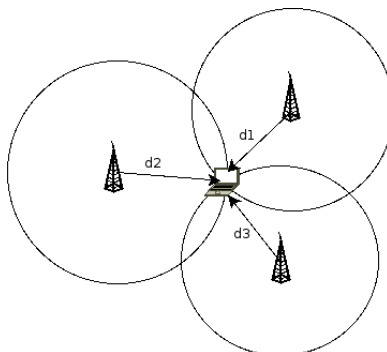


Figura 4.1: Triangulação de distâncias

Caso se utilize o ângulo de recepção, é possível inferir a posição apenas analisando a direção da recepção do sinal com maior potência. A técnica utilizada para obter o ângulo é a técnica de Ângulo de Recepção (SAYED; TARIGHAT; KHAJEHNOURI, 2005).

## 4.1 Localização por Análise de Tempo de Sinal

Existem duas técnicas para localização de dispositivos móveis utilizando o tempo de propagação dos sinais de radiofrequência: o Tempo de Recepção (ToA - *Time of Arrival*) e Tempo de Vôo (ToF - *Time of Flight*).

A técnica de tempo de recepção (ToA) utiliza o tempo gasto por um sinal/quadro desde sua transmissão até o recebimento. Tendo em vista a velocidade constante de propagação da microondas, é possível determinar-se a distância entre os dois pontos.

As microondas viajam à velocidades próximas da luz (aproximadamente 300.000 Km por segundo no vácuo), e para que o ToA funcione, é necessário que existe sincronização entre os relógios da estação móvel e do ponto de acesso, e que o mesmo possua precisão suficiente para que possa identificar diferenças de tempo/distância (a precisão necessária para o relógio irá depender do valor de erro permitido na localização que se deseja obter).

Ao transmitir um quadro, o transmissor anexa um carimbo de tempo, representando o momento da transmissão. Ao receber o quadro, o receptor verifica o tempo gasto pelo quadro para percorrer o caminho entre os dois pontos. Este tempo pode ser convertido, então, em distância (o mesmo princípio é utilizado para a localização de dispositivos através de sistemas de GPS - *Global Positioning System*).

Utilizando o tempo de vôo (ToF) de um sinal, é possível identificar a distância sem a necessidade de carimbos de tempo. Em (MORRISON, 2002), por exemplo, para descobrir a distância entre os pontos, é realizada a análise da latência entre o envio de um quadro de enlace e seu reconhecimento (ACK). Utilizando uma analogia ao sistema de localização utilizado em radares, o trabalho citado aproveita-se do protocolo de confirmação que ocorre a cada transferência de quadros de enlace para mensurar a distância.

Outros modelos, como (CAPKUN; HUBAUX, 2006), realizam a localização de estações através de ToF utilizando um protocolo a nível de aplicação, medindo o tempo do envio de informações pelo ponto de acesso, processamento pela estação móvel e resposta da estação para o ponto de acesso. Para que possa determinar a posição da estação, inicialmente é determinada a distância entre a estação e cada ponto de acesso. Com esta informação é realizada a triangulação das distâncias.

## 4.2 Localização por Análise de Ângulo de Sinal

A técnica de medida de ângulo de recepção (AoA - *Angle of Arrival*) requer um conjunto de antenas direcionais em cada ponto de acesso. O ponto de acesso, ao receber um sinal proveniente da estação móvel, determina qual das antenas recebe o sinal com a maior amplitude, e conseqüentemente consegue 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 a construção de duas linhas e é possível identificar a localização da estação através da intersecção destas, conforme apresentado na figura 4.2.

## 4.3 Localização por Análise de Amplitude de Sinal

A técnica de Amplitude de Recepção (AmpoA - *Amplitude of Arrival*) utiliza a amplitude do sinal recebido pela estação móvel para determinar a sua localização. Diversos sistemas utilizando esta técnica foram propostos, como (BAHL; BALACHANDRAN; PADMANABHAN, 2000), (KITASUKA; NAKANISHI; FUKUDA, 2003), (TAHERI;

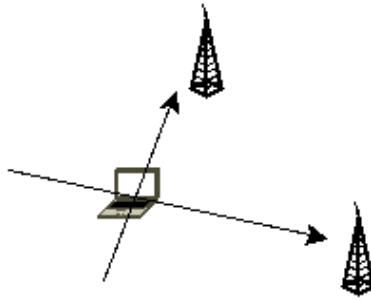


Figura 4.2: Exemplo de AoA.

SINGH; EMMANUEL, 2004) e (PANDEY et al., 2005).

Existem duas abordagens principais possíveis para que localize uma estação através da potência dos sinais entre a estação e o ponto de acesso: relação direta e *fingerprinting*. Sabe-se que devido à atenuação existente, quanto maior a distância entre uma estação e o ponto de acesso, menor será a potência do sinal recebido, e que é possível criar-se uma relação entre esta potência e a distância.

Na técnica de relação direta, utiliza-se a fórmula de FSPL (apresentada na seção 2.2.1, na fórmula 2.11) para identificar-se a distância, e realizar-se a triangulação. Neste modelo, no entanto, os obstáculos presentes no ambiente interferem diretamente na potência do sinal, e a precisão da localização depende diretamente deste fato.

Já utilizando *fingerprinting*, divide-se o ambiente em quadrantes, formando uma tabela. Para cada quadrante, é realizado um conjunto de medições de potência em relação aos pontos de acesso, criando-se uma referência de potência para cada ponto. Quando deseja-se localizar uma estação, basta que se verifique com qual potência ela está recebendo os sinais dos pontos de acesso (ou com qual potência o ponto de acesso está recebendo os sinais da estação) para que se consulte a tabela de amostras criadas e se determine o ponto mais próximo da estação no ambiente. Quanto maior a granularidade da tabela, maior será a precisão da localização.

As técnicas de tempo e ângulo adicionam uma maior complexidade aos mecanismos de localização de estações, quando comparados com a amplitude. A análise de tempo necessita de relógios precisos e sincronizados, ou de *hardware* específico para medição de tempos, especialmente ao se trabalhar em ambientes internos, onde a precisão da localização torna-se importante. A análise do ângulo necessita da adição de antenas direcionais nos pontos de acesso (cobrindo 360 graus), o que não é uma prática comum em soluções comerciais, e necessita de um sistema capaz de identificar para a mesma transmissão, qual antena recebe o sinal com maior potência.

Para que se consiga obter a localização utilizando-se os equipamentos comercialmente disponíveis sem alterações, o mecanismo proposto neste trabalho baseia-se na análise de amplitude. Existem algumas considerações que devem ser abordadas para seu uso em ambientes internos, as quais serão apresentadas na próxima seção.

#### 4.4 Localização em Ambientes Internos Utilizando Amplitude

Para que se possa criar uma relação direta entre a potência de recepção e a distância entre o ponto de acesso e a estação móvel, é necessária a existência de LOS (*Line Of Sight*), ou seja, é necessário que não existam obstáculos entre as antenas de transmissão e

recepção, respeitando a zona de fresnel (BARDWELL, 2003).

Os obstáculos causam alterações na direção e comportamento das microondas, refletindo estas alterações na potência recebida pelas estações. Da mesma forma, qualquer objeto dentro da zona de fresnel acarreta na perda de amplitude geral do sinal recebido.

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 espaço FSPL (fórmula 2.11).

Desta forma, quando o cliente identifica a potência de recepção do sinal proveniente de ponto de acesso pode utilizar as fórmulas 2.4 e 2.14. A partir da obtenção da potência de recepção  $R$ , a estação móvel pode descobrir a atenuação sofrida pelo sinal durante a transmissão, através da fórmula 4.1.

$$FSPL = ERP - R + G_{AR} - A_{CaboR} \quad (4.1)$$

Com a obtenção da FSPL, pode descobrir a distância percorrida pelo sinal, utilizando a fórmula 4.2.

$$FSPL = 20 \log\left(\frac{4\pi d}{\lambda}\right)$$

$$\frac{FSPL}{20} = \log\left(\frac{4\pi d}{\lambda}\right)$$

$$10^{\left(\frac{FSPL}{20}\right)} = \frac{4\pi d}{\lambda}$$

$$d = \frac{10^{\left(\frac{FSPL}{20}\right)}}{\left(\frac{4\pi}{\lambda}\right)}$$

$$d = \frac{10^{\left(\frac{FSPL}{20}\right)}\lambda}{4\pi} \quad (4.2)$$

Em comunicações sem fios NLOS (*Non Line Of Sight*), não existe linha de visada entre as antenas, ou seja, é necessário que além da distância, sejam considerados os obstáculos entre elas, e a conseqüente possibilidade de reflexão de sinal, refração, multi-caminho, atenuação e dispersão.

As implementações de Amplitude por *fingerprinting* realizam a construção de tabelas de amostragem justamente por estes problemas de propagação existentes em ambientes internos, pois qualquer alteração no comportamento da onda irá alterar a potência recebida pela estação móvel. Nesta técnica, por outro lado, não são considerados os obstáculos dinâmicos, ou alterações no ambiente que ocorram após a obtenção das amostras.

## 4.5 Trabalhos Correlatos

Diversos trabalhos relacionados com a localização de estações são encontrados na literatura. Todas as técnicas descritas nas seções anteriores possuem modelos e experimentos que validam a técnica e apresentam resultados. Como o trabalho aqui apresentado utiliza as técnicas de Amplitude, serão apresentados exemplos de trabalhos que a utilizam.



#### 4.5.1 Trabalhos em Amplitude

No modelo proposto em (BAHL; BALACHANDRAN; PADMANABHAN, 2000), assim como em (TAHERI; SINGH; EMMANUEL, 2004), é realizado um mapeamento em todo o perímetro físico que se pretende considerar na localização (técnica de *finger-printing*). 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. Nestes trabalhos considera-se na fase de calibragem (coleta de amostragens para construção da tabela de *finger-print*) todos os obstáculos presentes no ambiente. Isto significa que quando o sistema é colocado em produção, qualquer obstáculo que seja inserido (dinâmico ou não) não é considerado no modelo. A existência deste tipo de situação, onde obstáculos são incluídos no ambiente após a calibragem faz com que o sistema possua uma diminuição em sua precisão no momento da localização das estações.

Em (KITASUKA; NAKANISHI; FUKUDA, 2003), além de identificar a potência do sinal entre o cliente e os pontos de acesso, o cliente utiliza também a potência entre ele e seus vizinhos para refinar a localização (o serviço de localização consulta a posição dos vizinhos para realizar o refinamento). Já no modelo proposto por (PANDEY et al., 2005), a tabela de amostragens é criada através da utilização de diversos *sniffers* espalhados pelo ambiente físico. Estes *sniffers* capturam as informações de potência entre os pontos de acesso e os diversos clientes, construindo a tabela de amostragens sem a necessidade da equipe de infra-estrutura ter que realizar um mapeamento em quadrantes.

Em 2006, os autores de (MORAES; NUNES, 2006) realizam a localização das estações móveis também sem a necessidade da utilização de tabelas de *finger-print* ou fase de calibração. O processo é realizado baseando-se na utilização de estações *sniffer* sem fios, similar ao trabalho de (PANDEY et al., 2005). Estas estações utilizam interfaces sem fios 802.11 em modo monitor, capazes de capturar os pacotes dos clientes diretamente, sem a intervenção do AP. Ao mesmo tempo, os *sniffers* obtêm informações de potência do AP através da captura de pacotes do mesmo.

Os *sniffers* permanecem realizando a captura constantemente e a partir das informações de potência obtidas entre cada um destes equipamentos e cada AP, é construída uma tabela de *finger-print* atualizada. A atualização dinâmica da tabela de *finger-print* acaba por considerar os obstáculos existentes entre cada dupla AP/*sniffer* dinamicamente no processo de localização. A precisão deste modelo estabelece-se em um erro inferior ou igual a  $2m$  para 77% dos testes de localização realizados pelos autores (MORAES; NUNES, 2006).

Tanto o modelo proposto em (PANDEY et al., 2005), quanto em (MORAES; NUNES, 2006) adicionam a necessidade de estações monitoras distribuídas no ambiente. Estas estações não podem estar indisponíveis e as placas de rede em modo monitor não são capazes de associarem-se à rede. Força-se então a utilização de pelo menos duas placas de rede sem fios nestas estações, caso deseje-se utilizá-las na rede, além da administração e controle da disponibilidade das mesmas. Nota-se então o acréscimo da complexidade gerencial nestes modelos.

Outros modelos como (KRISHNAN et al., 2004) propõem a utilização de estações de baixo custo distribuídas no ambiente físico que transmitem sinais de rádio para as estações móveis. Estes sinais são utilizados como referência para a localização dos clientes. Novamente incrementa-se o ambiente sem fios com dispositivos extras para realizar a

localização.

Um exemplo de validação de construção da relação entre potência e distância é apresentado no trabalho de (FARIA, 2005). Neste trabalho, o autor apresenta um experimento prático na universidade de Stanford, comprovando a relação entre potência e distância. Para tal, é utilizada a fórmula de *Log-Distance Path Loss* (fórmula 4.3).

$$Pr(d) = Pr_{(0)} - 10\alpha \log(d) + X_{\sigma} \quad (4.3)$$

onde  $Pr(d)$  é a atenuação em função da distância  $d$ ,  $Pr_{(0)}$  é a atenuação em uma distância conhecida (geralmente 1m),  $\alpha$  representa um fator de atenuação dependendo do tipo de ambiente e  $X_{\sigma}$  uma variável probabilística com distribuição gaussiana e desvio padrão  $\sigma$ . Tanto  $\alpha$  quanto  $X_{\sigma}$  são dependentes do ambiente, de acordo com número e tipos de obstáculos. Em ambientes com poucos obstáculos, utiliza-se  $\alpha = 1,8$  e em ambientes muito obstruídos,  $\alpha = 5$ . O valor de  $\sigma$  normalmente varia no intervalo [4,12]dB.

A figura 4.3 demonstra os resultados obtidos por (FARIA, 2005) nas amostras realizadas, utilizando  $\alpha = 4,02$  em um ambiente interno na universidade de Stanford.

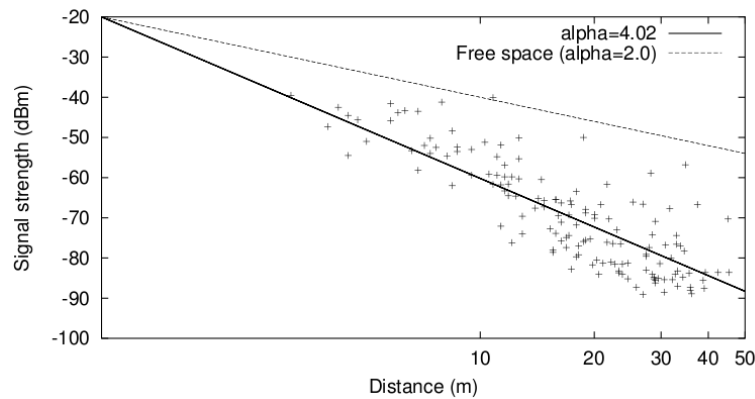


Figura 4.3: Resultados Obtidos em Ambiente Interno por (FARIA, 2005)

Ainda, foram realizadas amostragens no ambiente externo do prédio (tendo apenas a parede exterior como obstáculo) com  $\alpha = 3,32$ . Os resultados obtidos podem ser analisados na figura 4.4.

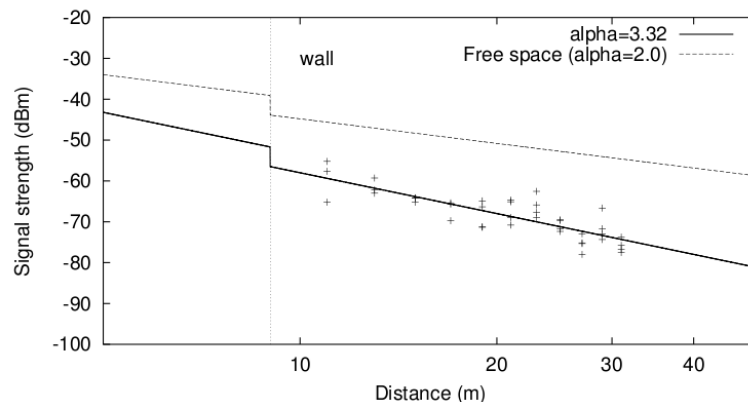


Figura 4.4: Resultados Obtidos em Ambiente Externo por (FARIA, 2005)

Nota-se na figura 4.4 a presença da parede externa a pouco menos de 10 metros do ponto de referência, causando atenuação no sinal.

A técnica tem sua precisão dependente da configuração adequada de  $\alpha$  e  $X_\sigma$ , e da homogeneidade de obstáculos do ambiente. Estes valores são responsáveis pela adequação da obtenção do valor da distância influenciada pelos diferentes obstáculos presentes.

Esta abordagem adota um valor de referência para descrever o impacto dos obstáculos em um ambiente. Desta feita, caso não se defina este valor com precisão, ou caso o volume (e índice de atenuação) de obstáculos varie, o sistema terá sua precisão prejudicada. Também deve-se considerar que este valor é único para todo o ambiente, mesmo existindo variações no índice de atenuação conforme a posição física que se deseja trabalhar.

O trabalho apresentado por (YASAR; ANSARI; FAROOQUI, 2006) refere-se diretamente aos problemas de localização de estações em ambientes *indoor*. Neste trabalho é utilizada a técnica de triangulação para definir a posição física da estação móvel.

A técnica de triangulação é baseada na identificação da potência de sinal dos clientes tendo como referência 3 servidores que constantemente monitoram esta informação para obter uma média do valor de potência (a média é necessária devido às constantes variações que o valor de potência de sinal sofre pelas interferências e multicaminho). Após a obtenção dos valores de média de potência em cada ponto de referência, é realizada a triangulação da posição da estação móvel. O método também utiliza uma base de dados de pontos conhecidos (contendo a posição dos servidores de monitoramento) para correlacionar os resultados da triangulação com esta tabela. Os autores identificaram uma média de erro de  $\pm 5m$  para a determinação do ponto de localização da estação.

Da mesma forma que os trabalhos em (PANDEY et al., 2005) e (MORAES; NUNES, 2006), são necessários servidores de monitoramento especificamente realizando a coleta de informações de clientes.

Para que se possa utilizar a potência de sinal, deve-se considerar os diversos aspectos entre os equipamentos utilizados, e no próprio ambiente, que interferem no valor de potência de sinal recebido. O trabalho (STOYANOVA et al., 2007) apresenta um estudo realizado com equipamentos sem fios, avaliando as variações de potência de acordo com a orientação (ângulo entre os equipamentos de transmissão/recepção) e na utilização de diferentes equipamento de mesmo fabricante e modelo (avaliando as diferenças na confecção dos equipamentos). Este trabalho também avalia as diferenças de propagação do sinal em ambientes de acordo com os obstáculos presentes em um ambiente externo (*outdoor*).

A localização da estação sem fios em (STOYANOVA et al., 2007) é feita em setores. Cada setor é delimitado por três APs, formando um triângulo. O objetivo do sistema é o de localizar em qual triângulo a estação se encontra. Para atingir este objetivo, o sistema mede os três APs com maior potência de sinal na estação móvel, identificando a sua localização.

Este trabalho identifica apenas o setor em que a estação móvel se encontra, não apresentando sua localização física. O trabalho baseia-se na localização de estações em um asilo de idosos (cada idoso possui um dispositivo móvel), sendo que em caso de acidentes, a identificação do setor no qual o idoso está é facilitada. Além disso, os setores utilizados nos testes são em uma área aberta (jardim do asilo, ou seja, *outdoor*) e só considera os obstáculos neste tipo de ambiente.

Técnicas de localização de estações baseadas em potência de sinal também são utilizadas em redes de sensores sem fios. O trabalho de (BUSCHMANN et al., 2007) utiliza a comparação de potência entre sensores vizinhos para estimar a localização de um sensor sem fios. Cada sensor possui uma listagem de todos os demais sensores aos quais recebe sinais com determinada potência. Quando se deseja localizar um determinado sensor,

compara-se a lista de sensores vizinhos com os demais. Um sensor estará próximo de outro quando ambos compartilham a maior parte de vizinhos. A distância é baseada no número de vizinhos em comum.

Neste caso, existe a necessidade da disponibilidade de equipamentos sem fios com posições fixas e conhecidas, além da possibilidade de comunicação direta entre os dispositivos móveis. Esta técnica é interessante para localização em redes *ad-hoc* ou MANET.

No trabalho apresentado por (KUWABARA; NISHIO, 2009), os autores realizam a construção dos mapas de potência a partir de poucas amostras no ambiente. Nesta pesquisa cada amostra é avaliada identificando a potência de sinal e distância da amostra. A partir destas informações o sistema proposto realiza a distribuição da potência entre o AP e a estação móvel na tabela. As variações de potência fornecem informações sobre os possíveis obstáculos presentes na área entre o AP e a estação, fazendo com que o sistema assuma a presença de obstáculos responsáveis por causar a atenuação do sinal.

O sistema opera a partir das seguintes etapas (KUWABARA; NISHIO, 2009):

1. Divisão da Área - a área de abrangência de cada AP é dividida em setores a partir do AP, e o ponto mais distante é utilizado para amostragem de potência de sinal;
2. Definição dos Obstáculos Hipotéticos - comparando-se a potência esperada em uma determinada estação (de acordo com a fórmula de FSPL) e o sinal efetivamente recebido, identifica-se a presença de obstáculos entre o AP e o ponto medido;
3. Cálculo da Curva de Atenuação - a partir das informações obtidas, cria-se a curva de atenuação para cada área. Assume-se que o obstáculo encontra-se no ponto médio entre o AP e o ponto medido;
4. Complementação do Mapa de Potência - o mapa de potência é atualizado de acordo com as informações obtidas nas etapas anteriores.

Nos testes realizados em (KUWABARA; NISHIO, 2009) a localização apresentou um erro médio de 18,65m. Além disso, não existe a identificação de obstáculos dinâmicos inseridos no ambiente após a fase de calibragem. Apenas os obstáculos presentes no ambiente nesta fase são considerados.

A tabela 4.1 apresenta um resumo comparativo dos trabalhos descritos nesta seção. Este comparativo leva em consideração os mecanismos utilizados na construção da solução de localização de cada técnica. Na tabela, a coluna de Referência correspondente a:

1. Paramvir Bahl, Venkata N. Padmanabhan e Anand Balachandran (BAHL; BALACHANDRAN; PADMANABHAN, 2000)
2. Ali Taheri, Arvinder Singh e Emmanuel Agu (TAHERI; SINGH; EMMANUEL, 2004)
3. Teruaki Kitazuka, Tsuneo Nakanishi e Akira Fukuda (KITAZUKA; NAKANISHI; FUKUDA, 2003)
4. Santosh Pandey, Byungsook Kim, Farooq Anjum e Prathima Agrawal (PANDEY et al., 2005)
5. Luís Felipe M. de Moraes e Bruno Astuto A. Nunes (MORAES; NUNES, 2006)

6. P. Krishnan, A. S. Krishnakumar, Wen-Hua Ju, Colin Mallows e Sachin Ganu (KRISHNAN et al., 2004)
7. Daniel B. Faria (FARIA, 2005)
8. Ansar-UI-Haque Yasar, M.A. Ansari e Sherjeel Farooqui (YASAR; ANSARI; FAROOQUI, 2006)
9. T. Stoyanova, F. Kerasiotis, A. Prayati e G. Papadopoulos (STOYANOVA et al., 2007)
10. Carsten Buschmann, Horst Hellbrück, Stefan Fischer, Alexander Kröller e Sándor Fekete (BUSCHMANN et al., 2007)
11. Masaaki Kuwabara e Nobuhiko Nishio (KUWABARA; NISHIO, 2009)

Tabela 4.1: Resumo Comparativo dos Trabalhos Correlatos

Ref	<i>fingerpint</i>	calibragem	obst. fixos	obst. din.	estações monit.	erro médio(m)
1	✓	✓	✓	X	X	2,6-5,9m
2	✓	✓	✓	X	X	não indicado no trabalho
3	✓	✓	✓	✓	estações cliente	2,8m (simulado)
4	X	X	X	✓	<i>sniffers</i>	não indicado no trabalho
5	X	X	X	✓	<i>sniffers</i>	2m
6	X	X	X	✓	equip. transm.	3,6m
7	X	X	constante	constante	X	não indicado no trabalho
8	X	✓	✓	X	estações referência	5m
9	X	X	X	✓	X	por setor
10	X	X	X	X	sensores vizinhos	dependente da densidade de sensores
11	X	✓	✓	X	X	18,65m

Salienta-se que apesar do erro médio em metros ter sido apresentado na tabela 4.1, utilizar este parâmetro como fonte de comparação pode ocasionar um erro de interpretação. A avaliação das técnicas deve considerar também todos os fatores de ambiente que podem contribuir para um melhor ou pior resultado na localização. A densidade de pontos de acesso, tamanho da área utilizada, densidade de obstáculos, número de pontos analisados, etc, devem sempre ser levados em consideração neste tipo de análise.

## 5 MECANISMO IMPLEMENTADO

Quando se utiliza um ambiente com enlace baseado em fios, a tarefa de definir uma política de segurança para uma determinada localização física (como uma sala, por exemplo) é relativamente simples. Basta que a estrutura da rede (endereçamento de rede) seja adequada à aplicação desta política. O objetivo do mecanismo implementado é o de garantir que uma determinada estação móvel possa ter sua localização obtida pela rede e que, com base nesta informação, se possa aplicar à ela a mesma política definida para as estações cabeadas localizadas no mesmo espaço físico.

Para se atingir este objetivo, o sistema foi estruturado de forma a garantir que:

1. durante o processo de associação de uma estação móvel na rede, ela seja devidamente localizada;
2. a localização da estação tenha a precisão suficiente a ponto de identificar a sala onde está fisicamente;
3. o sistema de localização repasse a informação de localização (indicação da sala) da estação móvel para o sistema responsável pela aplicação da política de segurança da rede;
4. o sistema responsável pela segurança da rede utilize a informação de localização da estação para reconfigurar os mecanismos adequados (*firewall*, *proxy*, etc) de forma a aplicar as mesmas restrições de segurança das estações cabeadas à estação móvel.

Nas próximas seções, serão descritos a implementação da solução, as técnicas utilizadas e os mecanismos desenvolvidos para alcançar os objetivos do sistema.

### 5.1 Protocolo de Associação Definido

Para garantir que a estação passe pelo processo de localização sempre que for se associar na rede, é necessário que após o processo inicial de autenticação/associação entre a estação e o AP, seja executado o sistema de localização. Conforme o tipo de processo de autenticação utilizado, o momento e a forma de acionamento do sistema de localização pode variar.

É importante, no entanto, que a localização da estação ocorra antes de garantir acesso aos recursos da rede, ou seja, a estação móvel deve estar isolada da rede até que a sua localização seja obtida. Após este processo, a política de segurança adequada deve ser aplicada à estação.

Existem diversos arranjos possíveis do processo de autenticação, tais como:

- autenticação via *proxy* com LDAP (*Lightweight Directory Access Protocol*) - neste sistema de autenticação, pode-se posicionar um *proxy* entre a estação e a rede, configurado de forma a exigir autenticação com um servidor LDAP. O processo de localização pode ser acionado pelo sistema *proxy* após a comunicação LDAP;
- autenticação via 802.1x - onde o servidor RADIUS executa o sistema de localização após a autenticação do usuário;
- autenticação via *captive portal* - estes sistemas possuem o objetivo de bloquear o acesso à internet (navegação) através do redirecionamento de requisições HTTP/HTTPS para um sistema de autenticação. Este sistema de autenticação pode ser alterado para que se execute o sistema de localização após a autenticação do usuário.

No sistema desenvolvido, utilizou-se uma solução de *captive portal*. Utilizando este tipo de ferramenta, após o processo de autenticação e associação na rede sem fios, sempre que um usuário tenta acessar a internet através de um navegador pela primeira vez, será redirecionado para uma página de autenticação. Para que possa acessar a internet, o usuário deve estar cadastrado na ferramenta. Como solução de *captive portal* utilizou-se a ferramenta *wifidog* (APRIL et al., 2008), a qual possui código sem restrições a alterações e farta documentação. Para o processo de localização, alterou-se este software para que após a entrada de usuário/senha, seja executado o processo de localização.

Para o processo de associação à rede, definiu-se um protocolo de associação de estações móveis de forma a garantir os requisitos definidos na seção anterior. A figura 5.1 apresenta o protocolo definido capaz de impor a política de segurança para a estação móvel. A comunicação ocorre da seguinte maneira:

1. a estação móvel requisita autenticação com o AP;
2. o AP concede autenticação à estação móvel para troca de pacotes na rede;
3. a estação móvel é direcionada a um *captive portal*;
4. o *captive portal* apresenta uma página de autenticação, requisitando usuário/senha;
5. o usuário da estação móvel informa usuário/senha de acesso;
6. o sistema de *captive portal* alterado realiza uma chamada ao sistema de localização, o qual deve trocar informações com a estação móvel para o processo de localização. A primeira informação requisitada são os valores de potência de sinal entre a estação móvel e todos os APs ao alcance da mesma;
7. a estação móvel envia ao sistema de localização as informações requisitadas;
8. o sistema de localização conecta-se ao AP ao qual a estação está associada e confirma o valor de potência informado;
9. o AP informa a potência identificada entre ele e a estação móvel para a confirmação do sistema de localização;
10. o sistema de localização induz a estação móvel a trocar a associação para outro AP ao alcance;

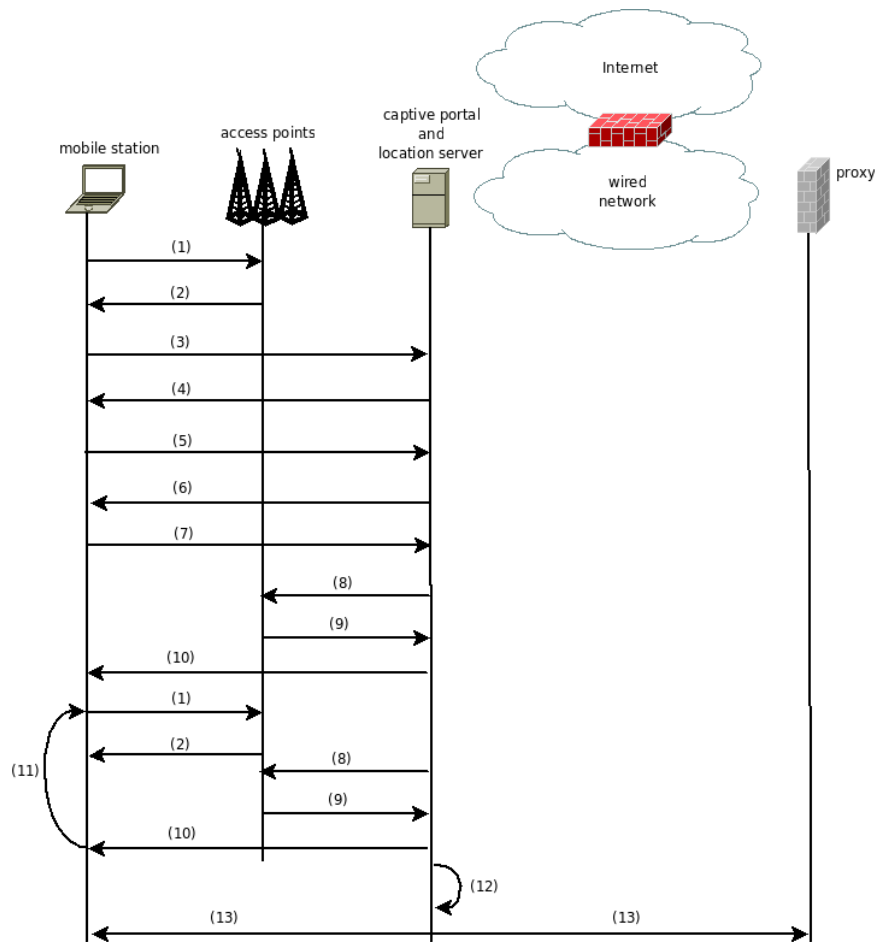


Figura 5.1: Protocolo Definido

11. a estação móvel deve repetir este processo de associação com no mínimo 3 APs para validação das informações repassadas inicialmente;
12. o sistema de localização realiza o processo de identificação da sala na qual a estação móvel está localizada e repassa esta informação ao *captive portal*;
13. o sistema de localização executa o procedimento de reconfiguração de mecanismos de segurança adequados à aplicação da política de segurança.

Como visto na fórmula 2.15, a potência de sinal recebido por uma placa de rede depende, entre outros fatores, da potência de transmissão. Como (geralmente) as placas das estações móveis possuem potência de transmissão diferentes dos APs, é necessário que a validação das informações repassadas pela estação móvel considere esta diferença de potência.

Para verificar a diferença (e a relação) entre a potência de sinal recebida pela estação e pelo AP em uma mesma comunicação, realizou-se uma série de medidas em ambos os dispositivos obtendo a relação apresentada na figura 5.2. Nesta imagem a linha superior é formada pelos dados de potência coletados na estação móvel e a inferior no AP.

É necessário esclarecer que uma vez localizada, a estação possui as restrições de acesso do local onde se encontra no momento. Caso a estação se desloque para outro ambiente, é necessário que o sistema identifique este deslocamento e atualize estas restrições. Um exemplo seria a associação de um usuário em uma área pública, com uma



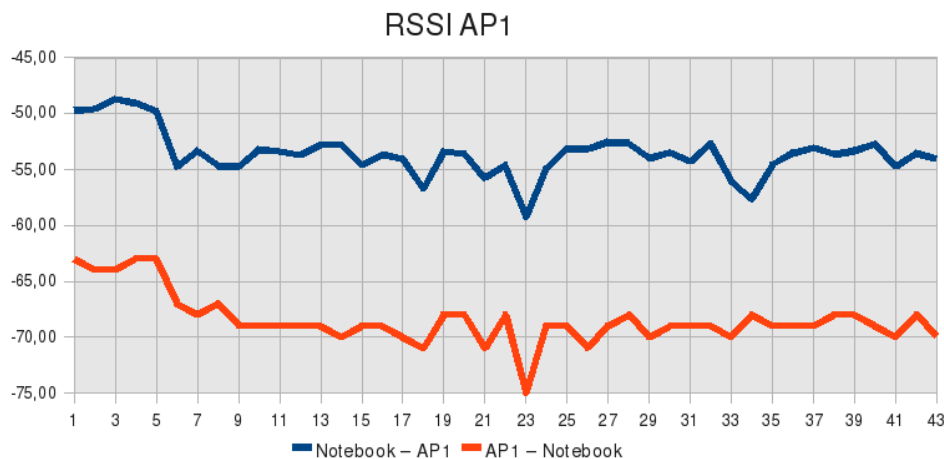


Figura 5.2: Relação de Potência em Uma Comunicação AP-Estação

determinada restrição de acesso, que se desloca para uma outra sala, onde possui restrições de acesso diferentes.

O sistema deve então, de tempos em tempos, renovar a política de segurança para todas as estações móveis, de forma a evitar que um usuário (malicioso ou não) burle as restrições de sua posição física atual.

## 5.2 Localização das Estações

Em relação ao processo de localização das estações, partiu-se da análise das diversas técnicas existente para a escolha do modelo mais adequado à solução proposta. Os requisitos para análise das técnicas levaram em consideração:

- necessidade de adição de *hardware* extra para o processo de localização tanto na infra-estrutura de rede quanto nas estações clientes;
- consideração da técnica quanto a obstáculos fixos presentes em um ambiente interno;
- consideração da técnica quanto a obstáculos dinâmicos presentes.

Inicialmente excluiu-se a utilização de equipamentos auxiliares (*hardware* extra) para a localização para que a solução não necessitasse da adição destes dispositivos (equipamentos de emissão de radiofrequência ou infravermelho) no ambiente e nas estações a serem localizadas.

O ângulo de recepção também foi excluído devido à necessidade de adição e controle de antenas direcionais em cada *access point*. Para a aplicação desta técnica seria necessário modificar o software existente internamente nestes equipamentos, o que não é permitido pela maioria dos fabricantes. Esta técnica também apresenta problemas de precisão na localização devido aos efeitos de reflexão, difração e dispersão dos sinais em um ambiente interno, o que prejudicaria o sistema.

Em relação às técnicas de tempo, decidiu-se pela sua exclusão devido à necessidade de alta precisão dos relógios envolvidos na localização (os equipamentos precisam medir diferenças de tempo na ordem de nanossegundos), conforme apresentado anteriormente.

Optou-se então pela utilização da potência do sinal recebido pela estação móvel proveniente dos APs presentes no ambiente para inferir a localização das estações. Em relação

às técnicas que utilizam esta informação, apenas o *fingerprint* considera os obstáculos fixos presentes no ambiente no momento da amostragem, porém a sua precisão depende da qualidade e número de amostras realizadas inicialmente.

A tabela 5.1 apresenta uma sumarização da análise realizada para a escolha das técnicas a serem utilizadas no sistema.

Tabela 5.1: Comparativo Entre Técnicas de Localização

considera	HW extra	ângulo	amplitude	tempo	<i>Fingerprint</i>
obst. ambiente	-	X	X	X	√
obst. dinâmicos	-	X	X	X	X
hw infra	sim	sim	não	sim	não
hw clientes	sim	não	não	não	não

A partir da análise realizada, optou-se pelo desenvolvimento de um sistema baseado nas informações de potência, utilizando a técnica de *fingerprint* com a adição da funcionalidade de dinamicamente atualizar as tabelas (matrizes) de amostras de acordo com os obstáculos presentes no ambiente. Isto se deve ao fato de mecanismo ser utilizado em um ambiente *indoor*. Foi necessário que se levasse em consideração também a presença de obstáculos dinâmicos no ambiente, capazes de alterar os dados de potência devido às interferências que causam nos sinais de microondas. Para que se pudesse obter maior confiabilidade no sistema de localização, foi desenvolvido um mecanismo que identifica a presença destes obstáculos e leva em consideração as alterações causadas por eles no processo de localização. Este técnica é utilizada pelo sistema para a detecção destes obstáculos dinâmicos com o objetivo de ampliar a precisão do sistema de localização. Também realizou-se pesquisas com a utilização da técnica de trilateração, conforme o trabalho (PERES; WEBER, 2009a).

Para obtenção das informações de potência, o sistema de localização foi concebido através de um software servidor instalado em todas as estações móveis e um software cliente adicionado à ferramenta *wifidog*. O software cliente conecta-se no servidor (na estação móvel) e coleta informações de potência de sinal entre a estação e todos os APs na área de abrangência da estação, conforme descrito na seção 5.1. Este processo configura um sistema de localização de estações *mobile based*.

### 5.2.1 Técnica de *Fingerprint*

Para realização do *fingerprint* inicialmente deve-se mapear todo o perímetro físico que se deseja utilizar como sendo a área passível de localização e dividir este perímetro em pontos de amostragem. Para cada ponto, deve-se coletar um conjunto de amostras de potência relativo a cada ponto de acesso a ser utilizado no processo de localização.

Estes pontos irão formar uma matriz por ponto de acesso, contendo como valor a média de potência de sinal relativo ao AP.

Com estas matrizes definidas, é possível que o sistema de localização, ao obter os valores de potência entre uma estação móvel e os APs existentes, consiga determinar qual o ponto da matriz mais se aproxima dos valores informados pela estação.

Considerando que a estação móvel informe que está recebendo de um dos *access points*  $AP_i$  a potência  $P_i$ , então consulta-se a matriz  $M_i$  referente ao  $AP_i$  buscando a diferença entre cada uma das células e a potência encontrada, formando uma nova matriz de diferenças  $D_i$  conforme a fórmula 5.1.



Tabela 5.4: Matriz de *Fingerprint* do  $AP3$ 

-56,28	-47,4	-49,25	-48,35	-22,9	-42,42	-38,65
-60,41	-54,33	-51,48	-56,2	-29,8	-38,71	-49,62
-65,36	-54,29	-57,85	-48,11	-49,07	-56,1	-51,93
-75	-71,85	-67	-59,01	-54,75	-57,45	-66,48
-100	-100	-74,6	-70,53	-51,81	-68,36	-56
-100	-100	-71,37	-61,35	-59,89	-66,79	-63,37
-100	-100	-100	-69,42	-69,61	-61,63	-68,2
-100	-100	-100	-66,45	-58,92	-70,87	-68,42
-100	-100	-100	-100	-60,7	-70,12	-68,87
-100	-100	-100	-72	-100	-74	-100
-100	-100	-100	-72,5	-100	-100	-100
-100	-100	-100	-69,27	-100	-100	-100
-100	-100	-100	-68,45	-100	-100	-73,23
-100	-100	-100	-100	-100	-100	-100

Tabela 5.5: Matriz  $D_{AP1}$ 

4	4	4	0	14	9	12
11	9	3	6	1	4	7
9	6	2	0	2	8	11
20	10	6	1	7	8	9
28	7	11	3	10	0	13
28	11	4	1	6	5	9
27	16	5	5	7	0	0
11	22	15	5	8	4	2
26	12	17	8	6	4	7
16	8	9	4	3	1	8
13	13	11	5	3	4	6
5	8	9	1	11	9	5
6	1	7	2	4	14	11
34	34	15	34	34	34	34

Ao final do processo, existe então este conjunto de matrizes contendo as diferenças entre cada célula e a potência informada pela estação (tabelas  $D_{AP1}$ ,  $D_{AP2}$  e  $D_{AP3}$  no exemplo). Para identificar o ponto de localização da estação, soma-se as células das matrizes, formando uma matriz contendo a soma das diferenças entre as células de  $P$  conforme a fórmula 5.2. Na fórmula 5.2,  $numaps$  representa o número de *access points* disponíveis no ambiente.

$$P[x, y] = \sum_{i=1}^{numaps} D_i[x, y] \quad (5.2)$$

A tabela 5.8 apresenta a soma das tabelas 5.5, 5.6 e 5.7.

A célula de  $P[x, y]$  que contiver o menor valor, será identificada como a provável localização da estação móvel. Caso mais de uma célula apresente o menor valor, o sistema deverá distribuir a probabilidade de localização entre estas células (tendo em vista que o sistema não tem como identificar dentre estas células qual representa a localização da

Tabela 5.6: Matriz  $D_{AP2}$ 

34	27	31	26	15	13	9
31	33	22	21	9	14	12
34	26	29	22	12	17	6
26	34	35	19	6	11	14
34	26	30	18	5	2	8
36	29	23	13	12	12	14
37	36	32	19	19	16	13
55	28	32	24	15	15	23
55	29	36	22	16	13	24
55	55	35	25	26	25	28
55	55	55	33	31	27	33
55	55	55	55	33	23	55
55	55	55	55	32	21	55
55	55	55	55	55	35	55

Tabela 5.7: Matriz  $D_{AP3}$ 

14	23	21	22	48	28	32
10	16	19	14	41	32	21
5	16	13	22	21	14	19
5	1	3	11	16	13	4
30	30	4	0	19	2	14
30	30	1	9	11	4	7
30	30	30	1	1	9	2
30	30	30	4	12	0	2
30	30	30	30	10	0	2
30	30	30	2	30	4	30
30	30	30	2	30	30	30
30	30	30	1	30	30	30
30	30	30	2	30	30	3
30	30	30	30	30	30	30

estação).

No caso do exemplo da tabela 5.8, a célula  $P[4, 5] = 4$  apresenta o menor valor, fazendo com que o sistema assuma que a estação móvel encontra-se nesta posição.

### 5.2.2 Identificação de Obstáculos Dinâmicos

A técnica de *fingerprint* descrita não leva em consideração a presença de obstáculos dinâmicos no ambiente. Desenvolveu-se então um mecanismo capaz de dinamicamente identificar a presença destes obstáculos e refletir o impacto dos mesmos na localização. O objetivo é o de incorporar como parte do sistema de localização a presença destes obstáculos.

Para identificar a presença de obstáculos dinâmicos, utilizou-se os APs como dispositivos capazes de monitorar a potência de sinal entre eles, através da operação de *site survey*. A operação de *site survey* faz com que um AP identifique todos os demais *access points* na área de abrangência, além de obter a potência entre eles. Um *access point*  $AP_i$

Tabela 5.8: Somatório das Matrizes de Diferença de Potência  $P$ 

52	54	56	48	77	50	53
52	58	44	41	51	50	40
48	48	44	44	35	39	36
51	45	44	31	29	32	27
92	63	45	21	34	4	35
94	70	28	23	29	21	30
94	82	67	25	27	25	15
96	80	77	33	35	19	27
111	71	83	60	32	17	33
101	93	74	31	59	30	66
98	98	96	40	64	61	69
90	93	94	57	74	62	90
91	86	92	59	66	65	69
119	119	100	119	119	99	119

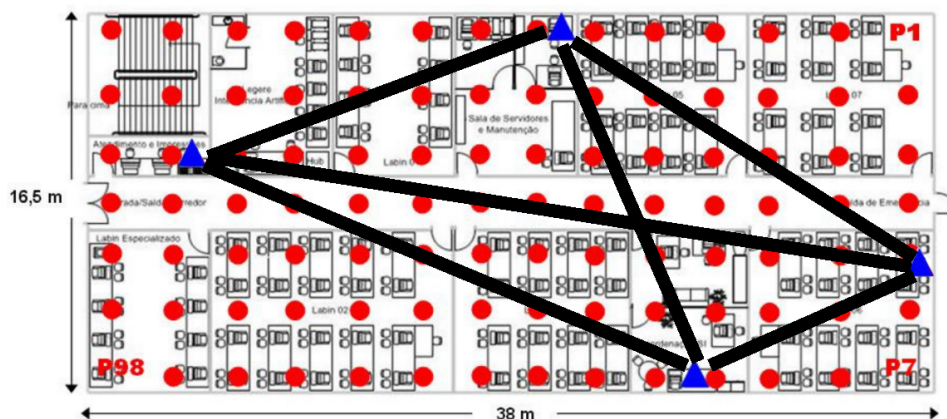


Figura 5.3: Linhas de Identificação de Obstáculos Dinâmicos

é capaz então de identificar a potência do sinal entre ele e todos os demais. Esta operação é realizada sempre que o sistema de localização inicia o processo de localização de uma estação móvel.

O sistema de localização possui um registro inicial da potência entre todas as duplas de APs (mapeamento inicial sem obstáculos dinâmicos) e, quando aciona a operação de *site survey* entre eles é capaz de identificar alterações no valor destas potências. Qualquer obstáculo entre os APs irá causar uma alteração de potência que deverá ser refletida na matriz de *fingerprint*. A figura 5.3 representa as ligações entre os *access points* (representados por triângulos) sendo as linhas entre os APs a região onde obstáculos dinâmicos serão identificados.

Cada *access point* na operação de *site survey* informa ao sistema de localização os seguintes dados:

$$info = [AP\_MAC_i; P_i]$$

onde  $AP\_MAC_i$  é o endereço MAC do *access point*  $AP_i$  (vizinho) encontrado no *site survey* e  $P_i$  é a potência em decibéis de sinal entre o equipamento que está realizando a

operação e  $AP_i$ . O sistema de localização deve identificar ainda quais são as coordenadas  $x, y$  do *access point* consultado, na matriz de *fingerprint*,

Quando o sistema de localização recebe estas informações do AP, ele deve verificar se houve alguma alteração no valor da potência do sinal entre uma dupla de *access points*. Caso seja descoberto um valor diferente de potência, a diferença deverá ser refletida na matriz de *fingerprint* em todas as células entre esta dupla de APs.

Se o valor mapeado inicialmente entre dois *access points*  $AP1$  e  $AP2$  for  $P_{inic}$ , e o valor retornado pelo *site survey* for  $P_{nova} \neq P_{inic}$ , então  $obst = |P_{nova} - P_{inic}|$ . Ao identificar esta alteração o sistema de localização deve buscar na matriz de *fingerprint* todas as células entre  $AP1$  e  $AP2$  e alterar o valor de potência das mesmas. O valor  $obst$  deve ser distribuído nestas células devido ao fato do sistema de localização não ter como precisar em qual destas células se encontra o obstáculo.

Para que se mantenha a referência inicial de mapeamento, e a garantia de localizar as estações móveis com uma matriz de *fingerprint* atualizada, definiu-se que cada *access point* possui duas matrizes sendo:  $FP_i$  a matriz inicial e  $FP_u$  a matriz atualizada pela descoberta de obstáculos dinâmicos.

Para determinar a distância das células entre os dois APs é utilizada a fórmula de distância euclidiana (este processo é eficiente devido às células representarem a mesma distância física do ambiente). Cria-se uma nova matriz representando a distância de cada célula relativa aos APs  $AP1$  e  $AP2$ . As fórmulas utilizadas para a identificação da distância de cada célula da matriz e a área entre os *access points* é definida em 5.3, 5.4 e 5.5.

$$DAP1[x][y] = \sqrt{(AP1_x - x)^2 + (AP1_y - y)^2} \quad (5.3)$$

$$DAP2[x][y] = \sqrt{(AP2_x - x)^2 + (AP2_y - y)^2} \quad (5.4)$$

$$dist = DAP1[x][y] + DAP2[x][y] \quad (5.5)$$

Onde  $DAP1[x][y]$  equivale à distância entre a célula  $[x][y]$  e o  $AP1$ , e  $DAP2[x][y]$  equivale à distância entre a célula  $[x][y]$  e o  $AP2$ . A distância  $dist$  é definida como a soma de  $DAP1 + DAP2$ . Para determinar quais células devem ser modificadas, identifica-se o menor valor de  $dist$  ( $dist_{min}$ ).

Conforme a área física entre  $AP1$  e  $AP2$ , deve-se considerar a possibilidade do obstáculo não estar posicionada exatamente entre os dois APs. Caso o obstáculo esteja próximo à reta entre  $AP1$  e  $AP2$ , mesmo assim poderá causar interferências na potência do sinal entre eles.

Para tratar esta situação, especificou-se uma constante de limiar  $\alpha_d$  para cada dupla de APs  $d$  (pois cada dupla possui uma distância diferente entre si e conseqüentemente um número de células também diferente). Toda célula que possuir o valor de distância  $dist \leq dist_{min} + \alpha_d$  será modificada. O novo valor de potência de uma célula é definido na fórmula 5.6.

$$FP_u[x, y] = FP_i[x, y] - obst \quad (5.6)$$

Se o valor de  $\alpha_d$  for zero, apenas as células que formam a linha entre os APs serão alteradas. Conforme o valor de  $\alpha_d$  for incrementado, mais células entre os pontos são afetadas (formando uma elipse de células modificadas). A figura 5.4 apresenta a utilização de  $\alpha$  entre os APs.

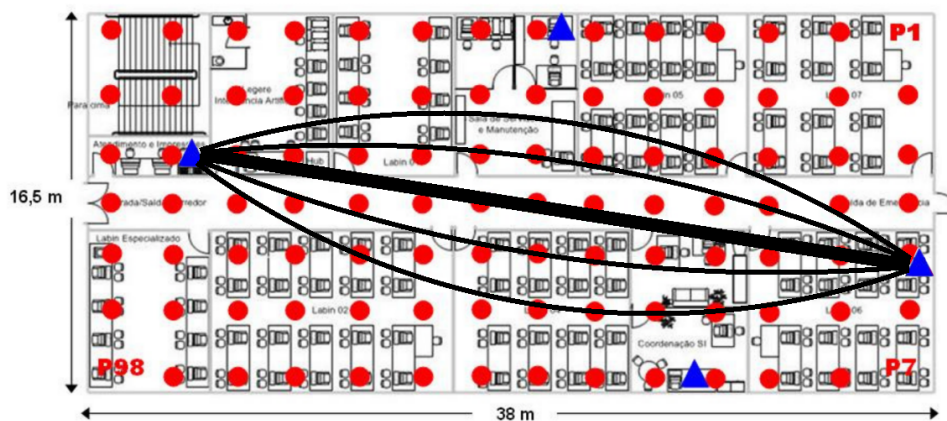


Figura 5.4: Definição de  $\alpha$  entre dois APs

A determinação do limiar  $\alpha_d$  mais adequado depende de testes no ambiente, verificando a distância entre os APs, a quantidade e impacto dos obstáculos dinâmicos e o ambiente em que se está aplicando a localização. A definição do valor de limiar  $\alpha_d$  é afetada por:

- o número de *access points* - com poucos dispositivos,  $\alpha$  deve possuir um valor maior;
- o tamanho da matriz - quanto maior a matriz, maior a área que deve ser considerada, portanto o valor de  $\alpha$  deve ser maior.

Sempre que o sistema iniciar o processo de localização de uma estação móvel, ele irá buscar em todos os *access points* os novos valores de potência entre eles para atualizar a matriz de *fingerprint*  $FP_u$ . Após esta atualização, o sistema irá realizar o mesmo processo de *fingerprint* original para determinar em qual posição a estação móvel se encontra.

### 5.3 Aplicação da Política de Segurança

O processo de localização deve retornar a posição física na qual a estação móvel se encontra. No caso do cenário utilizado, o prédio foi dividido em áreas que correspondem às salas, portanto é esta identificação que o sistema retorna.

Ao receber a identificação da sala, a parte do sistema responsável por aplicar a política de segurança gera uma nova regra no *proxy* para que o IP da estação móvel tenha acesso apenas aos sites liberados para a sala de aula na qual está, respeitando o horário da aula. Assim que a nova regra é adicionada no *proxy*, o mesmo é recarregado e passa a aplicar as restrições.

A reconfiguração do *proxy* é realizada alterando-se o arquivo de configurações do mesmo (incluindo a nova regra) e forçando o mesmo a recarregar as regras deste arquivo.

O modelo de autenticação proposto é apresentado na figura 5.5. Nesta figura observa-se que inicialmente o usuário/estação deve autenticar-se através do protocolo 802.1x, garantindo a identidade do usuário. Após este processo de autenticação, verifica-se a localização física onde a estação encontra-se. Posteriormente o sistema de *firewall/proxy* é adequado de acordo com a política de segurança especificada.



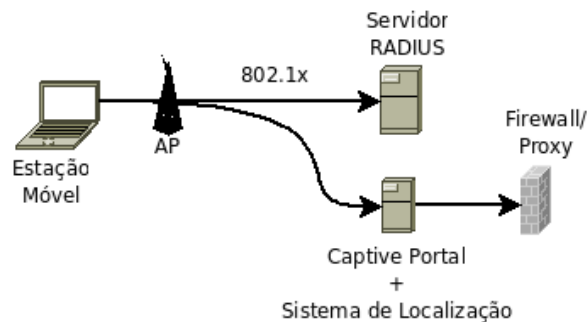


Figura 5.5: Processo de Autenticação com Localização de Estação

## 5.4 Relação da Técnica desenvolvida com o Estado da Arte

Quando compara-se a técnica desenvolvida com os demais trabalhos em localização de estações utilizando amplitude, identifica-se que a técnica desenvolvida:

- utiliza *fingerprint* com mapeamento inicial (calibragem) considerando os obstáculos fixos;
- utiliza atualização dinâmica com atualização das matrizes de *fingerprint*;
- não necessita a utilização de estações clientes para realização de atualização das tabelas (utiliza os próprios APs), sem necessidade de adição de equipamentos no ambiente.

Dentre todos os trabalhos analisados, nota-se que o trabalho que mais se aproxima da técnica proposta é o trabalho de (KITASUKA; NAKANISHI; FUKUDA, 2003). Este trabalho, no entanto apresenta os seguintes pontos a serem considerados:

- a utilização de estações de clientes como parte do processo de localização é considerado como sendo um fator negativo quando da utilização das mesmas para sistemas de segurança. Isto deve-se ao fato da possibilidade do comprometimento destas estações por usuários maliciosos de forma a comprometer todo o sistema. A confiabilidade das informações entre estações vizinhas depende unicamente na confiabilidade das estações, não sendo previsto mecanismo para verificar se uma estação está repassando informações alteradas sobre seus vizinhos para o sistema de localização;
- para que uma estação possa medir a potência do sinal entre ela e as demais estações, são necessárias modificações na interface de rede. Considera-se duas hipóteses para atingir este objetivo: 1 a estação deve estar em modo monitor, o que impede que a mesma seja inserida na rede; 2 exista uma alteração no *driver* existente para que esta funcionalidade seja atingida. Tais hipóteses não correspondem a utilização destas estações em um ambiente onde as mesmas não sejam controladas pela gerência da rede;
- não é considerada no trabalho a possibilidade da modificação da localização física de uma estação que faz parte do processo de localização, ou seja, caso uma estação que está monitorando estações vizinhas se desloque no ambiente. Nas simulações as estações móveis não se movimentam.

Todos estes aspectos devem ser considerados quando pretende-se utilizar a localização de uma estação como sendo uma informação a ser utilizada em mecanismos de segurança.

A tabela 5.9 apresenta o comparativo entre as técnicas analisadas e a técnica proposta, tendo como principais diferenças:

Tabela 5.9: Resumo Comparativo dos Trabalhos Correlatos e Técnica Desenvolvida

Ref	<i>fingerptint</i>	calibragem	obst. fixos	obst. din.	estações monit.
1	✓	✓	✓	X	X
2	✓	✓	✓	X	X
3	✓	✓	✓	✓	estações cliente
4	X	X	X	✓	<i>sniffers</i>
5	X	X	X	✓	<i>sniffers</i>
6	X	X	X	✓	equip. transm.
7	X	X	constante	constante	X
8	X	✓	✓	X	estações referência
9	X	X	X	✓	X
10	X	X	X	X	sensores vizinhos
11	X	✓	✓	X	X
téc. desenv.	✓	✓	✓	✓	APs

- (BAHL; BALACHANDRAN; PADMANABHAN, 2000) - não considera obstáculos dinâmicos;
- (TAHERI; SINGH; EMMANUEL, 2004) - não considera obstáculos dinâmicos;
- (KITASUKA; NAKANISHI; FUKUDA, 2003) - não considera os aspectos de segurança na utilização da técnica;
- (PANDEY et al., 2005) - necessidade de estações *sniffers* para obtenção de dados de potência;
- (MORAES; NUNES, 2006) - necessidade de estações *sniffers* para obtenção de dados de potência;
- (KRISHNAN et al., 2004) - necessita de equipamento específico para transmissão de sinais de potência;
- (FARIA, 2005) - utiliza valores constantes para descrever o impacto de obstáculos, não sendo estes adequados a qualquer ambiente, e não adaptando-se quando da alteração de densidade de obstáculos;
- (YASAR; ANSARI; FAROOQUI, 2006) - não considera obstáculos dinâmicos;

- (STOYANOVA et al., 2007) - localização por setor, não tendo a precisão necessária para aplicações *indoor* envolvendo segurança;
- (BUSCHMANN et al., 2007) - utilizado em redes de sensores sem fios, dependendo de informações de sensores vizinhos;
- (KUWABARA; NISHIO, 2009) - não considera obstáculos dinâmicos.

O fato da técnica proposta incluir a análise de obstáculos dinâmicos sem o impacto da utilização de estações extras de monitoramento, além de ter os APs (administrados pela gerência da rede) como fonte para esta informação, são considerados como sendo os pontos fortes desta técnica.

## 6 TESTES E RESULTADOS OBTIDOS

Para validação do método de localização, e avaliação da precisão alcançada pelo mesmo, foram realizados diversos testes em um ambiente real.

Os testes foram realizados buscando validar:

1. comprovação das interferências provenientes de obstáculos dinâmicos e avaliação do impacto real no cenário de testes;
2. nível de precisão da localização utilizando a técnica de *fingerprint*;
3. nível de precisão da localização utilizando a técnica de *fingerprint* considerando obstáculos dinâmicos.

### 6.1 Cenário de Testes

O cenário escolhido para a solução desenvolvida foi o laboratório de informática da Universidade Luterana do Brasil, campus Guaíba. O laboratório é composto por sete salas nas quais são ministradas as aulas, um laboratório de pesquisa, a sala de coordenação do curso de Sistemas de Informação, um *datacenter* com os servidores e uma sala de atendimento/impressão para os alunos. A figura 6.1 apresenta as salas de aula (1-7), o laboratório de pesquisa (8), *datacenter* (9), sala de coordenação (10) e atendimento (11).

Todas as estações possuem acesso à Internet, e para garantir a qualidade das aulas, e manter a atenção dos alunos no conteúdo da disciplina, foi desenvolvido um sistema de controle de acesso a sites garantido por um *proxy*. Cada professor possui acesso ao sistema onde deve informar uma lista de sites permitidos e/ou proibidos durante sua aula.

Para que a política definida seja aplicada apenas ao laboratório ao qual um determinado professor ministra suas aulas, cada professor deve dar entrada no sistema dos dias da semana de suas aulas e das respectivas salas. As estações estão organizadas em sub-redes IP definidas por sala da aula de forma a permitir que o *proxy* realize as restrições de acordo com a sub-rede, o dia da semana e horário de aula.

O laboratório permite, no entanto, acesso a uma rede sem fios, disponível através de quatro *access points* distribuídos pelo laboratório. Estes equipamentos fornecem acesso a uma sub-rede separada das demais.

Um aluno que possui acesso à rede sem fios, em uma sala de aula, está em uma sub-rede separada das estações cabeadas e conseqüentemente não possui as mesmas restrições de acesso impostas pelo professor.

Para contornar esta situação, o sistema de localização desenvolvido deve localizar a estação móvel e, de acordo com sua posição física, impor a ela as mesmas políticas de acesso das estações cabeadas (as restrições serão aplicadas para o endereço IP específico

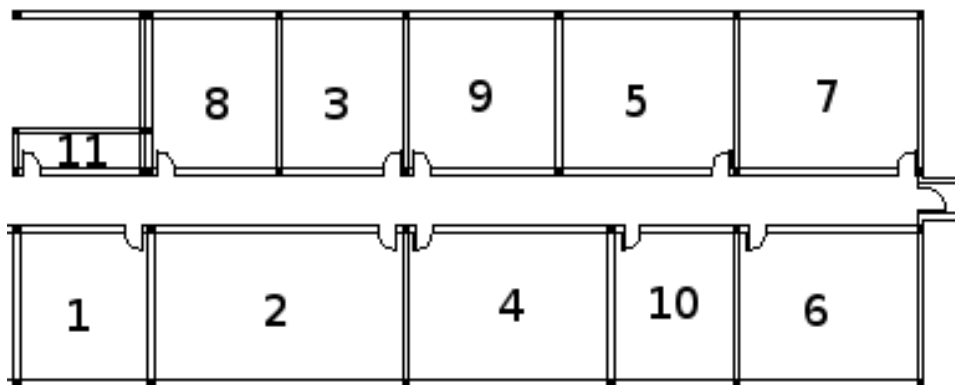


Figura 6.1: Planta Baixa do Cenário de Testes

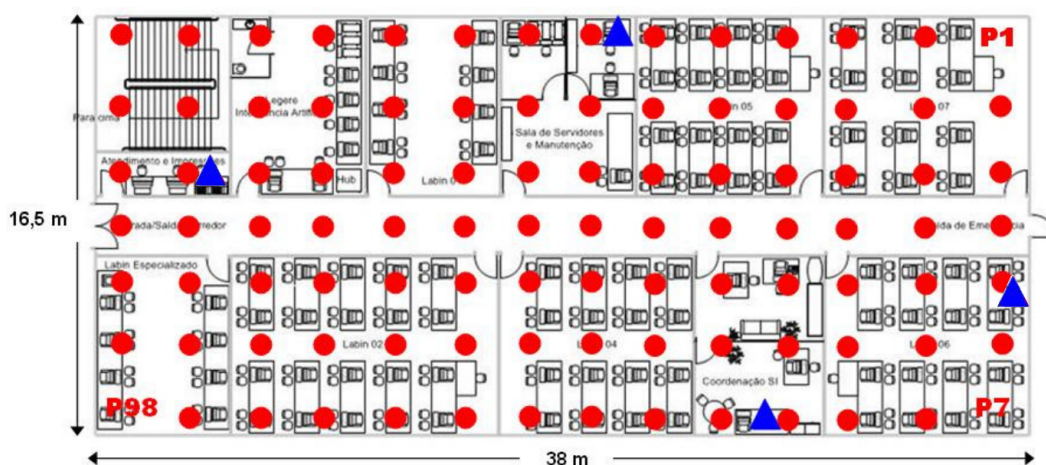


Figura 6.2: Pontos de Amostragem de *Fingerprint*

da estação durante o horário de aula). No caso das estações móveis, isto implica na migração de uma política de segurança baseada em sub-rede IP para uma política de segurança baseada em localização física das estações.

Os equipamentos disponíveis no ambiente para o sistema são:

- dois *access points* Linksys modelo WRT-54G alterados com o *firmware dd-wrt-mini*;
- dois *access points* D-link modelos DWL-G700AP e DWL-900AP+;
- um computador AMD Sempron 2500+ com 256 MB de memória RAM para o serviço de localização.

O laboratório possui uma área de  $627m^2$ , a qual foi dividida em uma tabela de  $14 \times 7$  pontos formando  $13 \times 6$  setores. Cada setor possui  $2m \times 2m$ . Em cada ponto foram coletadas 150 amostras de potência entre uma estação móvel e os *access points* acessíveis. A médias destas amostras foi inserida na matriz de *fingerprint*, armazenada no servidor de localização. Foi criada uma matriz diferente para cada um dos quatro APs, representando a potência entre este equipamento e cada ponto medido. A figura 6.2 apresenta os pontos de coleta na planta baixa do laboratório utilizado como cenário.

Na figura 6.2, os *access points* são representados como triângulos e os pontos de amostragem como círculos. Os APs possuem localização fixa e conhecida. O resultado da

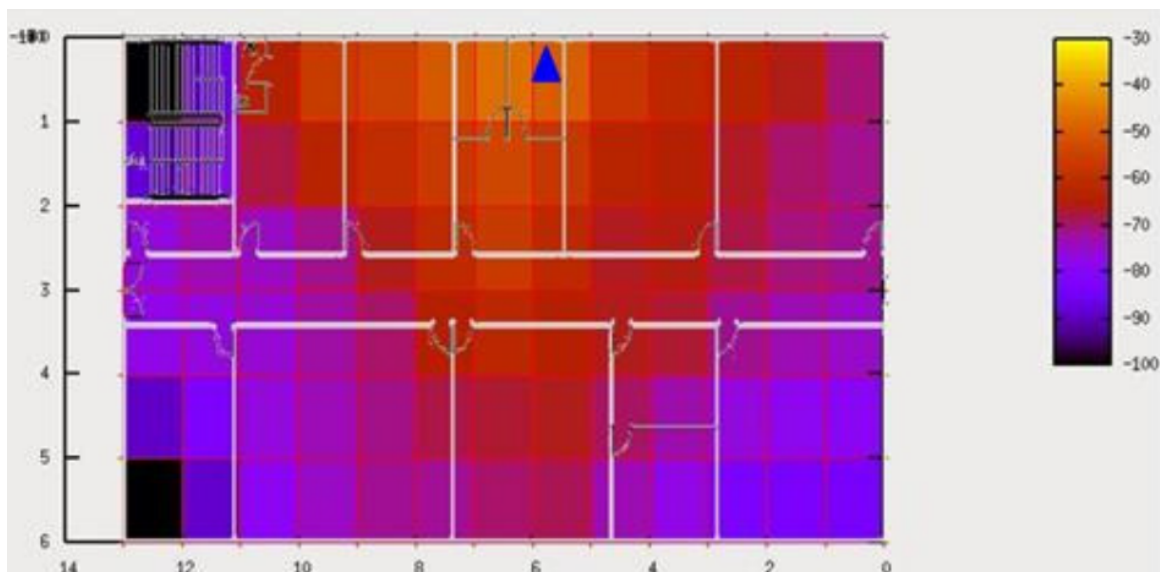


Figura 6.3: Distribuição da Potência de um AP (dB)

amostragem de um dos APs (localizado no *datacenter*) pode ser verificado na figura 6.3, a qual representa a potência do sinal deste equipamento no ambiente onde foram realizadas as amostras (matriz de *fingerprint* deste equipamento).

## 6.2 Análise Realizada

Para a validação e análise das interferências provenientes de obstáculos dinâmicos, posicionou-se um equipamento sem fios no cenário de testes, na sala de aula 7. Este equipamento permaneceu realizando medições de potência de sinais provenientes do AP localizado no *datacenter* (sala 9) durante 48 horas em intervalos de 5 segundos. A figura 6.4 representa a localização dos equipamentos.

A figura 6.5 apresenta os valores de potência de sinal obtidos neste processo. Esta figura apresenta um gráfico de 24 horas compilando as amostras de 48 horas (utiliza-se no gráfico duas amostras por instante de tempo). O objetivo é o de verificar a variação da potência nos períodos de maior movimentação de pessoas (obstáculos dinâmicos).

Percebe-se na figura 6.5 que o período que apresenta mais variações de potência encontra-se entre 12:00h e 23:00h, o qual corresponde ao período em que o laboratório permanece aberto ao público. Percebe-se também a variação significativa durante o período de aula, entre as 19:10h e 22:30h. Para melhor visualizar-se este último período, foi feita uma ampliação nesta faixa de horário (das 18:30h até as 23:00h), representada na figura 6.6.

A figura 6.6 mostra que durante a ocupação da sala de aula, existe uma diminuição da potência do sinal recebido pela estação. Esta diminuição é proveniente dos diversos obstáculos adicionados ao ambiente. Nota-se que no período de intervalo de aula, entre 20:45h e 21:15h existe uma melhora no sinal, correspondente à saídas dos alunos da sala de aula. Após as 21:15h o sinal volta a diminuir, retornando a um estado estável após as 22:30h (término da aula). Como visto na figura 6.5 o sinal permanece estável até as 12:00h do próximo dia.

Após a verificação do impacto dos obstáculos na distribuição da potência entre os APs e as estações móveis, passou-se a monitorar a variação de potência entre os APs. Para isto,

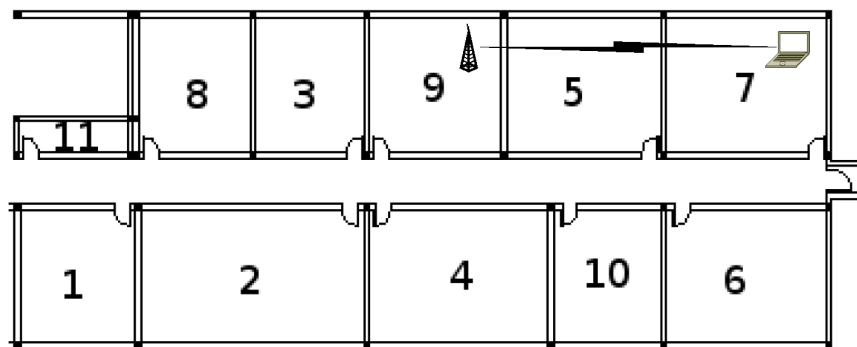


Figura 6.4: Obtenção de Variações de Potência por Obstáculos Dinâmicos

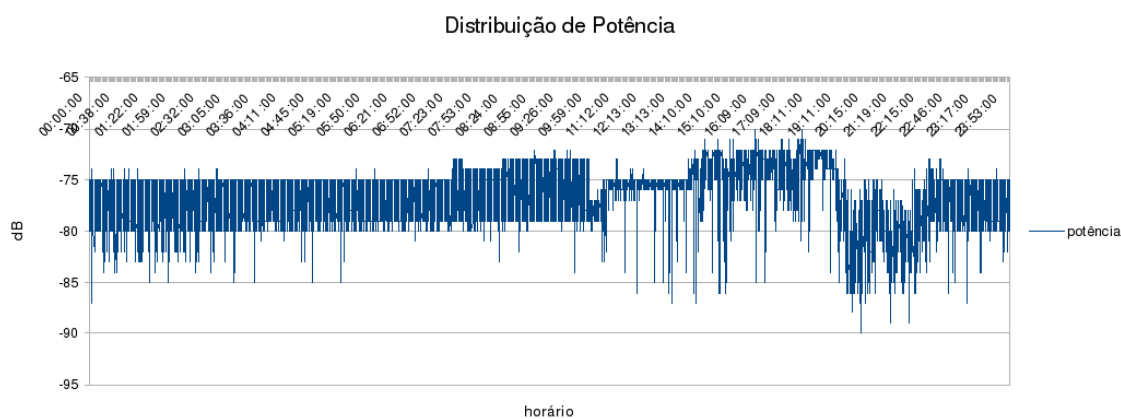


Figura 6.5: Obstáculos Dinâmicos - Compilação de 48 horas

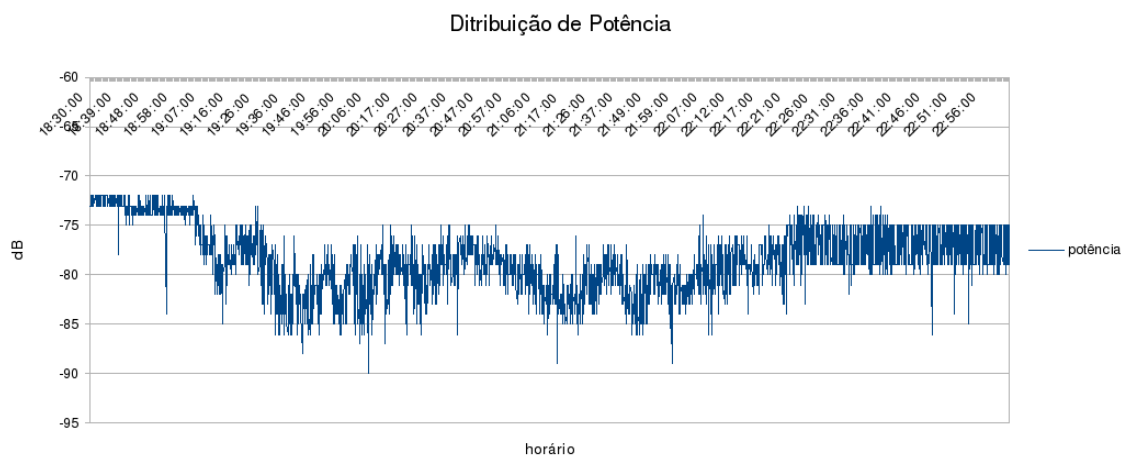


Figura 6.6: Obstáculos Dinâmicos - Período de Aula

desenvolveu-se um programa cliente capaz de conectar-se ao AP1 localizado na sala do *datacenter* (sala 9, conforme visto na figura 6.1). A forma de obtenção da potência dos sinais entre os APs é obtida através da funcionalidade de *site survey*, conforme descrito anteriormente no item 5.2.2. Foram realizadas 2700 amostras com intervalos de 5 minutos entre cada amostragem. A figura 6.7 apresenta o resultado das amostras de potência entre o AP1 (sala 9 - *datacenter*) e AP2 (sala 10 - coordenação). A partir destas amostras,

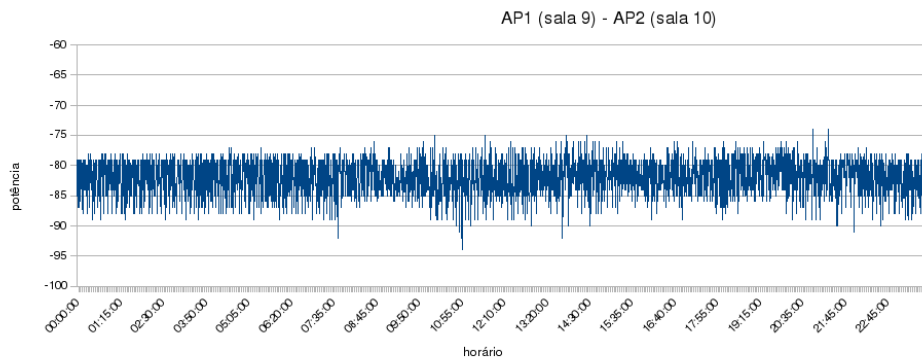


Figura 6.7: Obstáculos Dinâmicos - AP1 - AP2

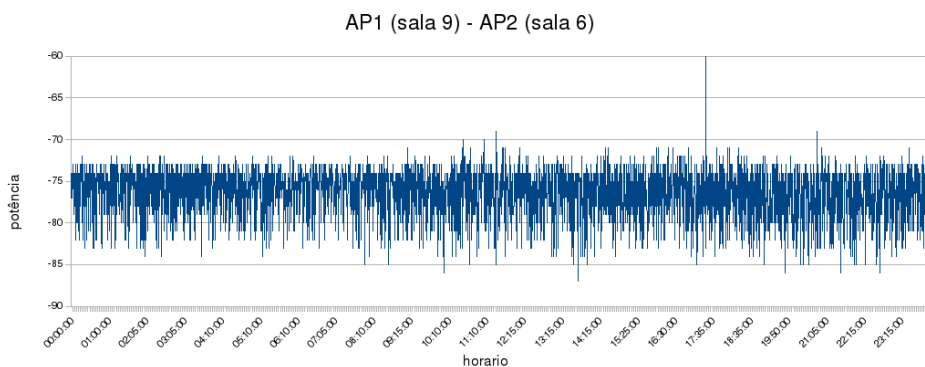


Figura 6.8: Obstáculos Dinâmicos - AP1 - AP3

constatou-se que o valor médio da potência do sinal entre o AP1 e o AP2 é de  $-81,89dB$  com desvio padrão de  $3,16dB$ . Na figura 6.8 os resultados da potência entre o AP1 e o AP3 (sala 6) com média de  $-74,41dB$  e desvio padrão de  $3,13dB$ .

Para avaliar o impacto dos obstáculos na localização e a precisão das técnicas, implementou-se um protótipo do sistema de localização que realiza este processo utilizando as informações fornecidas pela estação móvel. A estação informa a potência do sinal proveniente dos APs que estão em sua área de abrangência para o sistema de localização. O sistema de localização por sua vez realiza a localização utilizando as diferentes técnicas. É importante salientar que os mesmos dados fornecidos pela estação móvel são utilizados para localização via *fingerpint* e via *fingerpint* considerando obstáculos dinâmicos, permitindo a comparação da precisão entre as técnicas.

A validação do protótipo foi feita através da obtenção da localização de uma estação móvel em diferentes situações, descritas nas próximas seções (PERES; WEBER, 2009b).

### 6.3 Situação 1 - Cenário livre de Obstáculos

O objetivo da criação desta situação foi a de validar a alteração na obtenção da localização da estação móvel em um ambiente em que os obstáculos dinâmicos não causam grande impacto, ou seja, a interferência no sinal obtido pela estação é proveniente apenas dos obstáculos fixos já presentes no ambiente. Para obter-se esta situação, utilizou-se o cenário de testes em horário com baixo movimento de pessoas, na sala de aula 6.

Foram realizadas 80 rodadas de coleta de amostragens da potência de sinal recebido



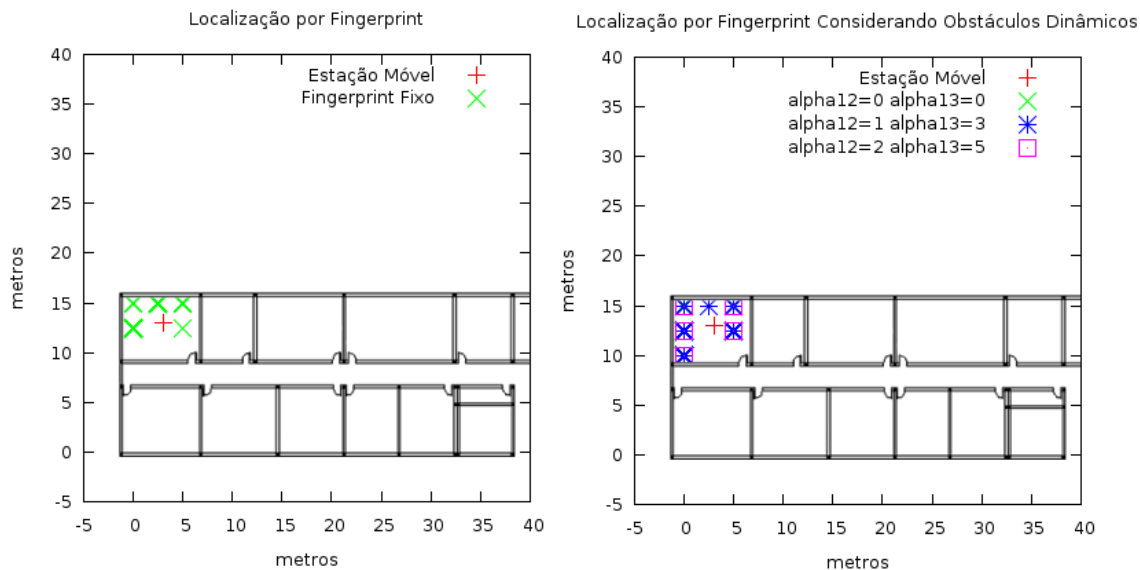


Figura 6.9: Situação 1 - Comparativo entre as Técnicas de *Fingerprint*

pela estação móvel e da potência do sinal entre os APs. Cada uma das amostragens de potência de sinal feita na estação móvel é o resultado da média de 50 coletas de potência de sinal. Estas coletas foram armazenadas e utilizadas em cada um dos diferentes algoritmos para obtenção da localização da estação. Simultaneamente às amostras de potência da estação móvel, foram tomadas amostras das alterações de potência entre os pontos de acesso para a obtenção da localização considerando obstáculos dinâmicos, totalizando também 80 amostras deste tipo.

A figura 6.9 apresenta a localização obtida a partir destas amostras utilizando o algoritmo de *fingerprint* sem alterações (lado esquerdo da imagem) e um comparativo com a técnica de *fingerprint* considerando obstáculos dinâmicos.

Ao analisar-se a figura 6.9 identifica-se que ambas as técnicas apresentam resultados semelhantes. A localização da estação sempre foi apontada como sendo a sala 6 em todas as 80 amostras realizadas. Dentro das possíveis posições físicas na sala, no entanto, as técnicas apresentaram diferentes resultados.

Nota-se também nesta imagem que o processo de localização também foi realizado com o intuito de verificar os diferentes resultados de acordo com o valor de  $\alpha$  utilizado. A figura 6.10 apresenta os resultados de precisão das técnicas considerando o erro em metros do valor apontando como sendo a localização da estação móvel.

Têm-se então que a técnica de *fingerprint* fixo apresenta um erro médio de localização de 2,71m. A técnica de *fingerprint* considerando obstáculos dinâmicos possui precisão de acordo com o valor de  $\alpha$  com erro médio de:

- $\alpha_{12} = 0; \alpha_{13} = 0$ : erro médio = 3,56m
- $\alpha_{12} = 1; \alpha_{13} = 3$ : erro médio = 3,48m
- $\alpha_{12} = 2; \alpha_{13} = 5$ : erro médio = 3,68m

sendo  $\alpha_{12}$  o valor de  $\alpha$  utilizado entre o AP1 e AP2 e  $\alpha_{13}$  o valor de  $\alpha$  utilizado entre o AP1 e AP3. A partir da determinação do menor erro para  $\alpha$ , manteve-se os valores constantes para as demais situações de testes.

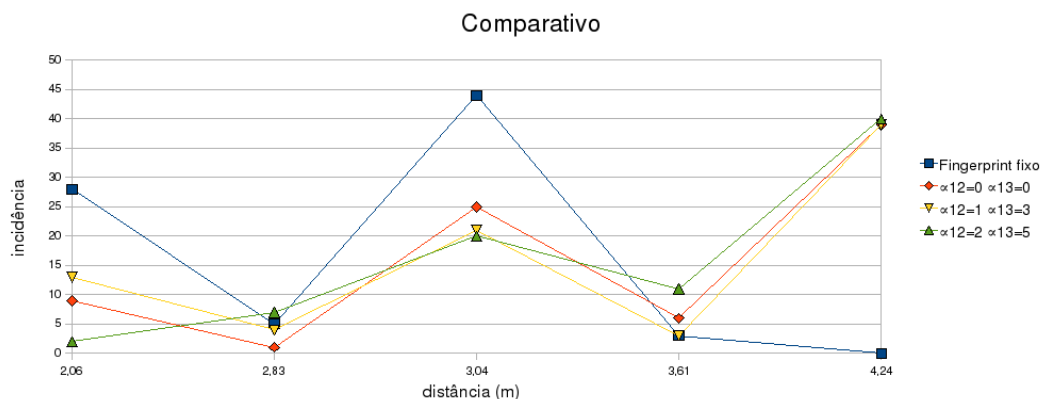


Figura 6.10: Situação 1 - Precisão das Técnicas

Nesta primeira situação, obteve-se sucesso na localização das estações, considerando-se que o objetivo final do sistema proposto é o de identificar a sala em que a estação móvel encontra-se. Apesar disto, em um ambiente livre da presença de obstáculos dinâmicos, a utilização da técnica de *fingerprint* considerando estes obstáculos apresentou um erro médio maior (aproximadamente  $80\text{cm}$ ) que a técnica de *fingerprint* fixo.

## 6.4 Situação 2 - Cenário Com Obstáculo Inserido

Para dar continuidade na validação e identificação da precisão da localização das estações proposta, criou-se uma segunda situação, na qual estavam presentes poucos obstáculos dinâmicos (os testes foram realizados em um período de baixa movimentação de pessoas) e inseriu-se um obstáculo entre a estação móvel e o AP2 para verificar o impacto deste obstáculo no sistema. Desta feita, realizou-se a tomada de 50 amostras de posição/variação de potência entre os APs.

A estação móvel foi posicionada na sala da coordenação em um ponto entre o AP1 e o AP2. Em um primeiro momento localizou-se a estação sem a adição do obstáculo. A figura 6.11 apresenta os resultados obtidos pelas técnicas no processo de localização da estação móvel.

Apesar das duas técnicas apresentarem praticamente os mesmos pontos de localização, diferentemente da situação 1, neste caso a técnica de *fingerprint* considerando obstáculos dinâmicos apresentou uma precisão superior à outra técnica. Na figura 6.12 nota-se que a técnica proposta possui um volume de localizações assertivas bastante superior à técnica de *fingerprint* fixo.

Comparando-se as técnicas identifica-se que o erro médio nesta situação fica:

- *fingerprint* fixo:  $5,7\text{m}$ ;
- *fingerprint* considerando obstáculos dinâmicos:  $2,84\text{m}$ .

Ao analisar-se a figura 6.11 identifica-se que nesta situação, em alguns casos o sistema de localização não obteve a localização da sala de forma correta (identificou que a estação móvel encontra-se em sala diferente da real). Isto acarreta em um erro no sistema de autenticação proposto no qual a estação receberá privilégios de acesso diferentes do especificado na política de segurança. Este erro de localização possui um percentual de ocorrência maior quando da utilização da técnica de *fingerprint* fixo como pode-se perceber na figura 6.13.

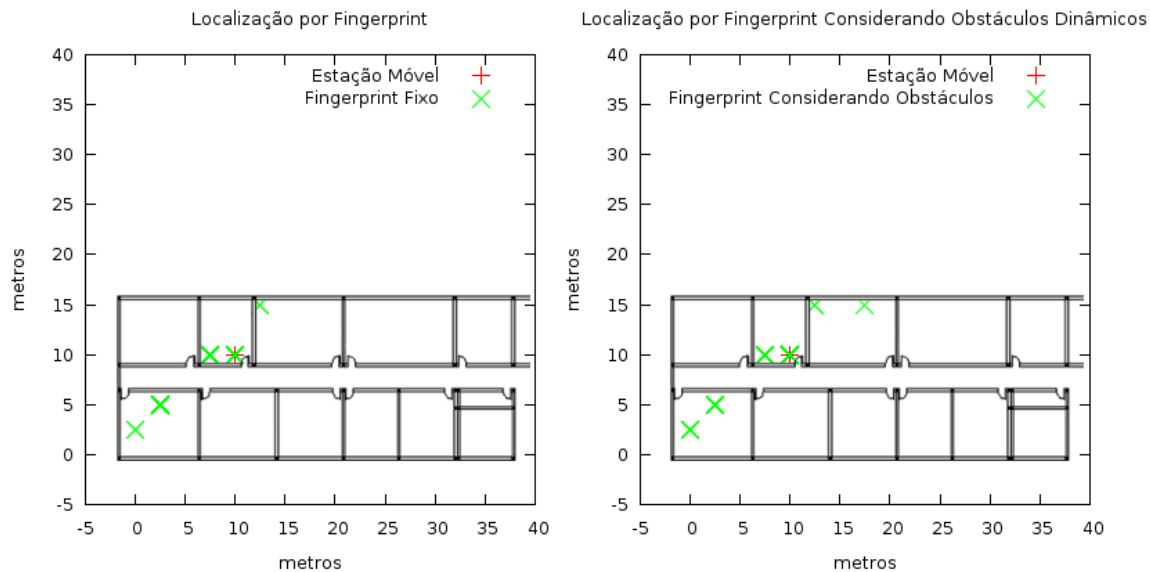


Figura 6.11: Situação 2a - Comparativo entre as Técnicas de *Fingerprint* Sem Adição de Obstáculo

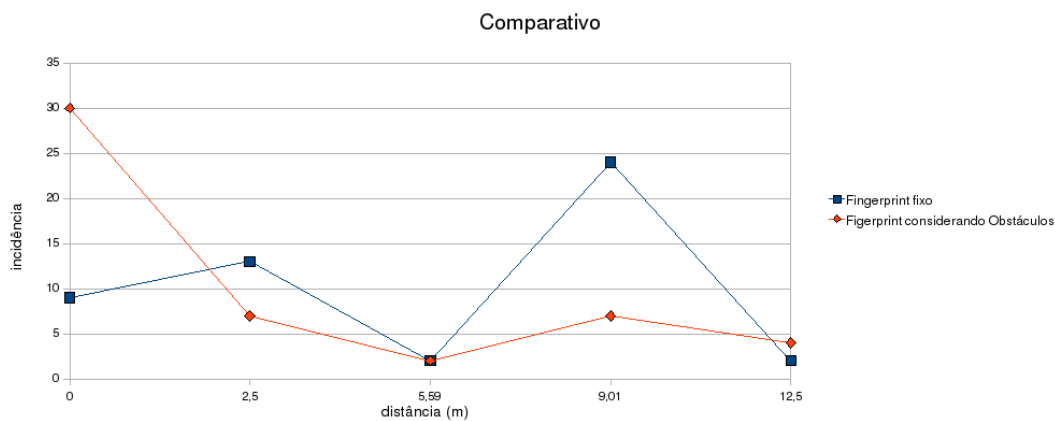


Figura 6.12: Situação 2a - Precisão das Técnicas

Comparando-se as técnicas identifica-se que a localização correta da sala ocorreu com percentual de:

- *fingerprint* fixo: 44% das ocorrências;
- *fingerprint* considerando obstáculos dinâmicos: 74% das ocorrências.

Após a realização deste levantamento com poucos obstáculos, manteve-se a posição da estação móvel e inseriu-se um obstáculo entre a estação móvel e o AP2. O obstáculo utilizado foi a grade de uma antena parabólica de  $24dB$  posicionada à frente do AP. Após medir-se o sinal, identificou-se que este obstáculo foi responsável pela queda de aproximadamente  $4dB$  da potência de sinal do AP2.

Realizou-se então novamente 50 amostras de localização e respectivas amostras de alteração de potência entre os APs. A figura 6.14 apresenta o comparativo entre as técnicas e posições apontadas por ambas como sendo a localização da estação móvel.

Nota-se que a técnica de *fingerprint* considerando obstáculos identificou um maior número de pontos de localização, porém (da mesma forma que as demais análises) para

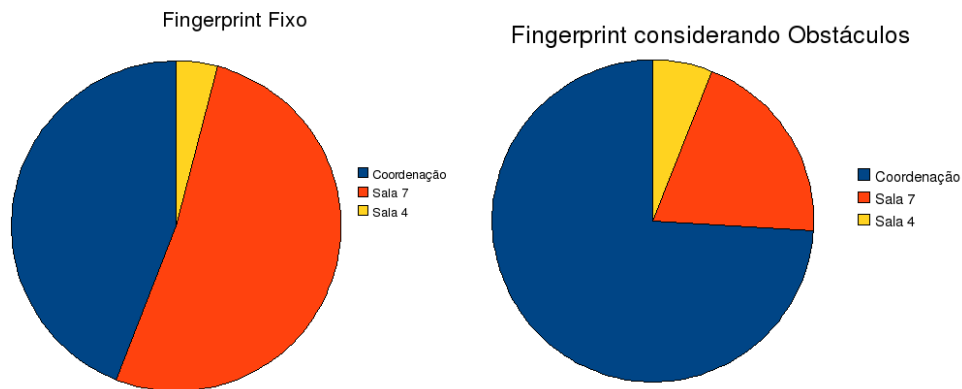


Figura 6.13: Situação 2a - Comparativo de Localização (sala)

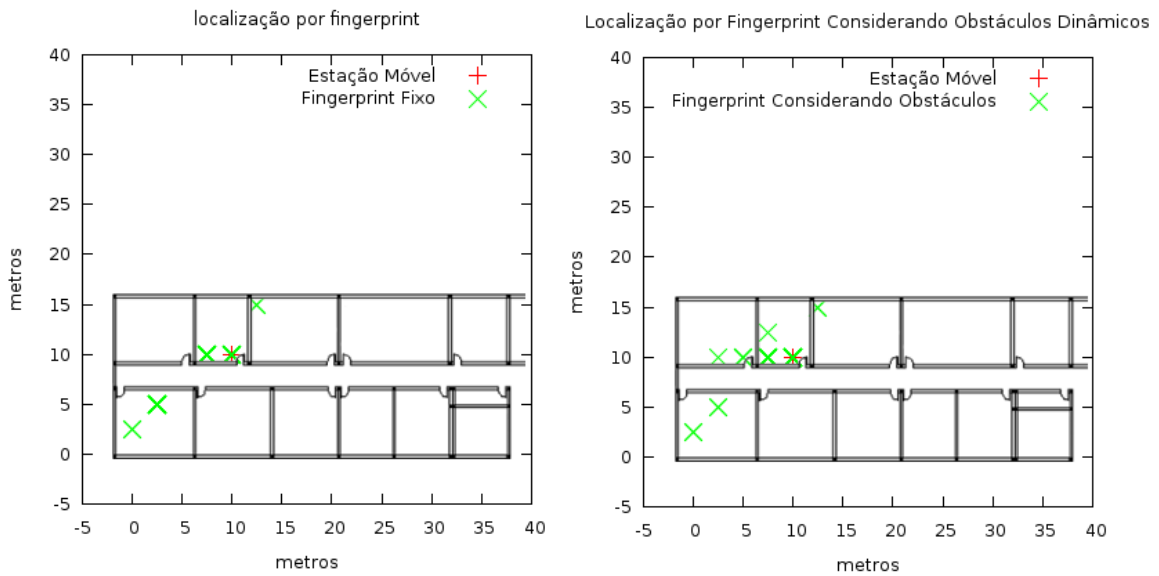


Figura 6.14: Situação 2b - Comparativo entre as Técnicas de *Fingerprint* Com Adição de Obstáculo

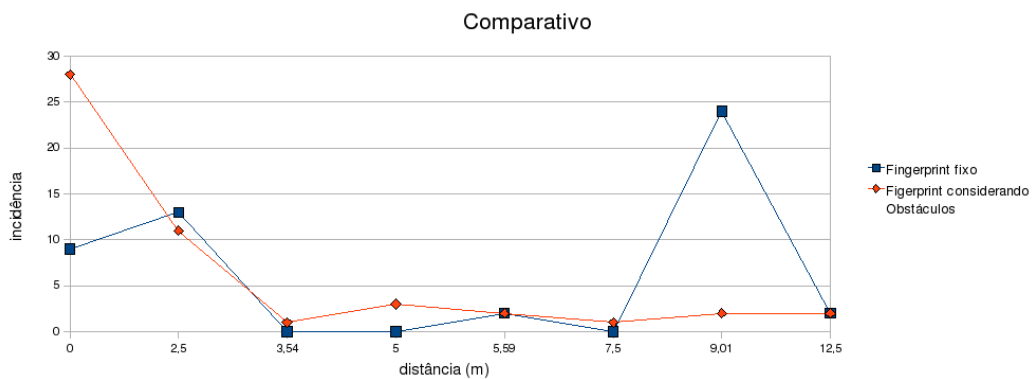


Figura 6.15: Situação 2b - Precisão das Técnicas

que se possa comparar a precisão das técnicas realizou-se a identificação do número de incidência de cada posição, conforme a figura 6.15.

Comparando-se as técnicas identifica-se que o erro médio nesta situação fica:

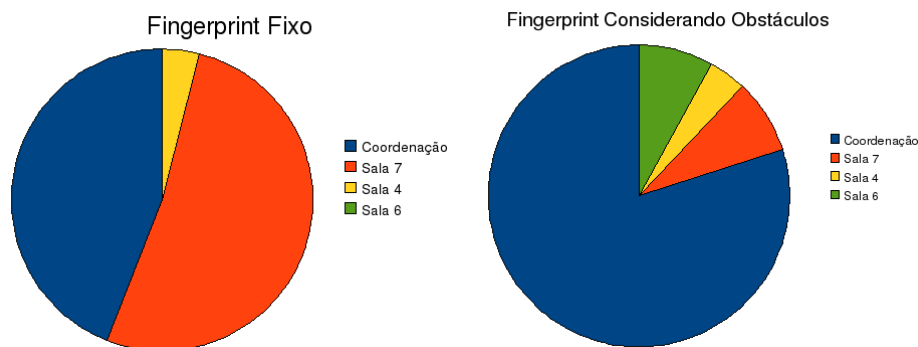


Figura 6.16: Situação 2b - Comparativo de Localização (sala)

- *fingerprint* fixo: 5,7m;
- *fingerprint* considerando obstáculos dinâmicos: 2,15m.

Comparando-se as técnicas, conforme apresentado na figura 6.16 identifica-se que a localização correta da sala ocorreu com percentual de:

- *fingerprint* fixo: 44% das ocorrências;
- *fingerprint* considerando obstáculos dinâmicos: 80% das ocorrências.

## 6.5 Situação 3 - Cenário Com Obstáculo Dinâmicos em Período de Aula

A situação 3 foi levantada durante o período normal de aula, o qual apresenta o maior número de obstáculos dinâmicos presentes no cenário de testes. Foram realizadas 50 amostras de localização da estação e as respectivas amostras de alteração de potência entre os APs.

A estação móvel foi posicionada na sala 5 e o resultado da utilização das técnicas para sua localização é apresentado na figura 6.17.

Nesta situação, um número menor de posições foi apontado pelas técnicas, sendo o comparativo de precisão apresentado na figura 6.18.

Comparando-se as técnicas identifica-se que o erro médio nesta situação fica:

- *fingerprint* fixo: 2,63m;
- *fingerprint* considerando obstáculos dinâmicos: 4,55m.

Nota-se que o maior erro da precisão na técnica de *fingerprint* considerando obstáculos dinâmicos ocorre devido ao fato de ter localizado a estação móvel em 23% das ocorrências na sala 4 (ponto distante 16m de onde a estação se encontra). Esta técnica porém localizou a sala correta da estação móvel com maior frequência que a técnica de *fingerprint* fixo, conforme apresenta a figura 6.19. A localização correta da sala ocorreu com percentual de:

- *fingerprint* fixo: 12% das ocorrências;
- *fingerprint* considerando obstáculos dinâmicos: 40% das ocorrências.

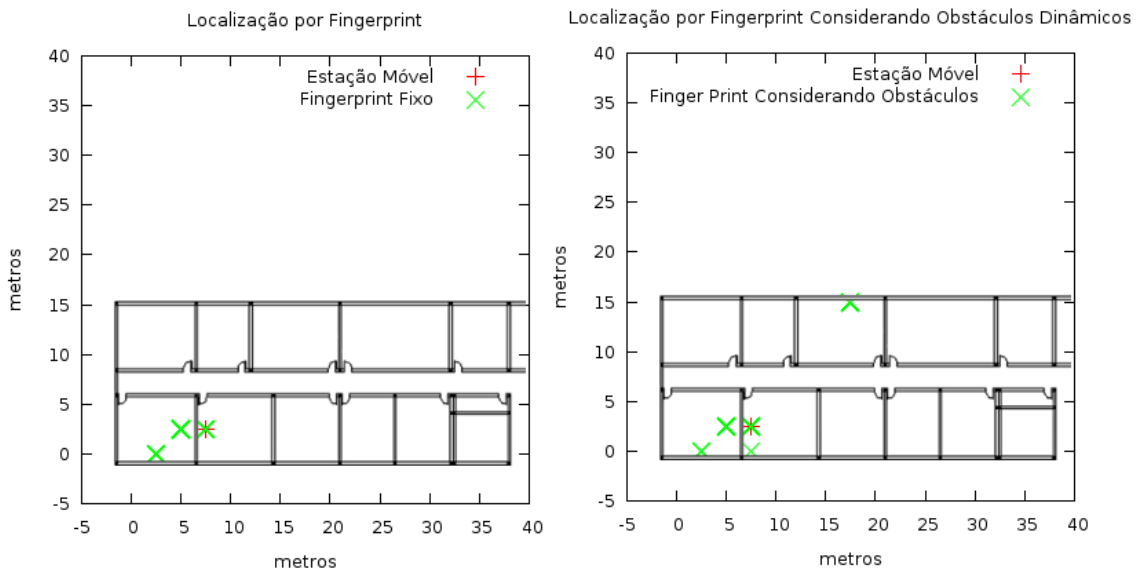


Figura 6.17: Situação 3 - Comparativo entre as Técnicas de *Fingerprint*

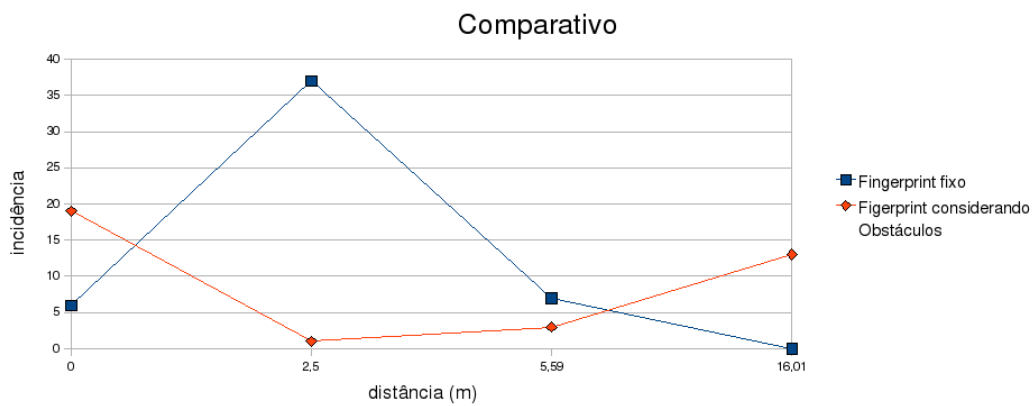


Figura 6.18: Situação 3 - Precisão das Técnicas

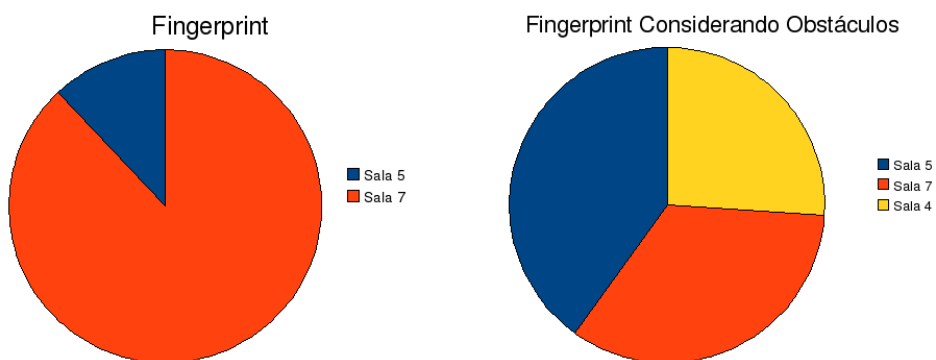


Figura 6.19: Situação 3 - Comparativo de Localização (sala)

## 6.6 Compilação dos Resultados Obtidos

Diversos outros testes foram realizados, com o objetivo de validar a técnica proposta. Todos os testes acabam fornecendo resultados similares a um dos três cenários apresen-

tados anteriormente. Considerando esta situação, compilou-se os resultados obtidos de forma a apresentar um resumo da assertividade da técnica.

A tabela 6.1 apresenta a compilação dos erros encontrados na técnica de *fingerprint* (*FP*) e na técnica de *fingerprint* considerando obstáculos dinâmicos (*FPOD*) desenvolvida. Nela é possível identificar o erro médio de localização em metros, e assertividade na identificação da sala na qual a estação móvel se encontra no momento da localização. Para cada situação analisada, é descrito o número de localizações realizadas, e para cada localização, o número de amostras de potência utilizados. Totalizou-se 230 localizações, tendo para cada uma 50 amostras de potência. O total de amostras de potência analisadas foi de 46000 amostras.

Tabela 6.1: Compilação dos Resultados Obtidos

<b>Técnica / Situação</b>	<b>Nro Localizações</b>	<b>Amostras de pot. por Loc.</b>	<b>FP erro</b>	<b>FPOD erro</b>	<b>FP id. da sala</b>	<b>FPOD id. da sala</b>
Situação 1	80	50	2,71m	3,48m	100%	100%
Situação 2a	50	50	5,7m	2,84m	44%	74%
Situação 2b	50	50	5,7m	2,15m	44%	80%
Situação 3	50	50	2,63m	4,55m	12%	40%
<b>Total</b>	<b>230</b>	<b>46000</b>	-	-	-	-
<b>Média</b>	-	-	<b>4,19m</b>	<b>3,26m</b>	<b>50%</b>	<b>73,5%</b>

Têm-se então uma diminuição média de erro de aproximadamente 1m, e um acréscimo na assertividade da identificação da sala na qual a estação móvel se encontra de aproximadamente 23% ao se utilizar a técnica desenvolvida.

## 7 CONCLUSÕES

O objetivo primordial desta tese é o desenvolvimento de um mecanismo capaz de realizar a localização de estações móveis em um ambiente *indoor* com uma precisão suficiente para que se possa identificar a sala na qual a mesma se encontra. A partir desta informação, o mecanismo deve ser capaz de realizar alterações em outros mecanismos de segurança de acordo com uma política baseada em posição física. Este processo está inserido na autenticação das estações, tendo em vista que se deseja a reconfiguração dinâmica dos mecanismos de segurança antes que a estação se associe à rede.

Pode-se então, a partir do sistema, criar-se uma política baseada nos dados mais usuais de autenticação (usuário, senha, horário de associação, etc) somando-se a eles a posição física na qual a estação se encontra.

Uma avaliação do processo de localização das estações desenvolvido e da forma de autenticação é realizada nas próximas seções.

### 7.1 Em relação à Localização das Estações Móveis

Atualmente diversos esforços tem sido despendidos na criação de mecanismos capazes de localizar estações móveis. Dentre os modelos desenvolvidos, trabalhou-se especificamente na localização baseada em informações de potência de sinal. Isto se deve ao fato da facilidade que os dispositivos móveis possuem em obter esta informação, sem a necessidade de alterações significativas ou adição de *hardware* específico nas estações e APs.

Também considerou-se a não adição de estações ou equipamentos extras na infraestrutura da rede, o que acarreta no acréscimo de gerência e garantia de disponibilidade destes equipamentos, além do custo financeiro envolvido na inclusão dos mesmos.

Muito tem-se criticado a utilização de potência de sinal no processo de localização. Estas críticas tem como base a grande variação destes valores em um ambiente de produção, devido a interferências de sinal, atenuação causada por obstáculos dinâmicos e até mesmo a mudanças de temperatura. Isto faz com que sistemas baseados unicamente em triangulação de potência e/ou tabelas estáticas (*fingerprint*) não sejam adequadas para este tipo de mecanismo.

Considerando estas críticas, partiu-se para um mecanismo que contasse com a facilidade de obtenção dos valores de potência, mas que ao mesmo tempo considerasse as variações do valor obtido devido à dinamicidade do ambiente.

Partiu-se então para a construção de um mecanismo que pudesse dinamicamente adaptar-se ao ambiente utilizando apenas os equipamentos lá existentes. Obviamente a necessidade de diversos APs para que o sistema aqui desenvolvido se torne operacional pode ser considerada como um custo extra à infra-estrutura. Porém deve-se considerar



que estes equipamentos são também uma necessidade para garantir que a área de abrangência da rede seja adequada no tipo de ambiente ao qual o trabalho se propõe. Além disso, os equipamentos utilizados não apresentam nenhuma funcionalidade incomum nos dispositivos comercializados (mesmo os de menor custo).

Teve-se então à disposição os APs já disponíveis quando do início do projeto, um servidor capaz de armazenar o sistema de localização, e um mecanismo de *proxy* já adaptado à necessidade do projeto. Com estes recursos teve início o desenvolvimento do protótipo.

Ao final da construção do sistema, pode-se considerar que o mesmo conseguiu de forma satisfatória atingir os objetivos iniciais de aprimorar a precisão da localização das estações móveis com resultados significativos. Também comprovou-se a grande influência que os obstáculos dinâmicos possuem sobre a abrangência da rede (através da variação de potência) e no processo de localização de estações.

## 7.2 Em relação à Autenticação das Estações

O sistema desenvolvido, tendo a localização de estações móveis como base, funciona como um mecanismo adicional ao processo de autenticação de estações.

O processo de autenticação deve fornecer informações aos sistemas capazes de garantir a identidade de um determinado usuário/sistema para que a partir desta identidade possa realizar as ações adequadas. Estas ações, no caso deste trabalho, dizem respeito ao acesso à rede. Deve-se garantir então que em nenhum momento um usuário malicioso possa fazer-se passar por outro usuário, burlando o processo de autenticação.

Em um ambiente sem fios existem alguns mecanismos capazes de realizar a autenticação de usuários e garantia de confidencialidade das informações trafegadas na rede (como o protocolo 802.11i e o protocolo 802.1x). A utilização do protocolo 802.1x, por exemplo, possui mecanismos de troca de informações de usuário/senha ou certificados digitais, utilizando-se de protocolos de cifragem de dados em trânsito considerados atualmente como sendo bastante seguros. Apesar da análise da segurança do 802.1x não ser o foco deste trabalho, considera-se que a correta configuração do mesmo, utilizando certificados digitais tanto no cliente quanto no serviço de autenticação, protegidos por senhas complexas seja suficiente para a garantia da identificação de um determinado usuário.

Preocupa, no entanto, a inexistência de um mecanismo capaz de verificar de onde (posição física) está sendo feito o acesso à rede. Focando-se nesta necessidade que se desenvolveu o sistema apresentado.

A partir da união dos mecanismos existentes, pode-se então criar uma política de segurança (seja de uso de recursos, ou de acesso à um determinado sistema) baseando-se na identificação inicial do usuário (através de um mecanismo de autenticação como o 802.1x) e posteriormente verificando a localização do mesmo. Conforme o local do acesso pode-se restringir totalmente, parcialmente, ou garantir-se o acesso.

Conforme apresentado na seção anterior, o sistema obteve êxito no acréscimo de precisão na localização das estações móveis. Apesar disso, ainda não se considera adequada a utilização da técnica desenvolvida como sendo viável em sistemas que carecem da localização da estação para adequar a segurança em ambientes críticos. Salienta-se neste caso que não se obteve uma precisão totalmente confiável em todas as amostras realizadas.

Deve-se então considerar a continuidade da pesquisa adicionando à mesma novas técnicas a análises como incremento da mesma. As sugestões de trabalhos futuros são apresentadas na próxima seção.

### 7.3 Trabalhos Futuros

O mecanismo desenvolvido neste trabalho não pode ser considerado como tendo esgotado o assunto abordado. Foi apresentado um novo modelo de localização no qual, com os recursos existentes na infra-estrutura da rede, consegue-se adaptar a localização de estações de acordo com as variações de potência.

Sabe-se que existe uma variação significativa nos valores obtidos da potência de sinal de acordo com as antenas utilizadas na comunicação. O próprio ângulo no qual a antena da estação móvel, ou antena do AP, se encontra em um determinado momento pode ser fonte de variação. Esta variação no entanto não foi considerada no presente trabalho.

A análise do impacto do uso de diferentes antenas, e a adaptação do sistema para considerar esta variação são fontes para possíveis trabalhos que venham a dar continuidade a esta pesquisa.

Outro fator importante que poderia ser desenvolvido no futuro é a interligação do mecanismo de localização desenvolvido com o protocolo 802.1x. Sabe-se que este é um protocolo bastante flexível, capaz de englobar a localização como sendo parte do processo de autenticação.

Ademais, outro aspecto que pode ser fonte de novos estudos, e pode ser apontado como um ponto fraco no protótipo desenvolvido, é a necessidade de obrigar-se a estação móvel a conectar-se a mais de um AP para que se possa verificar as informações de potência da mesma. Isto se deve ao fato de que os APs só informam a potência das estações clientes que estão diretamente associadas a ele, não monitorando as demais. A utilização de outros modelos de AP, ou o desenvolvimento de um *software AP* (colocação da interface de redes sem fios em um computador em modo *master*, tornando-o um AP) capaz de identificar a potência de clientes não associados, mas mantendo a funcionalidade de AP, seria de grande contribuição ao mecanismo.

Além disso, todo e qualquer estudo que foque na identificação de fatores no ambiente capazes de alterar a potência do sinal, e que sejam passíveis de se incluir ao sistema, seriam de grande interesse ao mecanismo desenvolvido.

## REFERÊNCIAS

- 3COM. **3Com Wireless Antennas Product Guide**. Disponível por: [http://www.3com.com/other/pdfs/products/en\\_US/101900.pdf](http://www.3com.com/other/pdfs/products/en_US/101900.pdf) (07/2008).
- ALLIANCE, W.-F. **Wi-Fi Protected Access: strong, standards-based, interoperable security for today's wi-fi networks**. Disponível por: [http://www.wi-fi.org/white\\_papers/whitepaper\\_042903\\_wpa](http://www.wi-fi.org/white_papers/whitepaper_042903_wpa)(01/2004).
- ALLIANCE, W.-F. **Deploying Wi-Fi Protected Access (WPATM) and WPA2TM in the Enterprise**. Disponível por: <http://www.wi-fi.org/files/wp9WPA-WPA2>(10/2006).
- ANDERSON, J. B. **Digital Transmission Engineering**. [S.l.]: Wiley-IEEE, 2006.
- APRIL, P.; CARMEL, A.; GRÉGOIRE, B.; HORVÁTH, M.; JANES, R.; LECLERC, P.; NAGUIB, M.; PROULX, F.; LENCZNER, M.; JONES, R. **Wifidog Captive Portal**. Disponível por: <http://dev.wifidog.org> (03/2008).
- BAHL, P.; BALACHANDRAN, A.; PADMANABHAN, V. **Enhancements to the RADAR User Location and Tracking System**. Disponível por: <http://citeseer.ist.psu.edu/bahl00enhancements.html> (04/2004).
- BARDWELL, J. **'I'm Going To Let My Chauffer Answer That' - Math and Physics for the 802.11 Wireless LAN Engineer**. Disponível por: [http://www.connect802.com/download/techpubs/2004/my\\_chauffeur\\_BD0414.pdf](http://www.connect802.com/download/techpubs/2004/my_chauffeur_BD0414.pdf)(01/2004).
- BUSCHMANN, C.; H.HELLBRÜCK; S.FISCHER; KRÖLLER, A.; FEKETE, S. Radio propagation-aware distance estimation based on neighborhood comparison. In: EUROPEAN WORKSHOP ON SENSOR NETWORKS, 2007. **Anais...** [S.l.: s.n.], 2007. p.325–340. (Springer Lecture Notes in Computer Science, v.4373).
- CAPKUN, S.; HUBAUX, J.-P. Secure Positioning in Wireless Networks. **IEEE Journal on Selected Areas in Communications (JSAC)**, [S.l.], v.24, n.2, p.221–232, 2006.
- FARIA, D. B. Modeling Signal Attenuation in IEEE 802.11 Wireless LANs - Vol. 1. **Technical Report TR-KP06-0118, Kiwi Project, Stanford University**, [S.l.], 2005. Disponível por: <http://www-cs-students.stanford.edu/dbfaria/files/faria-TR-KP06-0118.pdf> (07/2008).
- FETTE, B.; AIELLO, R.; CHANDRA, P.; DOBKIN, D. M.; BENSKEY, A.; MIRON, D.; LIDE, D. A.; DOWLA, F.; OLEXA, R. **RF and Wireless Technologies**. [S.l.]: Elsevier Inc., 2008.

FLUHRER, S.; MANTIN, I.; SHAMIR, A. Weaknesses in the Key Scheduling Algorithm of RC4. **Lecture Notes in Computer Science**, [S.l.], v.2259, 2001. Disponível por: <http://citeseer.ist.psu.edu/fluhrer01weaknesses.html> (01/2003).

FUSCO, V. F. **Teoria e técnicas de antenas: princípios e prática**. [S.l.]: Bookman, 2006.

GAST, M. **802.11 Wireless Networks: the definitive guide**. [S.l.]: O'Reilly and Associates, Inc. Sebastopol, CA, 2002.

IEEE. **IEEE Standards for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: wireless lan medium access control (mac) and physical layer (phy) specifications**. Disponível por: <http://standards.ieee.org/getieee802/download/802.11-1999.pdf> (06/2003).

IEEE. **IEEE 802.11b - Part 11: wireless lan medium access control (mac) and physical layer (phy) specifications: higher-speed physical layer extension in the 2.4 ghz band**. Disponível por: <http://standards.ieee.org/getieee802/download/802.11b-1999.pdf> (06/2003).

IEEE. **IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: wireless lan medium access control (mac) and physical layer (phy) specifications - amendment 1: high-speed physical layer in the 5 ghz band**. Disponível por: <http://standards.ieee.org/getieee802/download/802.11a-1999.pdf> (06/2003).

IEEE. **IEEE 802.11g Part 11: wireless lan medium access control (mac) and physical layer (phy) specifications amendment 4: further higher data rate extension in the 2.4 ghz band**. Disponível por: <http://standards.ieee.org/getieee802/download/802.11g-2003.pdf> (12/2003).

IEEE. **IEEE 802.11i Part 11: wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: medium access control (mac) security enhancements**. Disponível por: <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf> (10/2004).

ITU, I. T. U. **ITU Terrestrial Services FAQ**. Disponível por: <http://www.itu.int/ITU-R/terrestrial/faq/index.htmlg013> (06/2003).

KITASUKA, T.; NAKANISHI, T.; FUKUDA, A. Wireless LAN Based Indoor Positioning System WiPS and Its Simulation. **Communications, Computers and signal Processing**, [S.l.], v.1, n.28, p.272–275, 2003. Disponível por: <http://citeseer.ist.psu.edu/kitasuka03wireless.html> (08/2004).

KRAUS, J. D. **Antenas**. [S.l.]: Guanabara Koogan SA, 1950.

KRISHNAN, P.; KRISHNAKUMAR, A. S.; JU, W.-H.; MALLOWS, C.; GANU, S. A System for LEASE: location estimation assisted by stationery emitters for indoor rf wireless networks. **Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies**, [S.l.], v.2, n.7, p.1001–1011, 2004. Disponível por: <http://citeseer.ist.psu.edu/krishnan04system.html> (03/2005).

KUWABARA, M.; NISHIO, N. Wi-Fi based radio map for location sensing by hypothesizing existence of barriers. In: ICUIMC '09: PROCEEDINGS OF THE 3RD INTERNATIONAL CONFERENCE ON UBIQUITOUS INFORMATION MANAGEMENT AND COMMUNICATION, 2009, New York, NY, USA. **Anais...** ACM, 2009. p.12–17.

MORAES, L. F. M. de; NUNES, B. A. A. Calibration-free WLAN location system based on dynamic mapping of signal strength. In: MOBIWAC '06: PROCEEDINGS OF THE 4TH ACM INTERNATIONAL WORKSHOP ON MOBILITY MANAGEMENT AND WIRELESS ACCESS, 2006, New York, NY, USA. **Anais...** ACM, 2006. p.92–99.

MORRISON, J. D. **IEEE 802.11 wireless local area network security through location authentication.** Disponível por: [http://cistr.nps.edu/downloads/theses/02thesis\\_morrison.pdf](http://cistr.nps.edu/downloads/theses/02thesis_morrison.pdf) (01/2003).

MOSKOWITZ, R.; FLEISHMAN, G. **Weakness in Passphrase Choice in WPA Interface.** Disponível por: <http://wifinetnews.com/archives/002452.html> (01/2004).

NIST. **Announcing the ADVANCED ENCRYPTION STANDARD (AES).** Disponível por: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf> (01/2004).

OLSR.ORG. **OLSR - Open Link State Routing Protocol.** Disponível por: <http://www.olsr.org> (05/2005).

OPPENHEIMER, P.; BARDWELL, J. **Troubleshooting Campus Networks:** practical analysis of cisco and lan protocols. [S.l.]: John Wiley and Sons, 2002.

PANDEY, S.; KIM, B.; ANJUM, F.; AGRAWAL, F. Client assisted location data acquisition scheme for secure enterprise wireless networks. In: ACM, 2005. **Anais...** [S.l.: s.n.], 2005. v.2, p.1174–1179. Disponível por: [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=1424675](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1424675).

PERES, A.; WEBER, R. F. IEEE 802.11 wireless location and network security mechanism through fingerprint, triangulation and dynamic obstacle identification. In: INTERNATIONAL CONFERENCE ON WIRELESS COMMUNICATIONS AND MOBILE COMPUTING, 2009. **Anais...** [S.l.: s.n.], 2009.

PERES, A.; WEBER, R. F. Network Security Through Wireless Location. In: LANOMS 2009 PROCEEDINGS, 2009. **Anais...** [S.l.: s.n.], 2009.

SAYED, A.; TARIGHAT, A.; KHAJEHNOURI, N. Network-based wireless location: challenges faced in developing techniques for accurate wireless location information. **IEEE Signal Processing Magazine**, [S.l.], v.22, n.4, p.24–40, 2005.

SAYRE, C. W. **Complete Wireless Design.** [S.l.]: McGraw-Hill, 2001.

SMITH, C.; GERVELIS, C. **Wireless Network Performance Handbook.** [S.l.]: McGraw-Hill Professional, 2003.

SMITH, W. D. **1. AES seems weak. 2. Linear time secure cryptography.** Disponível por: <http://eprint.iacr.org/> (01/2008), Cryptology ePrint Archive, Report 2007/248.

STOYANOVA, T.; KERASIOTIS, F.; PRAYATI, A.; PAPADOPOULOS, G. Evaluation of impact factors on RSS accuracy for localization and tracking applications. In: **MOBIWAC '07: PROCEEDINGS OF THE 5TH ACM INTERNATIONAL WORKSHOP ON MOBILITY MANAGEMENT AND WIRELESS ACCESS**, 2007. **Anais...** ACM, 2007. p.9–16. Disponível por: <http://dx.doi.org/10.1145/1298091.1298094>.

TAHERI, A.; SINGH, A.; EMMANUEL, A. Location fingerprinting on infrastructure 802.11 wireless local area networks (WLANs) using Locus. In: **ANUAL IEEE INTERNATIONAL CONFERENCE - LOCAL COMPUTER NETWORKS**, 29., 2004. **Proceedings...** [S.l.: s.n.], 2004. p.676–683.

THOMPSON, A.; TAYLOR, B. N. **Guide for the Use of the International System of Units (SI)**. Disponível por: <http://physics.nist.gov/cuu/pdf/sp811.pdf> (01/2009).

WALKE, B. H.; MANGOLD, S.; BERLEMANN, L. **IEEE 802 Wireless Systems Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence**. [S.l.]: John Wiley & Sons Inc, 2006.

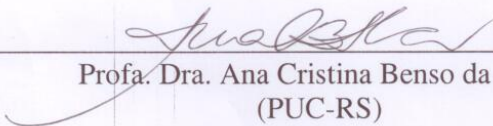
YASAR, A.-U.-H.; ANSARI, M. A.; FAROOQUI, S. Low cost solution for location determination of mobile nodes in a wireless local area network. In: **ACE '06: PROCEEDINGS OF THE 2006 ACM SIGCHI INTERNATIONAL CONFERENCE ON ADVANCES IN COMPUTER ENTERTAINMENT TECHNOLOGY**, 2006, New York, NY, USA. **Anais...** ACM, 2006. p.75.

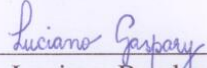
“Mecanismo de Autenticação Baseado na Localização de Estações Sem Fios  
Padrão IEEE 802.11”

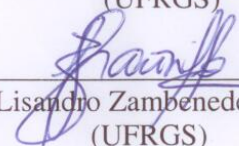
por

**André Peres**

Tese apresentada aos Senhores:

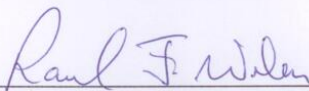
  
\_\_\_\_\_  
Profa. Dra. Ana Cristina Benso da Silva  
(PUC-RS)

  
\_\_\_\_\_  
Prof. Dr. Luciano Paschoal Gaspar  
(UFRGS)

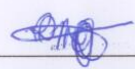
  
\_\_\_\_\_  
Prof. Dr. Lisandro Zambenedetti Granville  
(UFRGS)

Vista e permitida a impressão.

Porto Alegre, \_\_\_/\_\_\_/\_\_\_

  
\_\_\_\_\_  
Prof. Dr. Raul Fernando Weber

Orientador

  
\_\_\_\_\_  
P/ Prof. Alvaro Freitas Moreira  
Coordenador do Programa de  
Pós-Graduação em Computação - PPGC  
Instituto de Informática - UFRGS