UM SISTEMA DE LOCALIZAÇÃO PARA REDES WI-FI BASEADO EM NÍVEIS DE SINAL E MODELO REFERENCIADO DE PROPAGAÇÃO

Bruno Astuto Arouche Nunes

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Aprovada por:

Prof. Luís Felipe Magalhães de Moraes, Ph. D.

Prof. Cláudio Luis de Amorim, Ph. D.

Prof. Edison Ishikawa, D.Sc.

RIO DE JANEIRO, RJ - BRASIL

MAIO DE 2006

AROUCHE NUNES, BRUNO ASTUTO

Um Sistema de Localização para Redes Wi-Fi Baseado em Níveis de Sinal e Modelo Referenciado de Propagação [Rio de Janeiro] 2006

XIV, 81 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 2006)

Dissertação - Universidade Federal do Rio de Janeiro, COPPE

1. Redes Locais Sem Fio
2. Modelos de Localização
3. Modelos de Propagação de Sinal
4. Serviços Baseados em Localização

I. COPPE/UFRJ II. Título (série)

Dedicatória

Dedico esse trabalho a quem sempre fez de tudo para que eu apenas me preocupasse com os estudos. A quem sempre esteve ao meu lado em tudo. A quem sempre soube o que dizer em meus momentos de dúvida. A quem eu sempre recorro quando devo decidir sobre que rumo tomar em minha vida e/ou minha carreira. A quem nunca me disse o que fazer, mas sempre me ensinou como agir. Por isso e mais, dedico esse trabalho a Marcos Arouche Nunes, meu pai.

Agradecimentos

Aos meus pais Marcos e Miriam, ao meu irmão Rafael, bem como, a toda a minha família, por todo amor e carinho, não só durante a realização deste trabalho, como na vida inteira. Agradecimento mais que especial ao meu pai, pelo apoio, amor e preocupação, sempre. Sem você eu não teria conseguido.

Agradeço a Fernanda o amor e carinho dedicado a mim durante o tempo em que estive realizando esse trabalho. Obrigado pelos bons momentos e pela paciência nos momentos mais difíceis.

Agradeço a todos os amigos que conheci durante este período na COPPE. Agradecimento especial aos amigos Airon, Beto, Eduardo, Marcos Cesar e Paulo não só pelos ensinamentos transmitidos, bate-papos e longas trocas de idéias sobre tese, como também pelo seu companheirismo e amizade. Agradeço também ao Rafael Fernandes pela força na programação.

Agradeço ao meu orientador, Prof. Luís Felipe pelo apoio ao trabalho e aos demais integrantes da banca, os Professores Cláudio Luis de Amorim e Edison Ishikawa, pela valiosa contribuição nesta fase final.

À Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ) e à FINEP pelo financiamento da pesquisa e ao Programa de Engenharia de Sistemas e Computação (PESC/COPPE/UFRJ), pelo apoio operacional.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

UM SISTEMA DE LOCALIZAÇÃO PARA REDES WI-FI BASEADO EM NÍVEIS DE SINAL E MODELO REFERENCIADO DE PROPAGAÇÃO

Bruno Astuto Arouche Nunes

Maio/2006

Orientador: Luís Felipe Magalhães de Moraes

Programa: Engenharia de Sistemas e Computação

Serviços baseados em localização, aplicados no contexto de redes sem fio, têm sido alvo de pesquisas recentes, uma vez que abrem perspectivas para novas aplicações e agregam valor a estas redes. Neste tipo de aplicação, serviços podem ser oferecidos ao usuário de forma que parâmetros de entrada e/ou a saída sejam diretamente influenciados pela sua posição física. Esta é uma área de atuação muito abrangente, onde os problemas relacionados a localização e posicionamento podem ser atacados de diferentes formas, dependendo da aplicação, precisão desejada e ambiente onde o serviço deve ser implementado. Neste trabalho é proposto um sistema de localização de dispositivos para redes locais sem fio, baseado nas características de rádio freqüência destas redes. Assim, procura-se contribuir para a pesquisa na área abordando-se diversos aspectos de um sistema de localização, através de uma arquitetura baseada em sniffers sem fio e com a construção de um modelo de localização que utiliza modelos de propagação de sinal, cujos parâmetros são calculados dinamicamente e em tempo real. Isso garante ao sistema proposto considerável auto-suficiência, pois ele não necessita de intervenção humana, tanto da parte do administrador da rede, quanto do usuário. Além disso, foi implementado e testado, em um ambiente real um método probabilístico proposto para estimar a posição de um dispositivo sem fio.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

A LOCATION SYSTEM FOR WI-FI NETWORKS BASED ON SIGNAL STRENGTH AND REFERENCED PROPAGATION MODELS Bruno Astuto Arouche Nunes

May/2006

Advisor: Luís Felipe Magalhães de Moraes

Department: Systems Engineering and Computer Science

Location based services, applied in the context of wireless local area networks are being studied in recent researches, once they open new perspectives for new applications and aggregate value to such networks. In this sort of application some service is provided, where input and output parameters are directly influenced by the user's physical location. In this work we present a system for locating wireless local area network devices, based on the radio frequency characteristics of such networks. Thus, we addressed issues related to some aspects of location systems through, an architecture based on wireless sniffers and by constructing a location model based on signal propagation models, in which its parameters are calculated in real time. This guarantee a considerable self-sufficiency and adaptation capacity to the proposed system, once it does not need human intervention to work, neither from the network administrator or the wireless user being located. Moreover, a probabilistic method was used for estimating wireless devices positions, based on the previous constructed model. We later demonstrate the feasibility of our approach by reporting results of field tests in which the proposed technique was implemented and validated in a real-world indoor environment.

Lista de Acrônimos

AP	:	*Access Point*;
BS	:	*Base Station*;
BSS	:	*Basic Service Set*;
EE	:	Emissores Estacionários;
IBSS	:	*Independent Basic Service Set*;
IC	:	Intervalo de Captura;
IDS	:	*Intrusion Detection System*;
IEEE	:	*Institute of Electrical and Electronic Engineers*;
IR	:	*Infrared*;
MAC	:	*Medium Access Control*;
MP	:	Mapa de Propagação;
PC	:	*Personal Computer*;
PCI	:	*Peripheral Component Interconnect*;
PCMCIA	:	*Personal Computer Memory Card International Association*;
PHY	:	*Physical Layer*;
RF	:	Rádio Freqüência;
RSS	:	*Received Signal Strength*;
RSSI	:	*Received Signal Strength Indicator*;
STA	:	*Station* ou Estação;
SBLs	:	Serviços Baseados em Localização;
WLAN	:	*Wireless Local Area Network*;
WMAN	:	*Wireless Metropolitan Area Network*;
WPAN	:	*Wireless Personal Area Network*;

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

ESTE capítulo apresenta uma breve introdução às comunicações sem fio e aplicações baseadas em localização para redes locais sem fio. Neste tipo de aplicação, serviços podem ser oferecidos ao usuário de forma que parâmetros de entrada e/ou a saída sejam diretamente influenciados pela sua posição física. Vários métodos e modelos de localização têm sido propostos na literatura com o objetivo de melhorar o desempenho de localizadores que determinam a posição física de um usuário da rede sem fio, tornando possível o desenvolvimento de aplicações que se utilizam desta informação. O presente trabalho foi desenvolvido sobre redes que funcionam utilizando o padrão IEEE802.11 [2], assim, a primeira seção apresenta uma visão geral sobre estas redes, junto à motivação para o trabalho. Algumas idéias para aplicações baseadas em localização serão discutidas, mostrando como a informação de posição real pode ser útil dentro do contexto de aplicações e serviços para redes sem fio. Os objetivos do presente trabalho serão resumidos na seção 1.2, seguidos por uma breve descrição de suas principais contribuições e inovações. Por fim, a estrutura do trabalho será descrita na última seção.

1.1 Motivação

Atualmente muitos estudos estão sendo desenvolvidos com relação à utilização de pontos de acesso à Internet através de redes sem fio que utilizam o padrão 802.11 [2] do IEEE (*Institute of Electrical and Electronic Engineers*). Estes pontos de acesso, também chamados de *Hotspots*, possibilitam conexão à uma rede cabeada ligada à Internet, de forma que qualquer usuário de posse de um dispositivo sem fio, que suporte o padrão 802.11, possa conectar-se à Internet e utilizar as mais variadas aplicações.

Além dos *hotspots*, empresas e organizações estão rapidamente implementando infraestruturas de redes sem fio baseadas no padrão IEEE 802.11. Este padrão é o mais amplamente difundido através da aliança internacional de fabricantes WECA (*Wireless Ethernet Compatibility Alliance*), que possui 183 companhias associadas por todo o mundo e mais de 2.000 produtos certificados Wi-Fi (*Wireless Fidelity*) [3]. Estas redes tornaram-se extremamente populares nos últimos anos. Este crescimento na popularidade das redes locais sem fio (*Wireless Local Area Networks* - WLANs) se dá junto ao crescimento do número de aplicações diversas baseadas neste tipo de tecnologia sem fio.

Alguns comentários pertinentes podem ser feitos com relação a segurança. Vulnerabilidades no WEP (*Wired Equivalent Privacy*) e no WPA (*Wi-Fi Protected Access*) [4, 5], limitações e fraquezas no controle de acesso e a própria natureza do meio de transmissão neste tipo de rede, tornaram-se tópicos de intensa investigação. Em diversos trabalhos foram discutidas estas falhas [6, 7], no entanto, em muito poucos o problema de detecção e localização física destes pontos vulneráveis foi abordado.

Tomando-se as devidas precauções, já é possível implementar uma rede sem fio tão segura quanto uma rede interligada através de cabos. Contudo, é desejável ainda localizar tentativas de acesso não autorizado e até mesmo, localizar potenciais falhas em dispositivos de usuários legítimos. O administrador da rede deve ser capaz de ter acesso a um nó da rede quando existe suspeita da existência de alguma vulnerabilidade. Em um ambiente sem fio localizar este nó pode não ser trivial, devido a

capacidade móvel/portável inerente a este tipo de ambiente. Assim, torna-se interessante o uso de mecanismos capazes de localizar dispositivos sem fio não autorizados (como por exemplo, pontos de acesso não autorizados, conhecidos também como *rogue access points*) e mesmo dispositivos autorizados e confiáveis, uma vez que estes últimos podem conter vulnerabilidades.

Além da segurança, um outro grande desafio no campo das redes sem fio é o potencial para serviços e aplicações. Atualmente, provedores de serviços para WLANs procuram expandir sua área de mercado oferecendo cada vez mais serviços diferenciados. Serviços Baseados em Localização - SBLs (ou *Location Based Services* - LBS) é uma área que vem crescendo nos últimos anos e sendo alvo de muitas pesquisas. Sistemas de localização podem ser utilizados tanto no contexto de segurança, como visto acima, quanto no contexto de alimentar uma aplicação baseada em localização com a posição do dispositivo para um determinado fim.

Desta forma, o propósito deste trabalho é propor uma técnica e um sistema de localização capaz de determinar a posição física de dispositivos sem fio, para que esta informação possa ser utilizada por outros SBLs.

SBLs aplicados a um ambiente sem fio são um nicho crescente de mercado e vem também tornando-se o tema alvo de diversas pesquisas na área acadêmica. É possível citar algumas destas aplicações como por exemplo:

- **Segurança** - Aplicações podem receber a informação da localização de um intruso na rede sem fio, como um ponto de acesso não autorizado por exemplo, e mostrar sua posição física em um mapa das instalações de uma empresa.
- **Administração** - Um administrador de rede, após identificar que uma das estações sem fio sob sua responsabilidade está apresentando problemas, deve ser capaz de saber a posição física da mesma a fim de ir até ela e realizar os reparos pertinentes.
- **Limitação de Distribuição de Conteúdo por Localização** - Caso o dispositivo não esteja dentro do perímetro da empresa, ele não pode acessar outras informações além da página Web da mesma, por exemplo.

- **Recursos mais Próximos** - Localizar a impressora sem fio mais próxima, por exemplo.

- **Museus** - Em um museu o visitante pode possuir um dispositivo sem fio (um PDA - *Personal Digital Assistant*, por exemplo) e quando o sistema de localização detectar que este visitante se aproxima de uma obra de arte, um conteúdo multimídia sobre a obra em questão poderia ser disponibilizado através do PDA para visualização. Caso o visitante queira ver alguma outra obra em particular, ele poderia ver na tela do PDA um mapa do museu marcando onde esta obra se localiza, em que posição no mapa do museu ele se encontra (esta informação seria dada pelo sistema de localização) e como chegar até o destino desejado através de indicações no mapa.

- **Shopping Centers** - É possível utilizar um sistema de localização que disponibilizasse propaganda e/ou promoções na tela do PDA de um cliente quando esse passasse em frente a vitrine de uma loja no shopping. Também seria possível uma aplicação (como a do museu) onde fosse possível saber o caminho para alguma loja em particular, apenas clicando na tela do dispositivo sem fio portátil.

- **Casa Inteligente** - Um usuário poderia andar com o "controle remoto da casa" e o sistema de localização, ao perceber que o usuário entrou em um determinado cômodo, poderia acionar um sistema automático para acender luzes, ligar/desligar equipamentos eletrônicos etc.

Outras aplicações podem ser descritas aqui, mas foge ao escopo deste trabalho discuti-las mais a fundo, uma vez que o presente irá tratar do sistema de localização em si e não de suas aplicações.

Esta é uma área de atuação muito abrangente, onde os problemas relacionados a localização e posicionamento podem ser atacados de diferentes formas, dependendo da aplicação, precisão desejada e ambiente onde o serviço deve ser implementado. Uma série de métodos, modelos e propostas de sistemas de localização serão abordados no Capítulo 2.

1.2 Objetivo do Trabalho

No presente trabalho, o que se propõe é um novo sistema capaz de detectar e localizar dispositivos sem fio, com pouca ou nenhuma intervenção humana, tanto na implantação quanto no funcionamento do mesmo. Tal sistema deverá possuir precisão semelhante aos sistemas propostos na literatura até hoje e deverá utilizar a própria infra-estrutura de WLAN já existente no local onde o sistema de localização será implantado, sem a necessidade de se adquirir hardware especializado para este fim.

O método de localização proposto neste trabalho pode ser facilmente implementado em diversas linguagens de programação e em uma séria de equipamentos de rede comumente utilizados e encontrados no mercado, como será visto no Capítulo 4. Diversos mecanismos têm sido propostos na literatura para localizar dispositivos sem fio. Estas propostas abordam sempre o problema de localização com alternativas muitas vezes de alto custo, tanto em termos de equipamentos utilizados quanto em termos de esforço/tempo dedicado de trabalho humano na implantação e no funcionamento destas soluções.

Mecanismos de localização para redes sem fio que utilizam rádio freqüência (RF), quando implantados em ambientes fechados, sofrem com uma série de problemas de propagação de sinal [8, 9, 10, 11]. Este trabalho busca também mostrar que é possível utilizar modelos de propagação [12, 13] para fins de localização física de dispositivos. Busca-se com estes modelos, inferir determinadas características do sinal de rádio em uma rede sem fio em diversos pontos do local sendo monitorado, mesmo que em um ambiente fechado (*indoor*). A partir disso, é possível estimar a posição de um dispositivo sem fio, sem grandes prejuízos a acurácia da estimativa e diminuindo os custos de implantação e manutenção presentes na grande maioria dos sistemas encontrados no mercado e na literatura.

1.3 Contribuições e Inovações

Nesta seção serão apresentadas as contribuições e inovações que este trabalho busca trazer. O método proposto será descrito em detalhes nos Capítulos 4 e 5, onde será possível vislumbrar de que forma pretende-se alcançar as melhorias mencionadas na presente seção.

1.3.1 Sistema de Localização Auto-suficiente

Foi desenvolvido um sistema de localização auto-suficiente capaz de estimar a posição de um dispositivo sem fio, sem a necessidade de intervenção humana (por parte de um administrador, por exemplo) para funcionar. Também não existe qualquer participação do usuário no processo. Assim, alguém que esteja utilizando um dispositivo sem fio não precisa instalar qualquer software ou realizar qualquer ação para saber sua posição dentro do ambiente monitorado.

1.3.2 Sistema Baseado em Sniffers Sem Fio

Sniffers são softwares que monitoram uma interface de rede e recolhem todas as informações que trafegam por ela. Uma das principais contribuições trazidas por este trabalho é a utilização de uma arquitetura baseada em *sniffers*. O *sniffer* sem fio está definido em detalhes na Seção 4.1.2. A maioria dos sistemas de localização utilizados atualmente faz uso de uma arquitetura cliente-servidor (apresentada na Seção 4.1.1). Esta arquitetura implica em transferir a responsabilidade por coletar informações sobre a rede (utilizados na estimativa de localização) para os clientes sem fio. Isso é ruim em um contexto onde não se pode presumir que uma estação sem fio, ou um ponto de acesso não autorizado envie informações para auxiliar em sua localização. Mais detalhes das implicações da utilização de *sniffers* sem fio em sistemas serão dados na Seção 4.1.2.

1.3.3 Diminuição do Esforço e do Custo de Implantação e Manutenção

Os sistemas de localização atuais, na sua grande maioria, funcionam em duas fases. Uma primeira fase de calibragem, chamada na literatura também de fase *off-line* (definida em detalhes na Seção 2.2), onde medições sobre a qualidade do sinal de RF (rádio freqüência) são realizadas em diversos pontos específicos do ambiente no qual se deseja implementar o sistema de localização. A segunda fase consiste em coletar informações do sinal recebido por um dispositivo sem fio e utilizá-las, junto com os dados colhidos na primeira fase, para localizar tal dispositivo. O problema aqui é que essa fase de calibragem pode durar várias horas e muitas vezes, quando a calibragem é concluída, ela precisa ser refeita, pois o ambiente monitorado é constantemente alterado, principalmente por pessoas [8]. Em [14] é possível ver um exemplo do alto custo de implantação e manutenção destes sistemas. Em um dos experimentos os autores levam mais de 10 (dez) horas para realizar as medições necessárias à calibragem do sistema de localização, em uma área de aproximadamente $68mX26m$. O mecanismo proposto neste trabalho não necessita do mencionado esforço inicial de calibragem, o que diminui consideravelmente a relação custo/benefício, como poderá ser visto na Seção 6.3.2.

1.3.4 Mecanismo Dinâmico de Alteração de Parâmetros de Propagação de Sinal

Modelos de propagação são tratados em detalhes em [12] e serão abordados neste texto no Capítulo 3. Foi proposto aqui um mecanismo que utiliza estes modelos para inferir determinadas características do sinal de rádio de estações 802.11, em diversos pontos do local monitorado. Este mecanismo é capaz de perceber quando a propagação do sinal no ambiente é alterada, recalculando automaticamente os parâmetros do modelo de propagação utilizado e modificando assim, as características de sinal previstas para cada ponto do local monitorado. Estes novos parâmetros são, então, utilizados pelo modelo de localização (Capítulo 5) para estimar a posição dos

dispositivos comunicantes. Tal mecanismo fornece ao sistema aqui proposto uma característica adaptativa, tornando-o mais resistente à variações de sinal que poderiam influenciar negativamente a acurácia da estimativa de posição. Estatísticas sobre a acurácia do mecanismo proposto e o impacto de variações em seus parâmetros serão apresentados na Seção 6.2.

1.3.5 Modelo para Localização

Este trabalho apresenta um modelo analítico para localização baseado em modelos probabilísticos (Capítulo 5). Para avaliar e validar a solução proposta, o sistema foi implementado, colocado em funcionamento durante vários dias e estatísticas sobre acurácia do mesmo serão apresentadas no Capítulo 6. Tal modelo proporcionou acurácia semelhante a consagrados métodos e sistemas de localização, sem a necessidade de fase de calibragem ou hardware especializado.

1.4 Estrutura do Documento

No Capítulo 2 serão apresentadas várias técnicas de localização de forma ampla, não apenas no contexto de redes WLAN. Em seguida, alguns trabalhos relacionados ao problema de localização em redes 802.11 serão discutidos através de uma revisão bibliográfica.

O Capítulo 3 apresenta o comportamento do sinal de rádio em uma WLAN mostrando a viabilidade de se utilizar determinadas características deste sinal em sistemas de localização. Modelos, métodos e ferramentas para medição de sinal neste tipo de rede são também discutidos.

O Capítulo 4 descreve, em detalhes, o sistema proposto. O método de localização é apresentado, incluindo uma definição dos componentes do sistema (*sniffers*, ponto de acesso de referência, servidor de localização e mapa de propagação) e como os mesmos interagem uns com os outros.

O Capítulo 5 apresenta o problema de estimar a localização de um dispositivo sem fio, sob um ponto de vista analítico e propõe uma solução para o mesmo. Esta é baseada em uma combinação das características do sistema proposto neste trabalho, como a utilização de *sniffers* e o recálculo dinâmico do mapa de propagação, com conhecidos conceitos matemáticos como Regra de Bayes, Probabilidades Totais, independência de variáveis aleatórias e processos estocásticos [15]. A princípio apresenta-se formalmente o problema, alvo desta pesquisa, e definem-se alguns pontos importantes para o entendimento e tratamento do mesmo. Em seguida, uma solução é dada, baseada em um modelo analítico. Por fim, métodos para melhorar a acurácia do estimador são propostos.

No Capítulo 6 os resultados quanto a acurácia do sistema serão apresentados. Comparações quantitativas e qualitativas entre o sistema proposto e outros trabalhos encontrados na literatura serão apresentadas, junto a observações, justificativas e explicações pertinentes.

O Capítulo 7 finaliza este trabalho consolidando os resultados apresentados no capítulo anterior através das conclusões e observações relevantes. As principais contribuições da tese são descritas também neste capítulo. Finalmente, algumas perspectivas para trabalhos futuros são sugeridas.

Capítulo 2

Trabalhos Relacionados

VÁRIOS métodos e modelos de localização têm sido propostos na literatura, nos últimos anos, principalmente após o ano de 2002, data da publicação do RADAR [1]. Este é o trabalho mais referenciado na literatura quando o assunto é localização em redes sem fio e será este o principal alvo de comparações com o sistema proposto no presente trabalho. Neste capítulo, algumas referências relacionadas ao tema aqui abordado serão discutidas. As classes de sistemas serão apresentadas, mostrando-se as aplicações ideais para cada classe, apontando-se prós e contras da sua utilização. Serão levados em consideração sempre, custo de implantação/utilização e aplicabilidade em um ambiente de WLAN.

2.1 Mecanismos de Localização

É possível determinar a localização de um dispositivo sem fio em dois cenários principais: utilizando uma infra-estrutura especial para posicionamento tal como *Global Positionig System* (GPS) ou modificando de alguma forma o sistema de comunicação utilizado. Apesar de ser o mecanismo de posicionamento mais popular para ambientes externos, o GPS é ineficiente em uma série de aplicações, pois apesar de possuir boa acurácia (10 metros, em alguns casos podendo chegar a precisão submétrica), seu desempenho é muito baixo em lugares fechados. Além disso, GPS demanda hardware específico. Tal equipamento teria que ser implementado em cada um dos dispositivos sem fio, o que inviabilizaria em termos de custo sua utilização em diversas aplicações.

Um outro exemplo de sistema que utiliza infra-estrutura especial para posicionamento é o *Active Badge* [16], que trouxe grande contribuição para este campo de pesquisa, em sua época. Neste mecanismo, um crachá (*badge*) usado por uma pessoa emite uma assinatura única de sinal infravermelho - IR (*Infrared*) a cada 10 segundos. Sensores dispostos em posições conhecidas captam este sinal identificador e transmitem essas informações para o software de localização. Apesar de fornecer informação de localização acurada, mecanismos baseados em sinal IR sofrem com os seguintes problemas: são pouco escaláveis devido ao alcance muito limitado do IR; incorrem em significante custo de instalação e manutenção; e apresentam baixo desempenho na presença de irradiação direta de luz solar (ambientes com janelas).

Por estas razões, torna-se muito interessante implantar mecanismos de localização que utilizem um sistema de comunicação sem fio já implantado. Assim, o foco deste trabalho é utilizar a própria infra-estrutura de WLAN já existente, em particular aquelas que seguem o padrão 802.11b (podendo ser estendia para os padrões 802.11a e 802.11g), para localizar dispositivos comunicantes sob este mesmo padrão. O sistema, então, utilizaria as propriedades do sinal de rádio freqüência (RF), no ambiente da WLAN, para inferir a posição dos dispositivos comunicantes. Esta proposta proporciona vantagens, principalmente por tratar-se de uma solução que pode

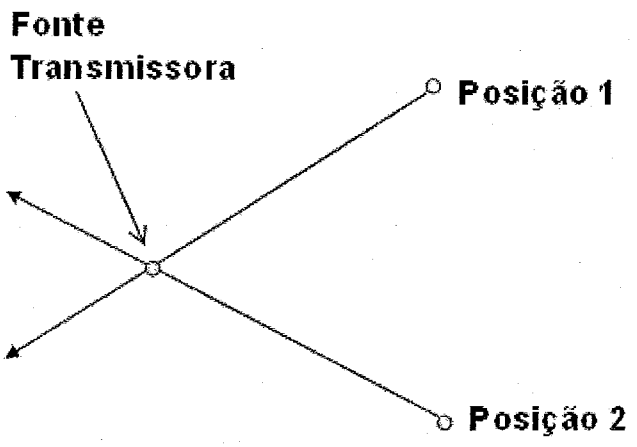

Figura 2.1: Ilustração da estimativa de posição de um transmissor a partir da medição do ângulo de chegada do sinal em duas posições distintas.

ser implementada simplesmente em software, o que reduz significativamente o custo em relação a sistemas dedicados.

Em [17] os autores comentam sobre três métodos básicos para se determinar a localização de usuários utilizando uma infra-estrutura de WLAN já existente. O primeiro é triangulação, que necessita de pelo menos três estimativas distintas da distância entre o dispositivo sem fio e algum local fixo conhecido [18].

O segundo método utiliza a direção ou ângulo de chegada do sinal (AoA - *Angle of Arrival*) medidos de pelo menos dois pontos fixos distintos. Basicamente, uma antena direcional é conectada ao receptor e a área entorno do receptor é testada para medir e marcar a partir de qual direção o sinal recebido é mais forte. Em seguida, o receptor é movido de lugar para uma segunda posição (como na Figura 2.1) e o mesmo procedimento de busca pela direção com melhor sinal é realizado. A localização da fonte transmissora é descoberta então, através de geometria básica, onde o encontro das retas que seguem as duas direções medidas é a posição do transmissor. Tais técnicas direcionais aplicam-se bem em ambientes externos, mas em ambientes fechados podem sofrer com fenômenos de multi-percurso de sinal.

O terceiro método é a utilização de esquemas de mapeamento, também conhecidos como esquemas de calibragem, ou *location fingerprinting*, ou ainda *site profiling*.

Este método baseia-se no princípio de amostrar determinadas características do sinal de rádio (neste trabalho será utilizado o nível de sinal recebido, ou *Received Signal Strength Indicator* - RSSI, definido formalmente na Seção 3.2), dependentes da localização do ponto onde tais características são aferidas. Estas características são diferentes para cada local medido, funcionando como uma impressão digital. Estas "impressões digitais" são armazenadas em um banco de dados e comparadas posteriormente com o sinal amostrado de um dispositivo sem fio que se deseja localizar. A fase de medição e registro, no banco de dados, das informações de RSSI nos diferentes locais (coordenadas [x,y]) será chamada aqui de fase de calibragem.

Um quarto método, não mencionado em [17], pode ainda ser citado aqui. Na técnica *time difference of arrival* (TDOA) o tempo de propagação do sinal de RF é medido e este valor é utilizado para estimar a posição/distância do transmissor. Esta técnica necessita de medidores de tempo capazes de resoluções de alta granularidade (ou seja, medidas de tempo muito pequenas), devido a velocidade de propagação do sinal de RF, da ordem da velocidade da luz. Problemas de multi-percurso e pequenas distâncias em ambientes fechados podem prejudicar os resultados obtidos com essa técnica.

O desenvolvimento de bibliotecas e APIs para suporte ao desenvolvimento de aplicações cliente-servidor baseadas em localização foi apresentada em [19]. Um middleware para suporte a aplicações baseadas em localização foi proposto e apresentado em [20]. Esta camada de software faz a interface entre a aplicação e o sistema de localização utilizado. No caso de [20], tal sistema foi o RADAR [1].

Atualmente, quando se fala em sistemas de localização de dispositivos sem fio em WLANs, o que se deseja são mecanismos capazes de estimar a posição do usuário em um ambiente onde se utiliza equipamentos e hardware (ex. pontos de acesso e placas sem fio) usualmente encontrados no mercado, sem a utilização de hardware adicional, com o menor custo possível e com o mínimo esforço de calibragem.

2.2 Calibragem e Fase Off-line

Como mencionado na seção anterior, define-se aqui como *fase de calibragem* a fase de medição e registro (podendo ser registro em um banco de dados) das informações de RSSI nos diferentes locais (coordenadas [x,y]) de uma malha (*grid*) que cobre um local que se deseja monitorar. Este registro de valores de RSSI para cada posição do *grid* forma então um "mapa" ou modelo, que será utilizado posteriormente na estimativa da posição de dispositivos sem fio.

Na Figura 2.2 é possível visualizar como se daria um procedimento de calibragem para um local fictício coberto por um *grid* de 10m X 10m (um ponto do grid a cada 1 metro). Neste exemplo, um local foi dividido em um *grid* onde em cada ponto do mesmo foi realizada a medição do nível de sinal RSSI (em dBm) transmitido a partir do ponto indicado como fonte transmissora. A partir dessas medições foi construído um mapa (Figura 2.2), onde cada posição do mesmo possui o valor de RSSI medido. A construção deste mapa constitui a fase de calibragem, também conhecida na literatura como fase *off-line*. Este mapa pode ser armazenado em um banco de dados ou disponibilizado de alguma outra forma para dispositivos que desejem estimar sua posição. Assim, na fase *on-line*, caso um usuário móvel esteja posicionado em algum ponto nesta área, supondo que ele esteja de posse do mapa construído na fase anterior (*off-line*), seria possível medir o valor de RSSI a partir da fonte transmissora e compará-lo com os valores contidos no mapa. Esta comparação pode ser feita de diversas formas (discutidas a seguir) e deve levar à estimativa de uma posição no mapa que mais se assemelhe à medição realizada pelo usuário na fase *on-line*. O exemplo da Figura 2.2 mostra um mapa construído com apenas uma fonte transmissora. Isso leva a *pontos redundantes*, ou seja, pontos que possuem os mesmos valores no mapa. Por exemplo, caso o sistema venha a medir, na fase *on-line*, um valor de RSSI igual a -27 dBm, ao compará-lo com o mapa criado na fase *off-line* (Figura 2.2), seriam possíveis duas posições distintas. Esse problema pode ser resolvido com a utilização de pelo menos mais duas (três no total) fontes transmissoras. Desta forma, quando se utilizam F fontes transmissoras, cada ponto no mapa passa a possuir, não um, mas F valores de nível de sinal, um para cada

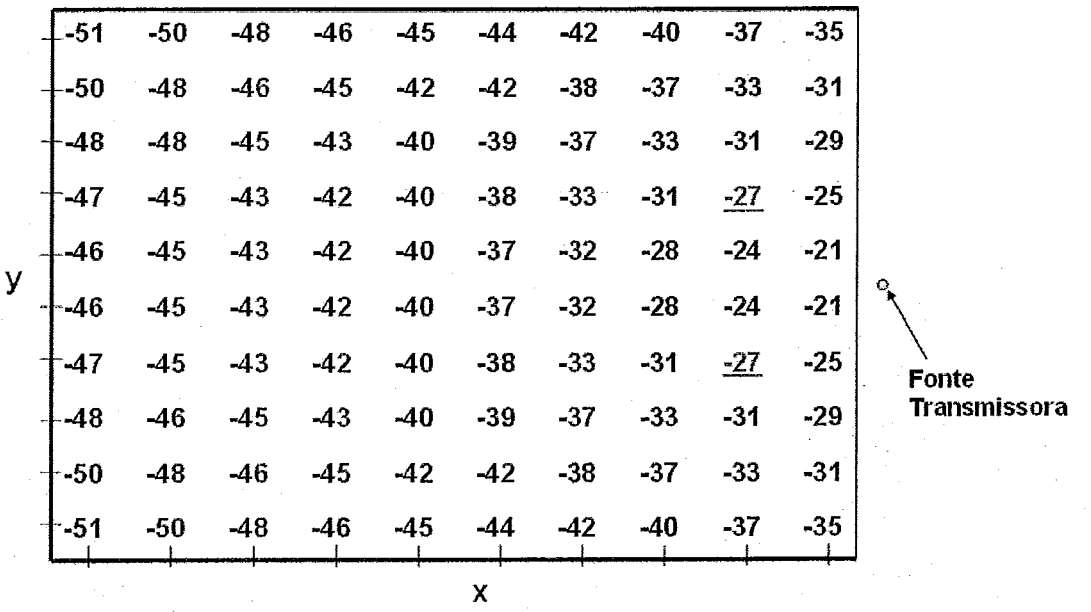

Figura 2.2: Ilustração do mapa de propagação construído na fase de calibragem para apenas uma fonte transmissora.

fonte transmissora. Já na fase *on-line*, o usuário irá medir o RSSI a partir de F fontes e compará-las com o mapa a fim de fazer uma estimativa de sua posição.

2.3 Discussão

A seguir apresenta-se uma discussão a cerca dos problemas encontrados na área de localização em WLANs, identificados durante a pesquisa bibliográfica. Os principais tópicos tratados neste trabalho foram destacados a seguir e os problemas relativos a cada solução estudada foram também comentados.

Técnica Utilizada na Estimativa

Trabalhos anteriores sobre construção de modelos para estimativa de localização de dispositivos sem fio incluem, na grande maioria dos casos, esforços de calibragem onde cada ponto do local de cobertura da rede sem fio é mapeado em um vetor de RSSI, de acordo com o procedimento ilustrado acima. Uma vez criado o

mapa/modelo de localização, alguma técnica deve ser utilizada, na fase *on-line* (descrita na seção anterior), para comparar as medições de RSSI realizadas em tempo real, com os valores contidos no modelo. Diferentes técnicas de comparação entre o RSSI medido em tempo real e os valores registrados no mapa de calibragem vêm sendo utilizadas. Dentre estas técnicas é possível citar, utilização de redes neurais [21], modelos probabilísticos [22, 23], distância euclidiana ou distância de Manhattan entre o valor medido e o valor registrado no mapa e o método dos k vizinhos mais próximos [1]. A técnica escolhida nesta comparação é crucial para a acurácia do sistema. No Capítulo 5 encontra-se uma proposta eficiente para este fim.

Necessidade de Modelos Adaptativos

A maior parte das técnicas atuais utilizam um esforço substancial de calibragem para gerar o modelo de localização [1, 19, 22, 23, 24, 25, 26, 27] e sofrem quando existem mudanças no local a ser monitorado. Até mesmo soluções comerciais como Ekahau [28], baseiam-se neste tipo de procedimento. Em ambientes dinâmicos, com grande fluxo de pessoas ou onde existe mudança na disposição da mobília, o mapeamento pode sofrer modificações significativas e a calibragem, nestes casos, deveria ser refeita. Estudos como em [8, 29] mostram a necessidade de modelos adaptativos para o mapeamento do RSSI, mesmo em ambientes aparentemente estáticos, pois estes valores oscilam muito ao longo do tempo como pode ser observado na Seção 3.3.

Em grande parte dos trabalhos, os autores não mencionam o impacto da utilização de um modelo de localização "mais velho" na acurácia de suas estimativas. Apenas em um único trabalho [29] estimativas de posição foram realizadas utilizando-se modelos criados anteriormente, com poucas semanas e até mesmo poucos dias de diferença. Neste mesmo trabalho os autores mostram que o erro na estimativa de posição pode aumentar consideravelmente, quando se utilizam modelos mais antigos nas estimativas de posição. Ou seja, a "idade" do modelo tem impacto grande na acurácia, o que mostra a necessidade de reconstrução periódica do mesmo. Isso pode ser difícil e de alto custo quando essa reconstrução envolve refazer todo o processo de

calibragem. Desta forma, técnicas que utilizam um mínimo, ou nenhum esforço de calibragem seriam particularmente úteis neste contexto, no entanto, estas mesmas deveriam levar em conta a grande oscilação do nível de sinal ao longo do tempo.

Em [23], tratou-se o problema de estimar a posição de um nó sem fio, como um problema de aprendizado de máquina (*Machine Learning*). Modelos probabilísticos foram também utilizados junto a essa abordagem, obtendo-se bons resultados (erros na estimativa da ordem de 1.56 metros). No entanto, para chegar a estes resultados, os autores utilizaram 10 APs e uma fase de calibragem de 4 horas para construção do mapa.

O mecanismo proposto aqui se destaca de outros mencionados neste capítulo. Diferente dos demais, não existe fase de calibragem e conseqüentemente, não existe também o esforço de refazê-la ao longo do tempo. Primeiramente por tratar-se de um mecanismo baseado em modelos de propagação (estes modelos serão vistos no Capítulo 3) e também por possuir um esquema de reconstrução automática e periódica do modelo de localização. Todo esse procedimento de construção do modelo será visto no Capítulo 4.

Utilização de Infraestrutura Pré-existente

Devido a problemas de multi-percurso e a falta de visada direta, em muitos casos, técnicas de triangulação, TDOA e direção (AOA) não são adequadas para serem aplicadas em ambientes fechados e podem levar a resultados pouco acurados. Além disso, estas técnicas muitas vezes necessitam de hardware dedicado [30, 31] e/ou antenas direcionais [32]. O TDOA ainda necessita de grande precisão nas medidas de tempo e sincronismo entre transmissor e receptor. Qualquer que seja a cobertura e a acurácia destes sistemas, eles sempre dependerão de hardware específico e/ou pessoal treinado para sua implementação. A utilização deste tipo de equipamentos, além de aumentar o custo de implantação do sistema, foge à proposta deste trabalho, cujo objetivo é utilizar a própria infra-estrutura de WLAN já existente, sem a necessidade de se adquirir hardware especializado para este fim.

Arquitetura Utilizada

Outro ponto em discussão é a utilização de arquiteturas de sistema diferentes. Define-se aqui arquitetura, como o comportamento do sistema de localização e a forma como os dados são colhidos. Neste contexto, duas arquiteturas são utilizadas em sistemas de localização: baseadas em cliente-servidor [1, 22, 24, 25, 26, 27] e baseada em *sniffers* [8]. Nas seções a seguir são apresentadas as duas arquiteturas, seus impactos no funcionamento dos SBLs e por fim uma comparação entre os dois.

Capítulo 3

Características do Sinal de RF em uma WLAN

UMA vez que o sistema utiliza informações sobre a qualidade do sinal de RF (valor de RSSI) como entrada para realizar as estimativas de localização, é importante abordar os aspectos do canal de comunicação utilizado e de que forma essas características de sinal são aferidas. Assim, este capítulo apresenta, primeiramente, o padrão de redes sem fio utilizado, incluindo aspectos da camada física e o funcionamento básico dos dispositivos que compõe estas redes. Mostra-se aqui também, através de experiências realizadas em laboratório, por que é possível utilizar a quantidade RSSI para auxiliar na localização de dispositivos. Por fim, são discutidos modelos de propagação e como estes se aplicam ao presente trabalho.

3.1 Redes Locais Sem Fio 802.11

Entre os padrões para redes locais sem fio existentes no mercado o mais popular e mais adotado atualmente é o IEEE802.11b. Redes que seguem este padrão estão cada vez mais presentes nas empresas, hotéis, fábricas e lugares públicos como aeroportos, universidades, hospitais e centros comerciais, oferecendo a possibilidade de acesso à rede com suporte à mobilidade.

Uma WLAN tem o mesmo alcance de comunicação (de 100 a 500 metros) e deve satisfazer os mesmos requisitos de uma LAN, incluindo alta capacidade, completa conectividade entre as estações e a capacidade de *broadcast*. Para isto, WLANs devem ser projetadas para atender algumas questões específicas de ambientes sem fio, tais como consumo de energia, mobilidade, segurança e limitações na capacidade do canal [33].

Um dos principais problemas desta tecnologia emergente está na sua falta de segurança, devido à particularidades do meio físico de transmissão. Como os dados são transmitidos pelo ar, não existem limites definidos como no caso das redes cabeadas. Dessa forma, é possível interceptar informações mesmo que à longas distâncias, sem necessariamente estar no mesmo ambiente ou prédio da WLAN. As redes sem fio geralmente estão conectadas à infra-estrutura da rede cabeada, tornando-se assim, mais fácil para o invasor ganhar acesso a todos os serviços de rede da empresa ou instituição. Por isso, é extremamente importante a implementação de mecanismos e sistemas de segurança nas WLANs.

3.1.1 Camada Física de Redes Sem Fio 802.11b

A camada física deste padrão é especialmente interessante no contexto deste trabalho, uma vez que podem ser utilizadas características desta camada para inferir a posição de um nó transmissor, como poderá ser visto posteriormente.

O padrão 802.11b lançado em 1997 pelo IEEE representa um conjunto de especificações para implementação de redes locais sem fio que prevê três técnicas de

transmissão:

1. Infra-vermelho.
2. DSSS (*Direct Sequence Spread Spectrum*)
3. FHSS (*Frequency Hopping Spread Spectrum*)

Os dois últimos métodos utilizam transmissão de ondas de rádio compreendidas pela banda não licenciada ISM (*Industrial, Scientifical, Medical*) de 2.4GHz. Dentre os métodos mencionados, o DSSS é o mais utilizado na implementação do padrão 802.11b.

FHSS (*Frequency Hopping Spread Spectrum*)

O FHSS utiliza 79 canais com largura de 1 MHz cada. As partes comunicantes utilizam esses canais para transmissão, alternadamente e de forma sincronizada. Transmissor e receptor mudam ou "saltam" (*hop*) de canal em canal durante a transmissão. Um gerador de números pseudo-aleatórios é utilizado para gerar a seqüência de saltos nos 79 canais. Desta forma, todas as estações que tenham utilizado a mesma semente em seu gerador e que se mantenham sincronizadas, saltarão para os mesmos canais simultaneamente. Cada estação de uma mesma rede, que utiliza a mesma seqüência de saltos, ficará em cada canal por um período denominado *dwell time*, que é ajustável. Com o FHSS tem-se um sistema robusto contra ruído de banda estreita, o que provê um nível de segurança já na camada física, pois somente as estações que conhecem a seqüência de saltos e o *dwell time* poderão "escutar" o meio de maneira adequada e organizada. No entanto, o FHSS possui a desvantagem de oferecer uma baixa largura de banda (apenas 1 MHz).

DSSS (*Direct Sequence Spread Spectrum*)

Já o DSSS "espalha" o espectro de freqüência de um sinal de banda estreita através de sua modulação com uma seqüência de bits denominada de *chip sequence*.

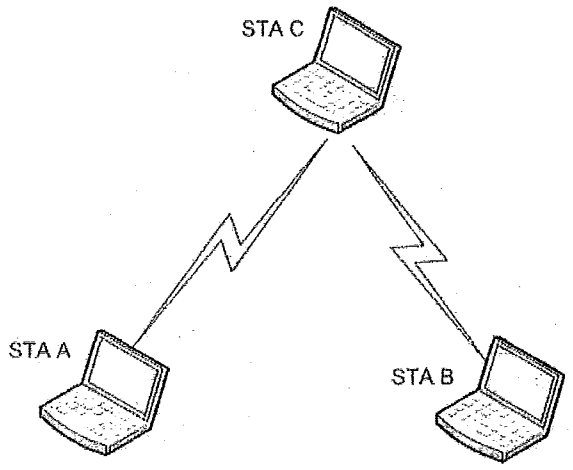

Figura 3.1: Exemplo de redes sem fio adotando topologia *ad hoc*.

Obtém-se, desta forma, um sistema robusto contra ruído de banda estreita ao preço da necessidade de um controle de potência para transmissão [2]. Com o DSSS foi possível elevar a taxa de transmissão do 802.11b de 1 Mb/s para 11 Mb/s.

3.1.2 Operação de Redes Sem Fio 802.11b

Redes deste tipo operam em um dos dois modos disponíveis - *ad hoc* (sem infraestrutura) ou infraestruturado. O padrão IEEE define o modo *ad hoc* como *Independent Basic Service Set* (IBSS), e o modo infraestruturado como *Basic Service Set* (BSS).

No modo *ad hoc* cada estação pode se comunicar diretamente com outras estações na rede, como exemplificado na figura 3.1. O modo *ad hoc* foi projetado de forma que apenas as estações que se encontrem dentro do alcance de transmissão (mesma célula) umas das outras possam se comunicar. Se uma das estações (STA A) quiser se comunicar com outra fora de seu alcance (STA B), uma terceira estação (STA C) dentro do alcance de STA A e STA B, deve ser utilizada como *gateway* e fazer o roteamento.

Já no modo infraestruturado, cada cliente envia todas as suas mensagens para uma estação central, o Ponto de Acesso ou *Access Point* (AP). Esta estação central funciona como uma *ethernet bridge* repassando as mensagens para a rede apropriada,

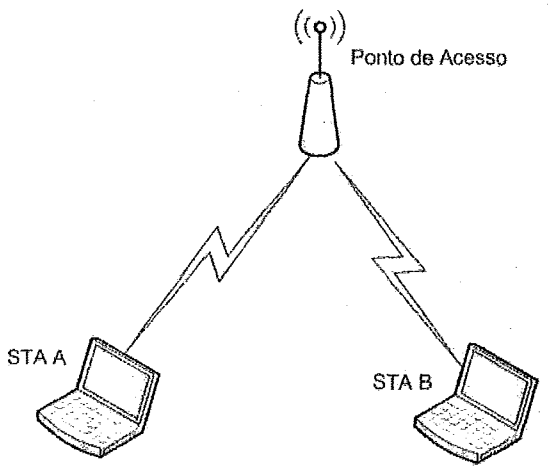

Figura 3.2: Exemplo de redes sem fio adotando modo infraestruturado, onde um AP é utilizado na comunicação.

ou seja, uma rede cabeada, ou para a própria rede sem fio. A figura 3.2 mostra este tipo de topologia.

Antes de trocarem dados, STAs e APs devem estabelecer um relacionamento, ou uma associação. Apenas depois que a associação for estabelecida as duas estações podem trocar dados. No caso de uma rede com infraestrutura, as STA se associam com o AP. O processo de associação possui dois passos, envolvendo três dos seguintes estados:

1. Não autenticado e não associado,
2. Autenticado e não associado, e
3. Autenticado e associado.

Para mudar de estados, as partes interessadas na comunicação trocam mensagens denominadas quadros de gerenciamento ou *management frames.*

No entanto, uma STA precisa saber se existe algum AP dentro do alcance de seu rádio e a qual AP ela deve se associar. Assim, todos os APs transmitem um quadro de gerenciamento chamado *beacon* em intervalos fixos de tempo. Para se associar a um AP e se unir a uma BSS, uma estação procura escutar *beacons* para identificar

APs dentro do alcance de seu rádio. Então a STA seleciona a qual BSS ela deseja se unir. Em seguida, AP e STA trocam diversas mensagens de gerenciamento com o objetivo de realizar uma autenticação mútua. Dois mecanismos de autenticação são previstos no padrão, mas não serão abordados neste trabalho, pois fogem ao tema principal do mesmo.

Após uma autenticação bem sucedida, a STA passa para o segundo estado, "autenticado e não associado". Passar do segundo estado para o terceiro, "autenticado e associado", requer que a STA envie um pedido de associação ao AP e este, em seguida, responda com a aceitação. Uma vez que esse processo ocorre, a STA passa a ser um ponto (*peer*) da rede sem fio e pode, então, transmitir quadros através da mesma.

3.2 Medindo o Nível de Sinal Recebido (RSSI) em uma WLAN

O *hardware* das interfaces sem fio é capaz de detectar o nível de sinal recebido e representá-lo através de um valor codificado por uma palavra de 8 bits [2]. Este valor pode ser lido pelo *driver* da placa de rede sem fio e passado para camadas de *software* superiores. Este valor dado pelo *hardware* da placa é chamado de *Received Signal Strength Indicator* - RSSI e é um número inteiro que varia de 0 até um valor $RSSI_{MAX}$. No entanto, apesar do padrão indicar 8 bits para representar este valor, cada fabricante utiliza uma forma diferente para representar o RSSI no *hardware*, de forma que o valor $RSSI_{MAX}$ venha a ser diferente para *chipsets* diferentes. Isso gerou uma necessidade de se investigar as formas de se representar o RSSI nos diferentes *chipsets* disponíveis no mercado e como converter os valores de uma representação para outra. O RSSI pode ser representado das seguintes formas:

- Valor inteiro variando de 0 até $RSSI_{MAX}$, onde $RSSI_{MAX}$ depende do *chipset* do equipamento;
- Porcentagem de sinal variando de 0% até 100%;

- Em dBm, cuja variação depende do *chipset.*

A representação escolhida para este trabalho foi a dBm, de forma que esta quantidade pudesse ser adequada a modelos de propagação de sinal utilizados neste trabalho. Assim, foi necessário descobrir como converter o valor inteiro do RSSI lido do hardware pelo driver, para um valor em dBm. Descobriu-se que para o *chipset prism*, o valor de RSSI lido pelo *sniffer* deve ser subtraído de 150 para fornecer o valor em dBm. Caso o chipset em questão seja *atheros*, 60 é o valor que deve ser subtraido do RSSI medido. Em resumo:

- Atheros: RSSI - 60 = RSSI(dBm);
- Prism : RSSI - 150 = RSSI(dBm);

3.3 Características do RSSI

Atenuação em espaço livre e multi-percurso [12, 34] são fenômenos de RF muito comuns. O primeiro refere-se a atenuação que o sinal sofre ao propagar-se através do meio. No segundo, o sinal transmitido pode chegar ao receptor através de diferentes caminhos, cada um possuindo amplitudes e fases diferentes. Estes componentes somam-se no receptor causando distorção no sinal recebido. Mais ainda, mudança na temperatura e humidade, disposição da mobilia e principalmente trânsito de pessoas no recinto alteram a qualidade e o nível de sinal recebido (RSSI). Os níveis de sinal recebido se alteram ao longo do tempo e variam em torno de um valor médio. Quando se deseja utilizar a informação de RSSI em aplicações de localização, é preciso saber se as variações neste valor são provocadas pelo movimento dos dispositivos sem fio, ou por alterações no ambiente onde os dispositivos se encontram fisicamente.

Um experimento simples foi realizado em laboratório para que fosse possível visualizar a influência de fatores externos como, pessoas transitando no ambiente de trabalho, nos valores de nível de sinal recebido. A distância entre receptor (*notebook Dell Latitude C840* + PCMCIA Wireless Orinoco Silver) e transmissor (*Cisco Access*

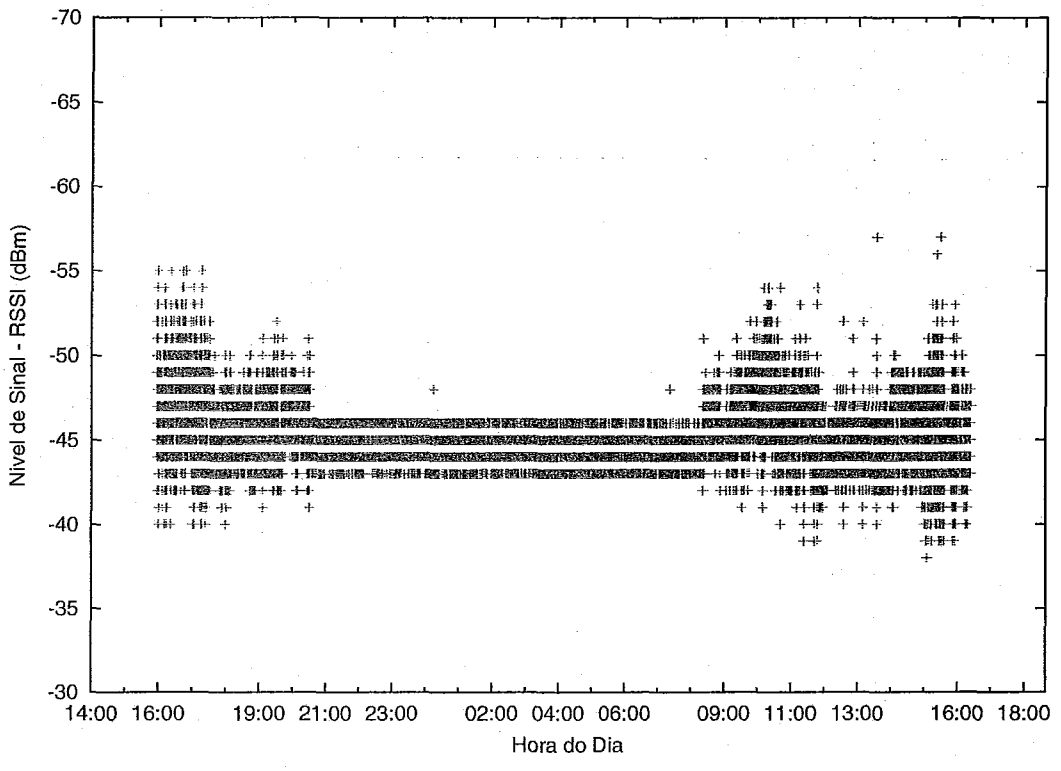

Figura 3.3: Medidas de nível de sinal recebido, realizadas a uma distância de 10.7 metros do t_x para o r_x ao longo de aproximadamente 24 horas.

Point Aironet 1200 Series) foi fixada em 10.7 metros, com visada direta e o tempo de duração das medições foi de pouco mais de 24 horas. É possível ver claramente na Figura 3.3 que ao longo do dia existem alterações tanto na média quanto no desvio padrão do valor de RSSI. No horario da noite, entre 20:30h e 8:30h, quando não existe movimentação de pessoas, esta variação é muito menor e o RSSI é bem mais estável. Esta experiência reforça as afirmações feitas acima sobre a influência do trânsito de pessoas na propagação de sinal em um ambiente fechado.

O objetivo principal então, passou a ser tentar modelar o RSSI. Assim, um estudo estatístico foi feito para se tentar determinar uma distribuição de probabilidade capaz de representar este valor e suas flutuações. Em diversos trabalhos [1, 22, 23, 24, 25, 26, 27], mostra-se que a distribuição Gaussiana (Equação 3.1) representa bem o comportamento do RSSI.

$$f(s_i) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(s_i - \mu)^2}{2\sigma^2}\right), \tag{3.1}$$

onde σ é o desvio padrão e μ a média dos valores de RSSI (s_i) medidos.

Medições foram realizadas para verificar este comportamento. O ponto de acesso foi colocado em um ponto fixo, à uma determinada distância do *notebook*. Este último, nesta experiência, capturava *beacons* [2] emitidos pelo ponto de acesso a uma taxa de 1 *beacon* por segundo. Cada *beacon* capturado tinha um RSSI correspondente e este era registrado.

A primeira experiência durou aproximadamente 3 horas e tinha como objetivo verificar a variação do nível de sinal recebido durante o funcionamento da rede sem fio. Transmissor (ponto de acesso) e receptor (*sniffer*) permaneceram imóveis em suas posições durante todo o experimento. A distância entre eles era de 5.8 metros com visada direta. Na Figura 3.4 é possível ver a variação do sinal ao longo do tempo. Percebe-se que a variação existe, mesmo quando a distância entre t_x e r_x permanece constante. Foi observada uma média em -51.06 dBm e um desvio padrão $\sigma = 2.1848$ dBm. A Figura 3.5 trás um histograma que revela a ocorrência dos valores das medidas de RSSI em dBm, durante o experimento. É possível observar que o comportamento se assemelha ao comportamento de uma curva normal (em linha cheia no mesmo gráfico).

É possível concluir a partir destes experimentos, que quando transmissor e receptor estão a uma distância fixa, as variações existentes no RSSI são devido, apenas, à interferência de pessoas e equipamentos próximos. Essa interferência gera variações pequenas, enquanto que a variação devido a distância é bem maior. Isso mostra que o nível de sinal pode ser utilizado como parâmetro para determinar quando um dispositivo sem fio se aproxima ou se afasta de outro.

A flutuação do RSSI pode ser explicada, mais formalmente, através de dois fenômenos conhecidos por decaimento em pequena escala (*small-scale fading*) e desvanecimento em grande escala (*large-scale fading*). O primeiro é dado pelas rápidas variações de RSSI em pequenos intervalos de tempo ou através de pequenas distân-

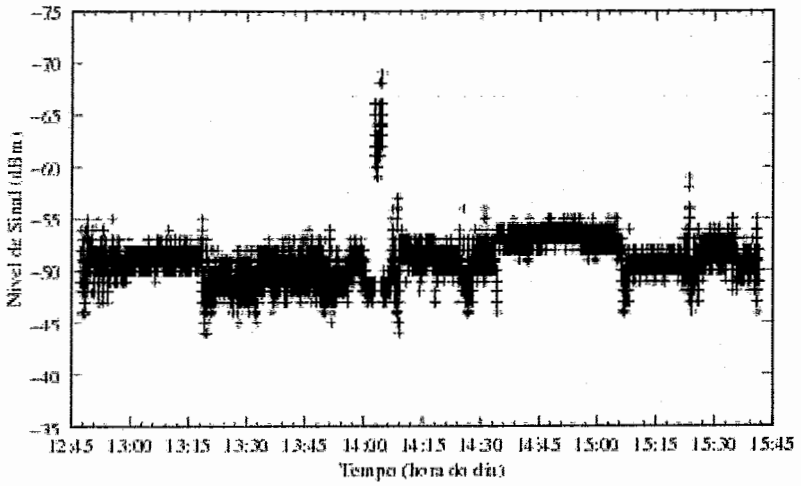

Figura 3.4: 10147 medidas de nível de sinal recebido, realizadas a uma distância de 5.8 metros do t_x para o r_x, durante 3 horas seguidas, em horário de trabalho, onde havia constante trânsito de pessoas e mudança na ocupação do ambiente.

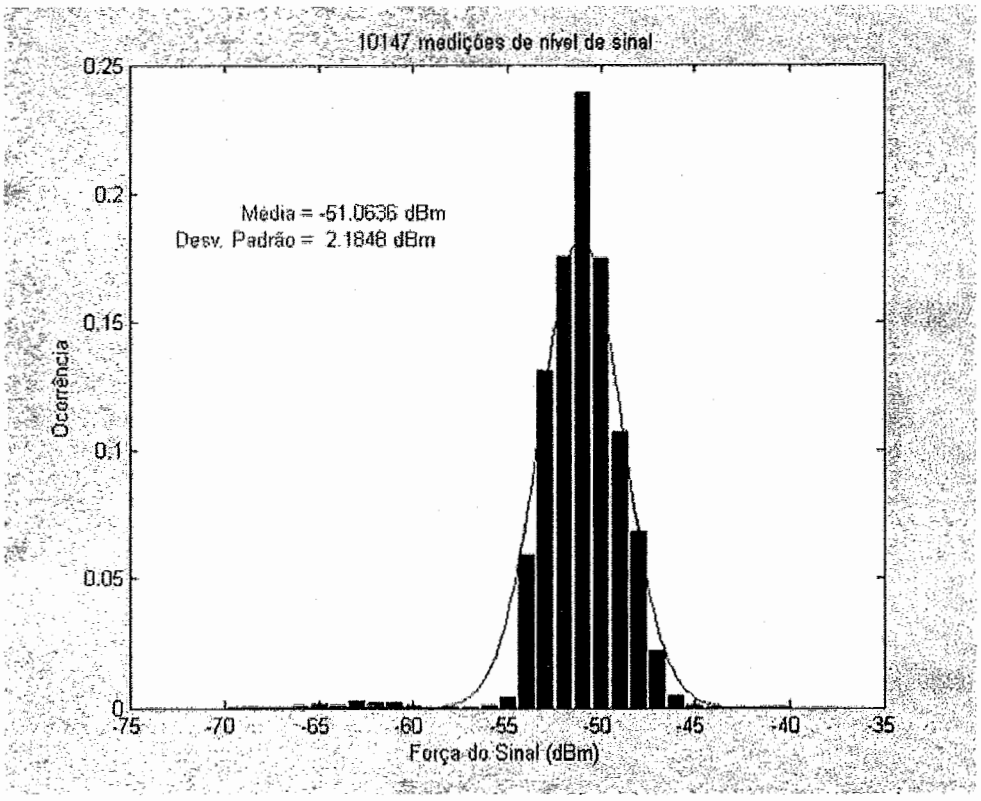

Figura 3.5: Ocorrência dos valores das medidas de nível de sinal recebido ao longo do experimento, realizado a uma distância de 5.8 metros do t_x para o r_x.

cias percorridas. O segundo é causado pela distância de separação entre t_x e r_x, onde o RSSI decresce na medida em que cresce a distância. A Figura 3.4 ilustra o decaimento em pequena escala onde o RSSI varia até 16 dBm em um intervalo de apenas 1 segundo.

Nos capítulos seguintes será discutida a técnica utilizada aqui para minimizar os efeitos do decaimento em pequena escala. Essa compensação pode ser atingida através de medições de RSSI realizadas ao longo do tempo e com a utilização de um modelo de propagação de grande escala, cujos parâmetros são determinados dinamicamente.

3.4 Modelos de Propagação

A utilização destes modelos em localização é mencionada em diversos trabalhos, mas é sempre preterida em relação a utilização de medições realizadas na fase de calibragem. O argumento principal é a maior acurácia apresentada por sistemas que utilizam uma fase anterior de calibragem, pois os modelos de propagação não refletem fielmente o ambiente onde o sistema é implementado e que este ambiente muda constantemente com o tempo, devido a uma série de fatores (discutido na Seção 3.3). No entanto, aqui pretende-se mostrar através de resultados experimentais, que a utilização de modelos de propagação para estimar o comportamento do canal aplicando-os a métodos de localização é viável e muitas vezes mais vantajoso. Isso porque modelando o comportamento do canal, elimina-se a necessidade da realização de medidas reais em diversos pontos.

Neste contexto, estudou-se a aplicação de um modelo de propagação de grande escala chamado em [12, 13] de *Log-distance Path Loss Model*. Neste modelo, a potência $P_l(d)[dBm]$ percebida pelo receptor r_x a uma distância d do transmissor t_x é descrita pela Equação 3.2 a seguir:

$$P_l(d)[dBm] = P_0(d_0)[dBm] - 10n_0 log\left(\frac{d}{d_0}\right) - X_\sigma, \tag{3.2}$$

onde $P_0(d_0)[dBm]$ é a potência de sinal recebido a partir de uma distância de referência d_0 de separação entre t_x e r_x, n_0 é a taxa de decaimento do sinal transmitido proporcional à distância, e X_σ representa uma variável aleatória de distribuição normal, cujo desvio padrão é σ dBm.

Outro modelo estudado, e de fato aplicado neste trabalho, é uma simples variação do modelo anterior, onde no lugar de se aplicar uma atenuação aleatória dada por X_σ, utiliza-se uma atenuação (chamada de WAF (*Wall Attenuation Factor*) em [1]), cujo valor é fixo e igual ao somatório da atenuação provocada por obstáculos que interceptam uma linha reta traçada entre t_x e r_x. A Equação 3.3 mostra este modelo.

$$P_l(d)[dBm] = P_0(d_0)[dBm] - 10n_0 log\left(\frac{d}{d_0}\right) - WAF \tag{3.3}$$

O principal motivo para a escolha deste modelo de propagação é a grande aceitação do mesmo em trabalhos onde existe a necessidade de modelar canal sem fio em ambientes fechados (*indoor*).

A modificação principal realizada aqui esta na forma como os valores para os parâmetros do modelo apresentado na Equação 3.3 foram determinados. Isto será abordado em detalhes na Seção 4.3, no capítulo seguinte

Capítulo 4

Proposta de um Sistema para Localização de Dispositivos Sem Fio

ESTE capítulo descreve, em detalhes, o sistema proposto. O mecanismo de localização é apresentado, incluindo uma definição de seus componentes e de que forma os mesmos interagem entre si. Todo o passo-a-passo do sistema é mostrado, desde as medições de qualidade de sinal, passando pela construção do mapa de propagação (Seção 4.3) até a estimativa de posição realizada pelo servidor de localização (Seção 4.2.2).

4.1 Arquiteturas para Localização

O objetivo desta seção é apresentar os componentes envolvidos na estimativa de posição de estações em uma WLAN. Estes componentes e a forma como interagem podem variar de acordo com o tipo de abordagem e o tipo de aplicações que irão utilizar as estimativas. A forma de interação entre os componentes e suas características, é chamada aqui de arquitetura do sistema. Assim, essa seção foi dividida em duas partes. A primeira trata da arquitetura baseada no paradigma cliente-servidor, que é a mais utilizada pelos mecanismos de localização encontrados na literatura e discutidos no Capítulo 2. Já na segunda subseção, foi proposta uma arquitetura baseada em componentes novos chamados *sniffers*. Arquitetura semelhante foi utilizada apenas em [8]. A seguir, serão apresentadas estas duas arquiteturas e discutidas suas diferenças, mostrando-se as vantagens da arquitetura baseada em *sniffers*.

4.1.1 Arquitetura Baseada em Cliente-Servidor

Neste tipo de sistema, o processo de estimativa de localização ocorre sempre em duas etapas, *off-line* e *on-line*, discutidas no capítulo anterior. Na Figura 4.1 é possível ver um exemplo de uma rede sem fio onde um mecanismo de localização baseado no paradigma cliente-servidor foi implantado. Os clientes sem fio estão associados a um determinado AP, mas recebem também, sinal de outros APs dentro da área de cobertura. Neste ambiente, cada cliente mede o RSSI de cada um dos APs em sua área de cobertura e os envia na forma de um vetor $[RSSI_1, RSSI_2, ..., RSSI_n]$ (onde n indica o índice do AP transmissor) para o servidor de localização. Este último compara o vetor recebido de cada cliente com as informações dos vetores de RSSI registrados no banco de dados, através de medidas de nível de sinal realizadas na fase de calibragem (a fase de calibragem e a construção do mapa de propagação foram discutidas na Seção 2.2). Esta comparação é feita utilizando algum algoritmo próprio para tal (alguns destes algoritmos para comparação foram mencionados na Seção 2.3) e assim, o servidor de localização estima a posição física do cliente.

A utilização desta arquitetura leva à algumas questões que devem ser levantadas.

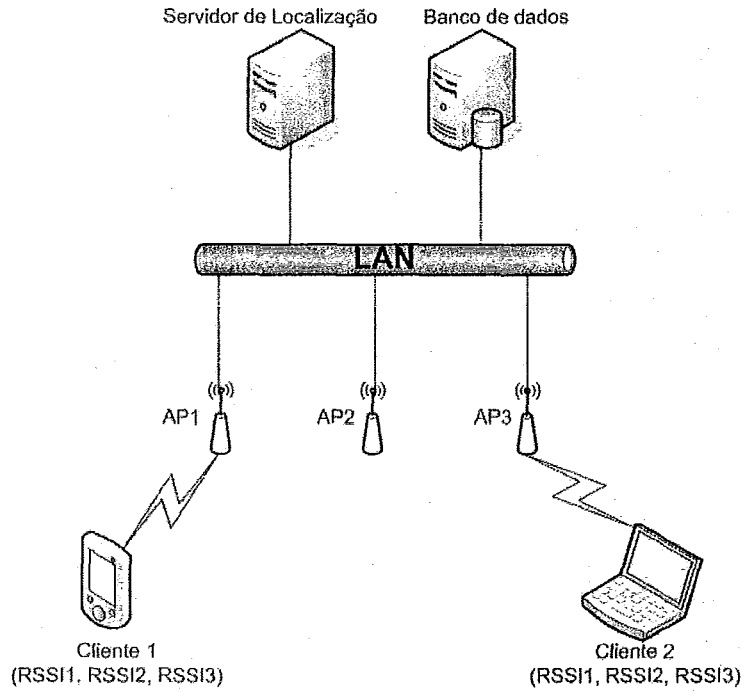

Figura 4.1: Arquitetura baseada em Cliente-Servidor.

Para que o cliente possa medir o RSSI dos APs, ele precisa de software específico para tal. O que acontece se o cliente não iniciar o software por algum motivo? Esta arquitetura é aplicável para SBLs onde existe interesse, por parte do cliente sem fio, que sua posição seja determinada. Em aplicações de gerência ou segurança este tipo de arquitetura pode não ser adequada. Esta discussão será mais elaborada na Seção 4.1.2 a seguir.

4.1.2 Arquitetura Baseada em *Sniffers*

Sniffers são softwares que monitoram uma interface de rede e capturam todas as informações que trafegam por ela. Neste trabalho serão chamados *sniffers* entidades formadas por um computador (PC - *Personal Computer*), uma interface de rede sem fio instalada e configurada neste PC e um *software* que captura o tráfego nesta interface de rádio. Estas entidades podem estar co-alocadas aos APs ou em máquinas distintas. Uma outra configuração seria a utilização de placas dedicadas e sistemas embarcados (também chamados sistemas embutidos) e de baixo custo no lugar dos

PCs [35].

Esta arquitetura pode ser vista na Figura 4.2. Neste caso, existem dois *sniffers* co-alocados com os pontos de acesso AP1 e AP2 e ainda um terceiro. Perceba que ambas as entidades, APs e *sniffers* estão representadas na figura por PCs comuns[1]. Estes *sniffers* monitoram a rede e ao receber pacotes, verificam e gravam informações sobre a fonte do pacote recebido. Entre estas informações podem ser citadas: endereço MAC (utilizado para identificar o dispositivo transmissor), modo de operação (pode ser usado para identificar se o transmissor é uma estação ou um AP), e RSSI. Estas informações são armazenadas em uma base de dados e utilizadas pelo servidor de localização para estimar a posição física do transmissor.

Arquiteturas semelhantes foram utilizadas em alguns poucos trabalhos recentes como em [29] onde se utiliza o modelo apresentado em [8]. No entanto, este sistema utiliza diversos dispositivos emissores estacionários (EE) espalhados pelo local a ser monitorado. Os autores afirmam que estes EEs são de baixo custo e apenas transmitem pacotes periodicamente utilizando o protocolo 802.11. Mesmo assim, segundo [8], pelo menos 7 (sete) EEs devem ser dispostos no local, para cada *sniffer* (sendo que um mesmo EE pode ser visto por vários *sniffers*). Isso significa que quanto maior a área a ser coberta pela rede sem fio, maior o número de APs, maior o número de *sniffers* e conseqüentemente, maior o número de EEs. Um estudo no sentido de avaliar o compromisso entre acurácia do sistema e a inserção ou não de dispositivos auxiliares como EEs, pode ser interessante para a proposta aqui apresentada. Uma avaliação do custo de implantação de novos EEs sobre uma determinada área, em função da acurácia do sistema será apresentada no Capítulo 6.

A principal motivação para o uso de *sniffers* para detecção e localização de dispositivos 802.11, é a possibilidade de detectar qualquer dispositivo, seja ele um usuário ou um AP, sejam estes legítimos ou não. Quando se utiliza uma arquitetura cliente-servidor, se o cliente, por algum motivo, não possuir o software instalado e

[1]Computadores pessoais podem ser utilizados como pontos de acesso [36] e prover acesso seguro à rede sem fio, através de mecanismos diversos, como VPNs (*Virtual Private Networks*) e *firewalls*.

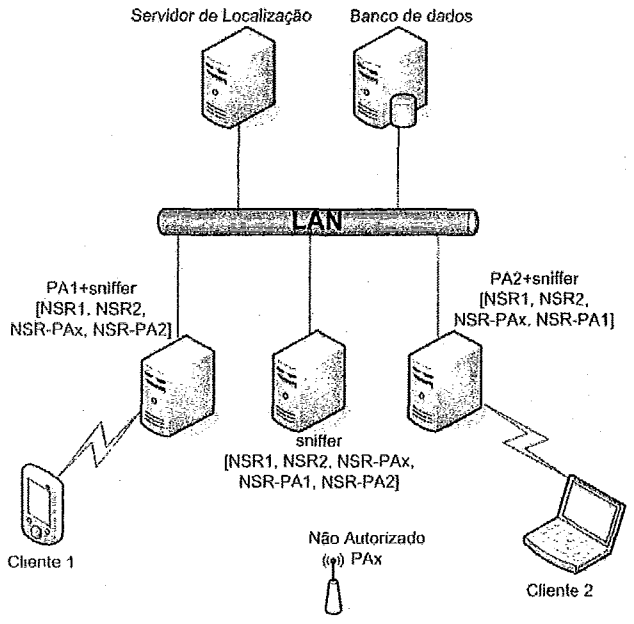

Figura 4.2: Arquitetura baseada em Sniffers.

executando, o sistema não será capaz de localiza-lo. Em aplicações de segurança ou onde um administrador precisa localizar o dispositivo sem fio para realizar manutenção, a arquitetura cliente-servidor mostra-se inadequada. Para este tipo de aplicação, existe a necessidade de monitorar o meio buscando por APs e clientes sem fio transmitindo pois, obviamente, não se pode esperar que o usuário não autorizado forneça as informações necessárias a sua localização.

Outro ponto negativo, na utilização de uma arquitetura baseada em cliente-servidor, é a preocupação com consumo de energia. Existe a necessidade de que o usuário faça o *download* do software que monitora o RSSI e envia as informações para o servidor de localização. Este processamento extra pode ter influência nos requisitos de energia dos dispositivos sem fio, o que é uma preocupação neste tipo de ambiente. Com o uso desta arquitetura, o cliente gera tráfego na rede sem fio periodicamente, quando envia os dados recolhidos para o servidor de localização, aumentando o tráfego na rede e a disputa pelo meio. Quando se utiliza *sniffers*, estas preocupações deixam de existir, pois tanto os *sniffers* quanto o servidor de localização podem estar ligados na rede cabeada e na rede elétrica, de forma que não haja limitações no uso de energia.

Quando se deseja implantar uma rede sem fio, os APs são geralmente dispostos de forma a conseguir a maior área de cobertura possível. Isso implica em que estes devam estar localizados de forma que as áreas de cobertura tenham o mínimo de sobreposição. Em sistemas de localização baseados em cliente-servidor, tipicamente, deseja-se sobreposição de cobertura pois são necessárias informações de RSSI de diversos APs para que seja possível localizar o cliente. Quando se utiliza uma arquitetura baseada em *sniffers*, os APs podem ser instalados de forma a atingir a maior área de cobertura e os *sniffers* podem ser instalados em locais estratégicos de forma a conseguir a sobreposição necessária. Estes *sniffers* podem ser instalados em estações de trabalho fixas de forma que seu funcionamento seja transparente ao usuário, ou ainda em dispositivos dedicados a este fim. O custo da implementação dos *sniffers* pode ser diluído não apenas nas aplicações baseadas em localização, mas também em aplicações de gerenciamento e monitoramento de tráfego.

Em um sistema cuja arquitetura é baseada em cliente-servidor, a inserção de APs adicionais pode aumentar a acurácia na estimativa de localização [1]. A inclusão de novos pontos de acesso, implica em preocupações extras para o administrador da rede. Mais APs podem significar mais "portas" a serem vigiadas. É preferível implantar dispositivos totalmente passivos como *sniffers*, a APs adicionais, tanto em termos de custo quanto em termos de gerenciamento e segurança. Um *sniffer* pode ser encarado como um "cliente especial", muito mais fácil de ser gerenciado.

4.2 Arquitetura do Sistema Proposto e Seus Componentes

A seguir serão discutidos os componentes do sistema, seus papéis na estimativa de localização, que ações executam e como eles se relacionam uns com os outros.

4.2.1 O *Sniffer*

O software dos *sniffers*, foi escrito em linguagem C, pois assim seria possível escrever código portável para outras plataformas. Foi preciso então, descobrir como extrair as informações de RSSI, dos pacotes 802.11. Em um primeiro momento tentou-se utilizar as ferramentas disponíveis no pacote *Wireless Tools* [37] para o sistema operacional Linux, principalmente por serem simples e muito utilizadas em diversos trabalhos na área [22, 23, 24, 25, 26, 27]. No entanto, descobriu-se que esta ferramenta reportava apenas o RSSI para pontos de acesso (extraía valores de RSSI apenas de *beacons*, um tipo de pacote originado apenas por APs), e não para estações de trabalho. Desta forma, modificou-se uma biblioteca escrita em C, encontrada no pacote do *driver hostap* [38], para que fosse possível extrair do quadro 802.11 (não importando o tipo de pacote) as informações desejadas, incluindo o RSSI e o endereço físico[2] da interface que transmitiu o pacote. Esta última informação é importente para identificar o dispositivo transmissor.

Assim, os *sniffers* foram implementados para desempenhar duas tarefas principais na arquitetura proposta:

1. Detectar estações sem fio e aferir os valores de RSSI para cada uma;
2. Medir o nível de sinal recebido de um ou mais pontos de referência para construir o modelo de localização.

Estas ações são executadas simultaneamente e de forma ininterrupta ao longo do tempo. A primeira consiste em capturar pacotes de todas as interfaces sem fio detectadas pelo *sniffer* e extrair informações sobre RSSI e MAC do transmissor x. Para cada interface transmissora detectada, são capturados pacotes durante um determinado tempo. Esse tempo é definido aqui como *IC* (*Intervalo de Captura*) e foi utilizado nos experimentos apresentados neste trabalho com o valor de 1 segundo.

[2] O endereço físico, também chamado de endereço MAC (*Medium Access Control*), é um valor constituído por 48 bits, representado em hexadecimal, que identifica unicamente cada interface sem fio.

Escolheu-se utilizar o RSSI médio medido durante um pequeno intervalo de tempo de forma tirar vantagem da alta auto-correlação existente entre medidas de RSSIs dentro deste intervalo de tempo [14]. Cada pacote possui seu RSSI respectivo e cada *sniffer* calcula o RSSI médio a partir dos pacotes capturados durante o IC, para cada transmissor detectado. Em seguida, cada *sniffer* envia ao banco de dados [39] a média calculada para cada transmissor detectado, repetindo sempre este procedimento a cada IC. Desta forma, no banco de dados serão armazenadas as tuplas $(RSSI_{1;x}, RSSI_{2;x}, ..., RSSI_{i;x}, ..., RSSI_{k;x}, MAC_x)$, onde $RSSI_{i;x}$ é a média dos RSSIs medidos a partir de todos os pacotes capturados pelo *sniffer* de índice i para o dispositivo transmissor detectado de índice x. Isso é feito em todos os k *sniffers* que monitoram o local.

Na segunda, são capturados pacotes de *beacon* oriundos do(s) ponto(s) de acesso que compõe a rede sem fio, chamados aqui de *pontos de acesso de referência*. Os *sniffers* então, extraem destes pacotes a informação de RSSI. Cada *sniffer* faz isso para cada ponto de acesso de referência M vezes. Assim, de posse de M medições de RSSI seguidas, o *sniffer* calcula média μ e desvio padrão σ destes M dados coletados, enviando em seguida para o banco de dados o par $(\mu_{i;n}, \sigma_{i;n})$, onde $\mu_{i;n}$ e $\sigma_{i;n}$ são respectivamente média e desvio padrão calculados pelo *sniffer* i a partir o ponto de acesso de índice n. Neste trabalho e na geração dos resultados foram utilizados $M = 100$ medições de RSSI, 3 *sniffers* e apenas 1 ponto de acesso que envia *beacons* a um intervalo de 100 mili-segundos.

Trabalhos anteriores que utilizam arquitetura cliente-servidor, concentraram-se em situações onde o cliente "vê" pelo menos três APs envolvidos na localização. Na Seção 2.2 aborda-se a questão de pontos redundantes e o porque da necessidade de se utilizar pelo menos 3 APs para evitá-los. De forma análoga, cada ponto $[x, y]$ do local monitorado deve estar dentro da área de cobertura de pelo menos três *sniffers*. Dentro deste contexto, deve-se notar que a grande maioria dos gerentes de rede sentiriam-se mais confortáveis implantando *sniffers* adicionais (dispositivos totalmente passivos) para auxiliar na estimativa de localização, do que APs extras apenas para este fim. APs adicionais trariam preocupações com questões de segurança e reutilização de canais, uma vez que APs adjacentes não podem utilizar

freqüências de transmissão próximas (*overlapping channels*) para evitar interferência. Do ponto de vista de um administrador de rede, um *sniffer* pode ser visto como um cliente especial, mais simples de se gerenciar e cujo custo de implantação pode ser dissipado em outras aplicações, como captura e monitoramento do tráfego da rede sem fio e segurança (detecção de intrusos).

4.2.2 O Servidor de Localização

O componente mais importante que integra o sistema proposto é o *Servidor de Localização*. Sua função é estimar a posição dos dispositivos sem fio detectados pelos *sniffers*. Este componente é um *software*, implementado em C/C++, que lê informações do banco de dados, as processa e fornece como saída a posição dos dispositivos sem fio detectados. Nele também, está implementado o modelo de localização proposto.

O servidor de localização funciona da seguinte forma. Uma vez iniciado o programa servidor, ele acessa o banco de dados e lê as informações necessárias para montar o modelo de localização e aplicá-lo. Estas informações são:

1. Tamanho do local monitorado (X_{max}, Y_{max}).
2. Resolução do *grid*. Define-se aqui, *grid*, como sendo um conjunto de pontos que cobre o local monitorado, espaçados de uma distância fixa chamada resolução do *grid*. Neste trabalho a resolução utilizada será 1 metro.
3. Posição (x,y) do(s) AP(s) de referência (apenas 1 neste trabalho).
4. Posição (x,y) dos *sniffers*.
5. Endereços MAC de todos os dispositivos sem fio detectados pelos *sniffers*.
6. Níveis de sinal recebido a partir dos dispositivos detectados $RSSI_{i;x}$. Isso é feito para todos os *sniffers* e todos os dispositivos detectados por cada *sniffer*.

7. Par $(\mu_{i;n}, \sigma_{i;n})$ calculado para cada *sniffer* i com os RSSIs medidos a partir dos *beacons* do AP de referência de índice n. Isso é feito para todos os *sniffers* e todos os APs de referência.

De posse destes dados o servidor pode construir o modelo de localização e estimar a posição dos dispositivos detectados. A construção do modelo no servidor será discutida na Seção 4.3 e o estimador será apresentado no Capítulo 5.

4.2.3 O Ponto de Acesso

O ponto de acesso, além de desempenhar as funções corriqueiras de um equipamento desta natureza, tais como permitir conectividade entre estações sem fio associadas a ele e funcionar como uma "ponte" para a rede cabeada, ele é também utilizado como ponto de referência para construção do mapa de propagação (descrito na Seção 4.3).

Este equipamento transmite pacotes de gerenciamento, controle e pacotes de dados [2]. No sistema proposto, os *sniffers* capturam todos esses pacotes, identificam quais foram transmitidos pelo ponto de acesso de referência e destes, extraem a informação de RSSI deste pacote. Apenas *beacons* são utilizados para este fim. Desta forma, os *sniffers* calculam o RSSI médio e o desvio padrão, par $(\mu_{i;n}, \sigma_{i;n})$, como indicado anteriormente, para a posição onde o AP de referência está localizado. O ponto onde o AP de referência se encontra, será chamado no texto de l_0 e a exemplo do que acontece também com os *sniffers*, é fixo e conhecido.

A relação entre AP de referência e *sniffers* é de 1:n, ou seja, cada *sniffer* possui um AP de referência e cada AP de referência pode estar associado a diversos *sniffers*.

4.3 Construção do Mapa de Propagação (MP)

Como dito anteriormente, o servidor de localização lê do banco de dados informações sobre o local monitorado, *sniffers* e ponto(s) de acesso(s) de referência. De

posse destes dados, o servidor usa (X_{max}, Y_{max}), a resolução do *grid*, as posições dos *sniffers* e do AP de referência e os valores $(\mu_{i;n}, \sigma_{i;n})$ de cada par *sniffer+AP de referência*, para construir um Mapa de Propagação (MP) do local monitorado. Para cada *sniffer+AP de referência*, o servidor de localização gera um mapa próprio, de forma que um total de k *sniffers* e N APs de referência, geram $(k \cdot N)$ MPs no servidor.

Esses mapas são compostos por um *grid* de duas dimensões que cobre toda a área do local monitorado e cujos pontos estão espaçados a uma distância igual a resolução do *grid*. É atribuída a cada local l (um local l é definido como sendo um ponto $[x, y]$ no *grid*) deste mapa uma distribuição de probabilidade $P(s|l)$, que define a probabilidade do *sniffer* medir, a partir do ponto fixo em que ele se encontra (lembrando que existe um mapa para cada par *sniffer+AP de referência*), um nível de sinal s dado que o transmissor está localizado em l. Em outras palavras, cada ponto l do mapa diz a probabilidade do *sniffer* em questão receber um nível de sinal s dado que um dispositivo hipotético estaria transmitindo a partir de l. Apesar do RSSI ser uma grandeza discreta, utilizou-se a distribuição Gaussiana para representar $P(s|l)$, em cada posição l (vide Capítulo 3):

$$P(s|l) = \frac{1}{\sigma_{(l)}\sqrt{2\pi}} \exp\left(-\frac{(s-\mu_{(l)})^2}{2\sigma_{(l)}^2}\right), \tag{4.1}$$

onde o parâmetro $\mu_{(l)}$ representa o valor esperado para o nível de sinal medido pelo sniffer em questão, dado que o transmissor está posicionado em l e $\sigma_{(l)}$ é o desvio padrão da distribuição. Para estimar a quantidade $\mu_{(l)}$ foi utilizado o modelo de propagação apresentado na Seção 3.4, tal que $\mu_{(l)}$ foi dado em função da distância de l (local onde hipoteticamente se encontra o transmissor) até o *sniffer* (receptor).

A idéia por trás da estimativa de $\mu_{(l)}$ está, de uma forma geral, em utilizar um modelo de propagação onde o RSSI fosse dado por uma função $RSSI(A, D)$, onde A é um valor que representa os parâmetros do local monitorado (decaimento em espaço livre, por exemplo) e D a distância entre transmissor em receptor. Quando se deseja localizar um dispositivo, esta função pode ser escrita na forma, $D(A, RSSI)$, onde os *sniffers* medem o RSSI vindo deste dispositivo e, de posse do parâmetro

A previamente medido para o local monitorado, calculam a distância até o mesmo. Escrevendo, agora, a função dada pelo modelo de propagação da forma $A(D, RSSI)$ é possível calcular o parâmetro A dinamicamente, uma vez que *sniffers* e APs são equipamentos fixos, o que indica que o parâmetro D também não se altera. Assim, os *sniffers* medem o RSSI dos APs e/ou estações sem fio fixas (cujas posições são conhecidas) e calculam o parâmetro A. Uma vez de posse deste parâmetro, eles medem os RSSIs dos dispositivos sem fio e calculam a distância D' (distância do *sniffer* até o transmissor cliente) para localizar os mesmos. Quando o mecanismo descrito na Seção 4.4 detecta alterações no parâmetro A, uma ordem pode ser enviada para que A seja recalculado. O parâmetro A, dinamicamente calculado, pode ser utilizado para estimar o nível de sinal recebido a partir de cada ponto de um *grid* que cobre todo o local monitorado, uma vez que as distâncias entre o *sniffer* e os pontos deste *grid* são fixas e conhecidas.

Desta forma, baseado no modelo de propagação dado pela Equação 3.3, podemos calcular $\mu_{(l)}$ para cada par *sniffer*+AP de referência, através de equação análoga:

$$\mu_{(l)}(d) = \mu_0(d_0) - 10n_0 log\left(\frac{d}{d_0}\right) - \alpha, \tag{4.2}$$

onde α (chamado de WAF (*Wall Attenuation Factor*) em [1]) representa o valor da atenuação provocada por obstáculos entre o transmissor localizado no ponto l e o *sniffer*. O valor d representa a distância entre o transmissor localizado no ponto $l = (x, y)$ e o *sniffer*, d_0 é a distância entre o AP de referência localizado no ponto $l_0 = (x_0, y_0)$ e o *sniffer*, n_0 indica a taxa de decaimento do sinal transmitido proporcional à distância e $\mu_0(d_0)$ é a média dos valores de RSSI aferidos pelo *sniffer* i a partir de seu respectivo AP de referência de índice n. $\mu_0(d_0)$ é descrito pela Equação 4.3.

$$\mu_0(d_0) = \mu_{i;n} \tag{4.3}$$

As distâncias d e d_0 são dadas pelas equações 4.4 e 4.5 respectivamente.

$$d = \sqrt{(|x_{sniffer} - x|)^2 + (|y_{sniffer} - y|)^2} \tag{4.4}$$

$$d_0 = \sqrt{(|x_{sniffer} - x_0|)^2 + (|y_{sniffer} - y_0|)^2} \tag{4.5}$$

Sendo o valor de $\mu_{(l)}$ (média da Equação 4.1) dado pela Equação 4.2, resta definir o valor do desvio padrão $\sigma_{(l)}$ da distribuição de RSSI para cada posição l do transmissor (desvio padrão da Equação 4.1). Assim como $\mu_{(l)}$, $\sigma_{(l)}$ também muda com a posição l do transmissor, no entanto, utilizou-se aqui $\sigma_{(l)} = \sigma_{i;n}$. O valor de $\mu_{(l)}$ pode ser estimado através de um modelo de propagação, mas o valor de $\sigma_{(l)}$ poderia ser determinado apenas através de medições empíricas realizadas em cada ponto l do local monitorado. Desta forma, para evitar essas medições (como na fase de calibragem), utilizou-se $\sigma_{(l)} = \sigma_{i;n}$. Essa igualdade fixa o valor de $\sigma_{(l)}$ para todo l como sendo o valor do desvio padrão calculado através dos níveis de sinal recebidos pelo sniffer i a partir do AP de referência n. Os resultados experimentais apresentados no Capítulo 6 mostram que essa é uma boa aproximação para $\sigma_{(l)}$.

Supondo que em cada ponto l do *grid* existe um transmissor hipotético, deseja-se encontrar $\mu_{(l)}$, que determina o valor esperado de nível de sinal medido pelo *sniffer* i, para cada um destes transmissores. A Figura 4.3 ilustra a aplicação do método proposto e as grandezas utilizadas no cálculo de $\mu_{(l)}$, em um exemplo onde $\mu_0(d_0) = \mu_{i;n}$ = -35 dBm e $\sigma_{i;n}$ = 2.8 dBm.

Em [1] os autores estudaram a aplicação de modelos de propagação para fins de localização e confrontaram os resultados obtidos com medições reais de nível de sinal em diversos pontos do local monitorado. A partir disso, concluiu-se que a utilização de modelos de propagação para estimar valores de RSSI neste tipo de sistema é uma alternativa simplificadora. Contudo é preterida em relação ao método empírico, quando se analisa apenas a acurácia do sistema de localização.

O principal argumento utilizado em trabalhos anteriores para não se utilizar modelos de propagação para fins de localização é o fato de que os parâmetros do modelo utilizado (parâmetros como índice de refração dos obstáculos, número de

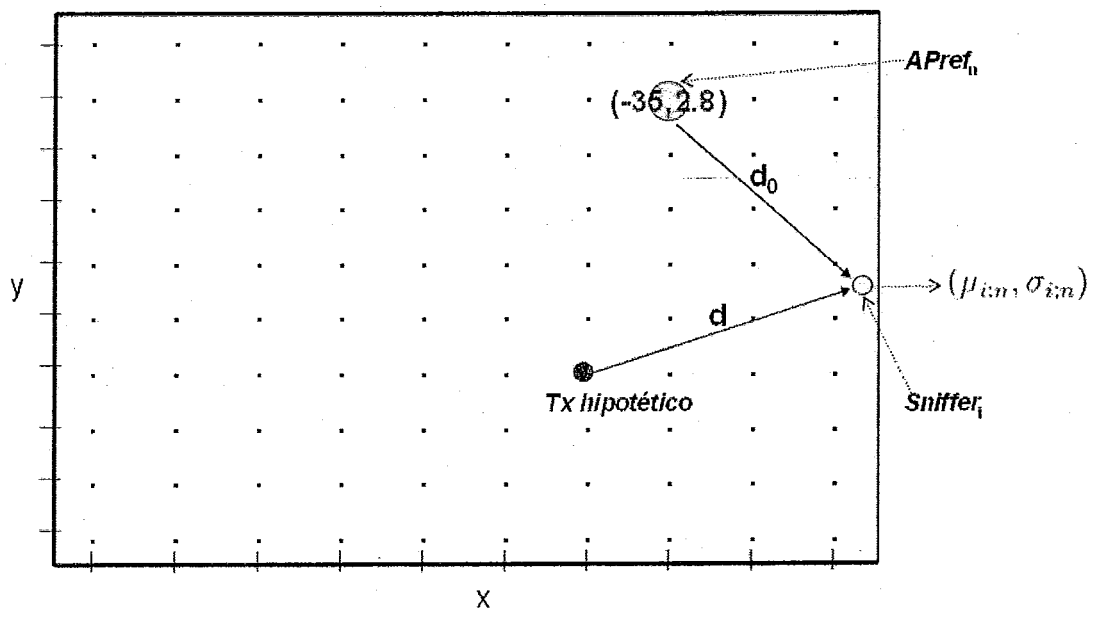

Figura 4.3: Exemplo de aplicação do método proposto.

obstáculos entre transmissor e receptor, parâmetros de decaimento em espaço livre e etc) podem mudar durante o funcionamento do sistema, aumentando o erro na estimativa da posição do usuário sem fio. No sistema proposto aqui, o mecanismo idealizado na Seção 4.4 pode ser utilizado para identificar alterações e recalcular dinamicamente os parâmetros do modelo de propagação utilizado.

4.4 Reconstrução do MP

Em trabalhos anteriores e nas medidas de RSSI apresentadas no Capítulo 3, claramente verifica-se que o RSSI segue uma distribuição normal cuja média μ e desvio padrão σ podem ser estimados para cada par *sniffer* + AP de referência. Assim, para o sistema proposto, é possível reconstruir o MP para cada par *sniffer* + AP de referência sempre que o *sniffer* k observar que RSSIs medidos a partir do seu ponto de acesso de referência i apresentam alterações estatísticas significativas. Em outras palavras, caso n em N medidas de RSSI seguidas estiverem fora do intervalo $(\mu_{k,i} + \sigma_{k,i}, \mu_{k,i} - \sigma_{k,i})$, um novo MP deve ser construído.

Uma alternativa ao procedimento de atualização do MP descrito acima é fazê-

lo a cada T segundos. Ou seja, periodicamente reconstruir o MP independente da existência de alterações estatísticas significativas. Esta segunda opção foi a utilizada nos experimentos relatados no Capítulo 6 de resultados. O motivo de se utilizar a reconstrução periódica está no fato de que caso não exista necessidade de reconstruir o MP (média e desvio padrão não têm alterações significativas), a reconstrução ocorrerá assim mesmo e os novos valores de $\mu_{k,i,t}$ e $\sigma_{k,i,t}$ serão muito próximos dos valores de $\mu_{k,i,t-T}$ e $\sigma_{k,i,t-T}$. Caso fosse necessário atualizar o MP devido a alterações nos valores de $\mu_{k,i,t}$ e $\sigma_{k,i,t}$ essa necessidade duraria, no pior caso, T segundos.

O mecanismo utilizado para comparar o MP, discutido neste capítulo, com os níveis de sinal medidos a partir dos dispositivos sem fio que se deseja localizar, será apresentado no capítulo seguinte.

Capítulo 5

O Modelo de Localização Proposto

ESTE capítulo apresenta o problema de estimar a localização de um dispositivo sem fio, sob um ponto de vista analítico e propõe uma solução para o mesmo baseado em uma combinação das características do sistema proposto neste trabalho, como a utilização de *sniffers* e o recálculo dinâmico do mapa de propagação, com conhecidos conceitos matemáticos como Regra de Bayes, Probabilidades Totais, independência de variáveis aleatórias e processos estocásticos [15].

A princípio apresenta-se formalmente o problema, alvo desta pesquisa, e definem-se alguns pontos importantes para o entendimento e tratamento do mesmo. Em seguida uma solução é dada, baseada em um modelo analítico. Por fim, métodos para melhorar a acurácia do estimador são propostos.

5.1 Descrição do Problema

Antes de descrever o problema de localização de um dispositivo sem fio a partir do sistema proposto no Capítulo 4, é necessário fazer algumas definições. Seja L um espaço físico bidimensional, a partir de cada posição $l \in L$, é possível obter medições de nível de sinal de k *sniffers* (receptores), dado um transmissor posicionado em l. Neste trabalho assume-se que L é discreto. Define-se assim, um espaço amostral S de k dimensões, onde cada elemento deste espaço é um vetor de dimensão k, cujas posições representam leituras de níveis de sinal feitas por k diferentes *sniffers*. Desta forma, amostras do espaço S são referenciadas por s.

O problema então, pode ser descrito como de máximo a *posteriori*, ou seja, dado um vetor de medições de nível de sinal $s = (s_1, s_2, ..., s_k)$, deseja-se determinar uma posição $l \in L$, tal que a probabilidade $P(l|s)$ seja maximizada. Pode-se dizer de forma mais explicita que $P(l|s)$ é a probabilidade de um transmissor estar localizado fisicamente em uma posição l, dado que medidas de nível de sinal s foram feitas por k *sniffers* diferentes.

Para este trabalho foi necessário assumir que as amostras colhidas para um determinado dispositivo sem fio, a partir de diferentes *sniffers* são independentes. Uma discussão a respeito desta suposição pode ser encontrada na Seção 5.3.

5.2 Estimador Proposto

A proposta apresentada aqui é uma modificação dos métodos descritos em [22, 23, 25]. Estes trabalhos foram discutidos no Capítulo 2, onde os autores consideram que um dispositivo móvel mede o nível de sinal recebido a partir de um determinado número de pontos de acesso e disponibiliza tais informações à uma entidade central (semelhante ao servidor de localização definido na Seção 4.2.2), para que esta estime sua posição.

Já no método proposto aqui, a idéia é de que não se pode esperar colaboração alguma por parte dos dispositivos móveis cuja posição deseja-se estimar. O que

se faz é medir o nível de sinal recebido por k *sniffers* a partir do dispositivo que se deseja localizar. De posse deste conjunto de dados (medições realizadas pelos *sniffers*) o servidor de localização pode estimar a posição do dispositivo sem fio através do modelo descrito a seguir.

Como mencionado anteriormente, dado um vetor de medições $s = (s_1, s_2, ..., s_k)$, deseja-se encontrar uma posição $l \in L$, tal que a probabilidade $P(l|s)$ seja maximizada. Aplicando-se a regra de *Bayes*, minimiza-se a probabilidade de erro e é possível encontrar a distribuição a *posteriori* da localização:

$$P(l|s) = \frac{P(s|l) \cdot P(l)}{P(s)} = \frac{P(s|l) \cdot P(l)}{\sum_{l' \in L} P(s|l') \cdot P(l')}; \tag{5.1}$$

onde o somatório segue através de todos os valores possíveis para posições $l \in L$. $P(s|l)$ é a probabilidade de um *sniffer* receber o sinal s, dado que o mesmo foi supostamente transmitido a partir de um local l. Em caso de um espaço L contínuo, a soma deverá ser substituída pela integral correspondente. $P(l)$ por sua vez, é a probabilidade a *priori* de se encontrar o transmissor em uma posição l, antes de conhecidas as leituras de níveis de sinal s, por parte dos *sniffers*. Este parâmetro pode ser usado em um mecanismo de localização para dar "peso" a determinadas posições mais prováveis de se encontrar um usuário (transmissor). Esta probabilidade a *priori* possibilita uma forma simples de incorporar ao sistema, informações sobre padrão de mobilidade e/ou rastreamento. Em outras palavras, é possível supor que usuários da rede podem ser encontrados de forma mais provável perto de mesas ou no interior de salas de aula ou de reunião, do que dentro de um banheiro, por exemplo. A probabilidade $P(l)$ poderia ser determinada, também, através de perfis de mobilidade, atendo-se ao fato de que se um usuário estivesse posicionado em um dado local, seria mais provável localizá-lo em alguma posição adjacente em um futuro próximo. Caso o perfil do usuário seja desconhecido ou simplesmente não seja utilizado, pode-se assumir que é igualmente provável encontrá-lo em qualquer das localidades $l \in L$. Sendo assim, $P(l)$ seria dada uniformemente sem apresentar tendências de encontro a qualquer posição l em particular.

$P(s|l)$ foi estimada para cada local $l \in L$, construindo-se assim um mapa, chamado aqui de *mapa de propagação (MP)* (ver Seção 4.3). Cada posição deste mapa possui a distribuição de probabilidade dos k *sniffers*, que integram o sistema, medirem os níveis de sinal $s = (s_1, s_2, ..., s_k)$, dado que um transmissor esteja posicionado neste local l do mapa. Na realidade, cada *sniffer* i possui seu próprio mapa de propagação. Cada posição deste mapa possui uma distribuição de probabilidade $P(s_i|l)$ que denota a probabilidade deste *sniffer* medir o nível de sinal s_i, dado que o transmissor estivesse, supostamente localizado na posição l. Neste trabalho, para estimar $P(s_i|l)$, em cada posição, foi utilizada uma distribuição Gaussiana, como já mencionado anteriormente no texto.

$$P(s_i|l) = \frac{1}{\sigma_{(l)}\sqrt{2\pi}} \exp\left(-\frac{(s_i - \mu_{(l)})^2}{2\sigma_{(l)}^2}\right) \tag{5.2}$$

Os valores $\mu_{(l)}$ e $\sigma_{(l)}$ são dados em função da posição l no mapa e denotam o nível de sinal médio e o desvio padrão percebido para esta posição, respectivamente. Estes valores, para cada posição do MP, são calculados a partir de um modelo de propagação escolhido, como visto na Seção 3.4. Os parametros deste modelo são estimados por medições realizadas pelo *sniffer* i a partir do sinal transmitido pelo ponto de acesso de referência (mencionado na Seção 4.2). A construção do MP foi abordada na Seção 4.3.

Assumindo que as medições realizadas pelos *sniffers* são independentes (ver Seção 5.3), pode-se escrever que:

$$P(l|s) = P(l|s_1, s_2, ..., s_k) = P(l|s_1) \cdot P(l|s_2) \cdot ... \cdot P(l|s_k) = \prod_{i=1}^{k} P(l|s_i); \tag{5.3}$$

onde $P(l|s_i)$ é dado pela equação 5.1. A equação 5.3 denota a probabilidade de um transmissor estar localizado na posição l, dado que k *sniffers* mediram os níveis de sinal a partir deste transmissor, criando o vetor $s = (s_1, s_2, ..., s_k)$. O resultado do estimador proposto poderá ser a posição $l \in L$ que proporcionar à equação 5.3 o maior valor. Na Seção 5.4, são propostas variações no estimador de forma a melhorar

a acurácia do sistema.

5.3 Independência Entre Amostras

Nesta seção será discutida a suposição de independência entre as amostras de sinal colhidas pelos *sniffers*. Tal suposição é importante para que seja possível simplificar o problema e chegar aos resultados obtidos na Seção 5.2.

Quando se fala na probabilidade de um transmissor estar em um local l, dado um vetor s, podemos escrever $P(l|s) = P(l|s_1, s_2, ..., s_k)$, onde s_i é o sinal medido pelo i-ésimo *sniffer*, em um cenário onde existem k *sniffers*. O sinal s_i varia com a distância entre transmissor (t_x) e receptor (r_x). Dado que a potência do t_x é constante, o sinal recebido s_i é função apenas das posições do par t_x/r_x e dos anteparos, objetos e pessoas no entorno destas posições. Assim, assume-se que as variações no nível de sinal recebido s_i, ao longo do tempo, são resultado de interferências causadas pela posição da dupla t_x/r_x.

O sinal recebido por um *sniffer* i é uma variável aleatória que segue um processo estocástico (definido em [15]). Qualquer mudança na posição do transmissor e/ou do *sniffer* define um processo estocástico diferente. Desta forma, pode-se assumir que, para um transmissor posicionado em um local $l \in L$, o nível de sinal s_i recebido por um *sniffer* i ao longo do tempo é uma variável aleatória independente de outra medição s_j realizada por um *sniffer* j, quando l_i e l_j são posições distintas. Assim, assumindo independência entre as medições de *sniffers* distintos, é possível escrever que $P(s_1, s_2, ..., s_k) = P(s_1) \cdot P(s_2) \cdot ... \cdot P(s_k)$. Este resultado foi utilizado na Seção 5.2 para o cálculo de $P(l|s)$ (Equação 5.3).

5.4 Acurácia do Sistema

Nas seções anteriores deste capítulo, foi descrita a técnica proposta para localizar dispositivos sem fio, baseada no nível de sinal recebido. Este método diferencia

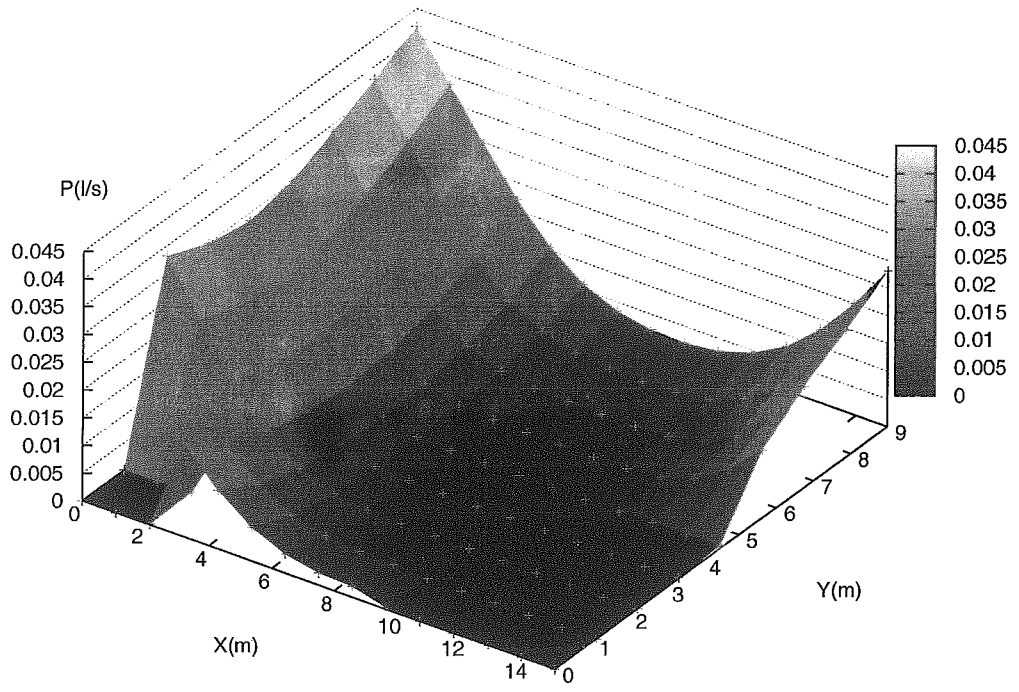

Figura 5.1: Distribuição de probabilidade de se encontrar o dispositivo transmissor em algum ponto l do *grid* sobre o local monitorado, calculada pela técnica proposta. Cada ponto possui uma probabilidade do transmissor estar em l, dado que os k *sniffers* mediram os níveis de sinal $s = (s_1, s_2, ..., s_k)$.

as posições possíveis no *grid* do local monitorado, calculando a probabilidade do dispositivo transmissor em questão estar localizado em cada um destes pontos. A Figura 5.1 mostra um exemplo da distribuição de probabilidade da localização de um dispositivo, calculada pela técnica proposta durante uma tentativa real de localização. Ainda assim, uma última questão permanece em aberto: *Baseado nestes cálculos, qual será a saída do estimador?* A técnica utilizada na estimativa de posição baseada na probabilidade $P(l|s)$ é de fundamental importância para a acurácia do sistema. Desta forma, foram utilizadas duas para estimar de forma mais acurada a localização dos dispositivos: *Janela de Estimativas* e *Centro de Massa.*

5.4.1 Janela de Estimativas

A primeira proposta para melhoria na acurácia baseia-se em escolher o ponto l do *grid* mais provável de se encontrar o transmissor, dado um vetor de medições $s = (s_1, s_2, ..., s_k)$, para k *sniffers*. O exemplo observado na Figura 5.1 mostra um *grid* formado por pontos espaçados de 1 metro, sobre o local monitorado de dimensões $16m$ x $10m$. É possível observar que o ponto de maior probabilidade é o $(0, 9)$, resultado da estimativa. Esse resultado é então computado como sendo a saída do sistema.

Na medida em que os *sniffers* medem novos valores de RSSI, as probabilidades em cada ponto do *grid* são recalculadas e modificadas ao longo do tempo. Em algumas ocasiões, diversos pontos l diferentes podem possuir valores de $P(l|s)$ próximos, sendo que o maior valor pode, na verdade, ser encontrado em um ponto distante da posição real do dispositivo sem fio que se deseja localizar, o que caracteriza um erro grande. Um exemplo deste fenômeno pode ser visto na Figura 5.2.

Durante experiências realizadas, um transmissor (*notebook* equipado com interface sem fio) foi colocado em 10 posições diferentes escolhidas aleatoriamente no laboratório. Para cada uma destas posições foram feitas 500 estimativas de posição pelo sistema, gerando um total de 5000 estimativas de localização. Estas experiências preliminares mostraram que casos como o representado na Figura 5.2 (um gráfico como este é gerado a cada estimativa) são comuns mas, menos freqüentes que situações de acerto como na Figura 5.1. Estas imagens foram geradas a partir de duas estimativas espaçadas por apenas 1 segundo (nesta experiência o sistema gerava uma estimativa a cada 0.5 segundos), o que mostra a grande volatilidade do sinal medido e a capacidade de adaptação do mecanismo proposto. A situação de erro, como observada na Figura 5.2, não permanece por muito tempo e estatisticamente ocorre poucas vezes comparando-se com situações de erro pequeno, como pode ser visto a seguir.

Notou-se também que em situações onde o erro é grande, como na Figura 5.2, a probabilidade $P(l|s)$ é pequena e que quando a probabilidade é grande, existe um

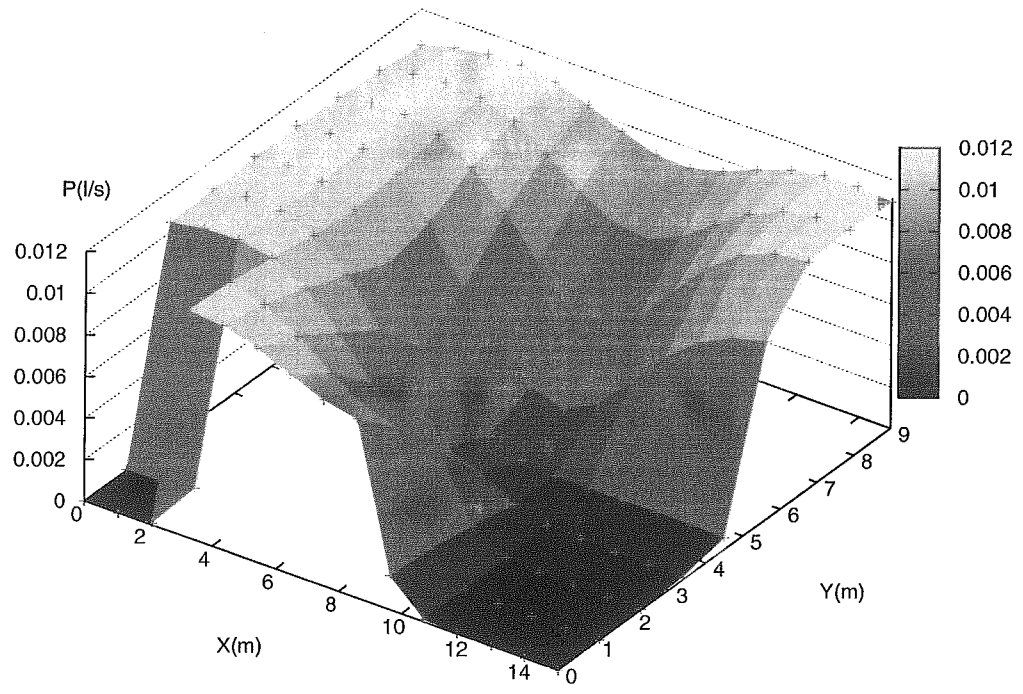

Figura 5.2: Distribuição de probabilidade de se encontrar o dispositivo transmissor em algum ponto l do *grid* sobre o local monitorado, quando ocorre um erro na estimativa de posição. Este erro é provocado por interferência momentânea nas medições dos *sniffers*.

destaque maior para um determinado ponto do *grid* (como na Figura 5.1) e o erro é pequeno. Isso pode ser visto claramente na Figura 5.3, onde quando a estimativa de posição tem probabilidade maior, o erro é menor e quando o erro é maior, a probabilidade é menor. Não se pode afirmar nada quando a probabilidade é baixa. Porém, esses resultados motivaram uma variação da proposta original.

Cada vez que o sistema proposto gera uma saída (grava no banco de dados coordenadas $[x, y]$ da posição l estimada), ele deve calcular as probabilidades $P(l|s)$ para todo $l \in L$ e gerar dados como observados nas Figuras 5.1 e 5.2. Assim, cada estimativa gera uma saída.

Foi proposta então uma variação que consiste em gerar uma saída a cada W estimativas, de forma que W *seria o tamanho da Janela de Estimativas.* Ou seja,

para $W = 10$, seriam geradas 10 estimativas de posição l. O sistema então, verificaria qual dessas 10 estimativas possui o maior valor de probabilidade $P(l|s)$ e apenas essa posição seria escolhida como saída do sistema. De forma que $W = 10$ corresponde a uma saída para cada 10 estimativas e $W = 1$ é o cenário original onde cada estimativa gera uma saída.

Esta variação funciona como um "filtro" e causa impacto nos resultados de duas formas: no tempo de resposta e no erro médio (acurácia). O primeiro, devido ao fato de que cada saída demoraria o tempo de calcular W estimativas e não mais seria gerada uma saída para cada estimativa. O segundo, pelo fato de que os erros maiores por serem, na grande maioria das vezes, associados a pequenas probabilidades $P(l|s)$ seriam filtrados e descartados. O valor de W seria então um parâmetro do sistema utilizado para "ajustar" o compromisso entre acurácia e tempo de resposta. O sistema proposto foi então, avaliado para valores de janela $W = 1$ e $W = 10$ e resultados comparativos serão apresentados no Capítulo 6.

5.4.2 Centro de Massa

A técnica descrita na seção anterior, pode ser considerada um estimador discreto, pois aponta como saída do sistema apenas pontos sobre o *grid* (neste trabalho, espaçados de 1 metro). Já a técnica apresentada nesta seção, pode ser considerada um estimador contínuo, por fornecer uma saída do sistema em qualquer coordenada $[x, y]$, para x e y contínuos. O *Centro de Massa* CoM (*Center of Mass*) foi utilizado previamente em [25] e foi utilizado aqui como o estimador contínuo do sistema.

A idéia básica por trás desta técnica é tratar cada local l do *grid* como um objeto no espaço físico, cuja massa é igual a probabilidade normalizada $P(l|s)$ calculada para todo $l \in L$, pelo modelo proposto na Seção 5.2. Por comodidade, a probabilidade $P(l|s)$ será tratada aqui de m ($P(l|s) = m$). Assim, sendo m_i a massa do local l_i, podemos definir a saída do sistema como sendo um local Z (o centro de massa) dado pela Equação 5.4, tal que $\overline{L}$ é uma lista de todos os locais do *grid*, ordenados de forma decrescente de acordo com a probabilidade normalizada de cada um. Através

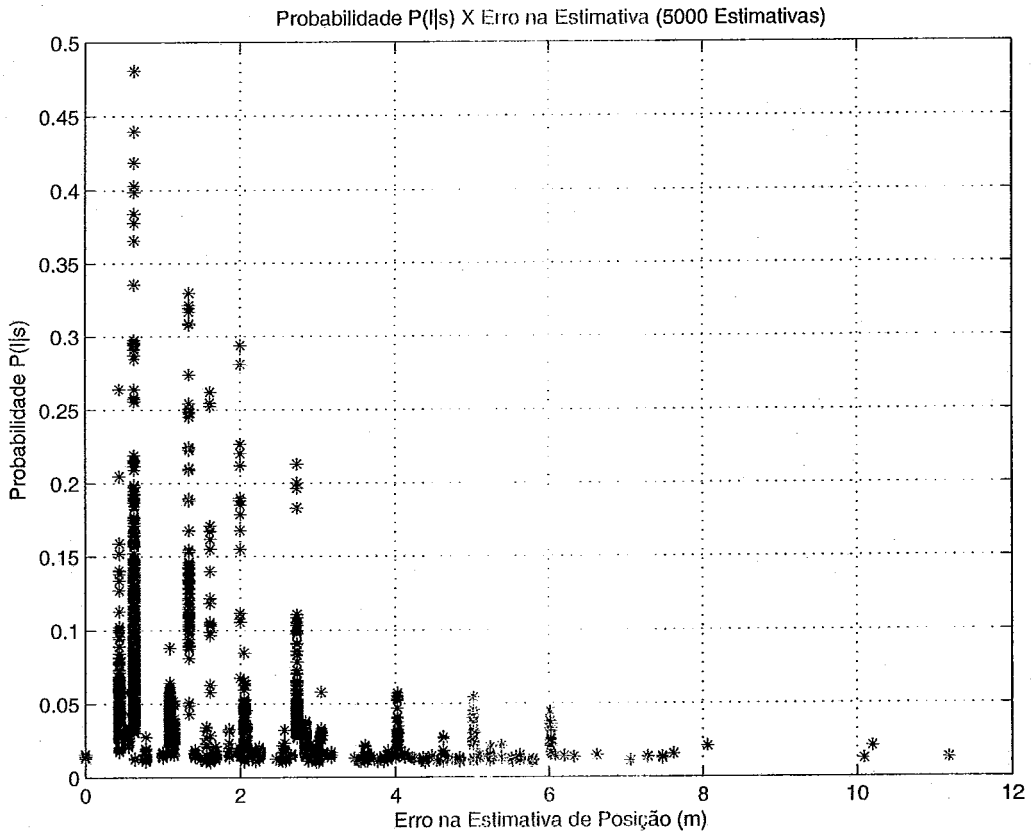

Figura 5.3: Dispersão das 5000 estimativas. Cada estimativa está associada a uma probabilidade $P(l|s)$ e a um erro.

desta equação, pode-se obter o centro de massa para os N objetos (locais) de maior massa, onde N é um parâmetro do sistema, tal que $1 \leq N \leq ||\overline{L}||$. Mais explicitamente, as coordenadas x e y do centro de massa Z são dadas pelas Equações 5.5 e 5.6, onde $m_1 > m_2 > ... > m_N > ... > m_{||\overline{L}||}$. O leitor deve notar que para o caso particular onde $N = 1$, a técnica de CoM é equivalente a Janela de estimativa para $W = 1$.

$$Z = \frac{\sum_{i=1}^{N} m_i \cdot \overline{L}(i)}{\sum_{i=1}^{N} m_i}; \tag{5.4}$$

$$Z_x = \frac{x_1 \cdot m_1 + x_2 \cdot m_2 + ... + x_N \cdot m_N}{\sum_{i=1}^{N} m_i}; \tag{5.5}$$

$$Z_y = \frac{y_1 \cdot m_1 + y_2 \cdot m_2 + ... + y_N \cdot m_N}{\sum_{i=1}^{N} m_i}; \tag{5.6}$$

No capítulo seguinte, a implementação do modelo de localização proposto será discutida. O ambiente de testes do sistema implementado será descrito e resultados gerados serão apresentados, seguidos de comentários pertinentes.

Capítulo 6

Resultados Experimentais

NSTE capítulo encontram-se os resultados obtidos após a implementação do mecanismo de localização proposto. Primeiramente serão apresentados os resultados com relação a acurácia do sistema descrito neste trabalho. Alguns parâmetros do sistema foram alterados de forma que fosse possível avaliar o impacto dos mesmos no erro da estimativa de localização. Em seguida, o sistema proposto é comparado com outros métodos de localização já consagrados e freqüentemente referenciados na literatura.

6.1 Procedimento e Ambiente Experimental

Para avaliar as técnicas propostas, um ambiente de testes foi montado em laboratório. Interfaces sem fio foram instaladas em 3 estações de trabalho (máquinas de produção do laboratório) sob o sistema operacional Linux, controladas pelo *driver* da Orinoco [40]. O *software* do *sniffer* foi instalado e configurado em cada uma dessas estações. Uma quarta estação de trabalho Linux foi utilizada para desempenhar as funções do servidor de localização e do banco de dados. O *software* do servidor de localização foi instalado e configurado para utilizar o banco de dados MySQL [39], também presente nesta mesma máquina. Uma outra estação de trabalho foi configurada para funcionar como um ponto de acesso sem fio. Esta última possuía uma interface de rede sem fio com adaptador para barramento PCI (*Peripheral Component Interconnect*), sistema operacional OpenBSD e o *driver hostap* [41]. Todas estas estações já estavam interconectadas por uma infraestrutura de rede cabeada pré-existente, de forma que apenas as interfaces sem fio precisaram ser instaladas. Os dispositivos sem fio clientes, cujas posições seriam estimadas, foram representados por um *notebook* com interface PCMCIA (*Personal Computer Memory Card International Association*) e por uma estação de trabalho com interface PCI. O ambiente de testes ficou então, como mostrado na Figura 6.1.

Este ambiente foi montado dentro de um local de dimensões $16m$ x $10m$, cujo mapa e disposição dos equipamentos pode ser visto na Figura 6.2. Nesta figura, os *sniffers* são representados por quadrados, o ponto de acesso por um triângulo e os dispositivos sem fio detectados (dispositivos cliente), por um círculo. No exemplo desta figura, apenas um dispositivo cliente foi encontrado e localizado. As posições dos *sniffers* e do ponto de acesso são conhecidas e não se alteram durante os experimentos.

Para coleta dos resultados apresentados neste capítulo, os dispositivos clientes sem fio (*notebooks* e estações de trabalho) foram dispostos em 10 posições $[x, y]$ diferentes dentro do perímetro do laboratório e suas posições foram estimadas pelo sistema proposto 500 vezes para cada posição, para cada uma das técnicas propostas na Seção 5.4 e suas variações. Ou seja, 500 saídas do sistema foram dadas para cada

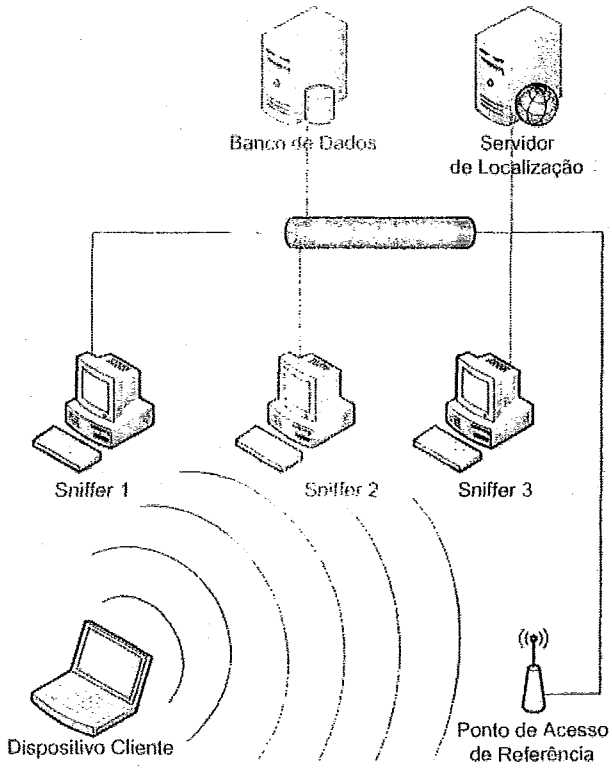

Figura 6.1: Ambiente de testes utilizado na avaliação de desempenho do mecanismo de localização proposto.

uma das 10 posições, totalizando 5000 estimativas de posição para cada uma das técnicas utilizadas (para W=1, W=10 e CoM). A Tabela 6.1 trás um resumo dos valores dos parâmetros do sistema utilizados nos experimentos.

6.2 Avaliação da Acurácia do Sistema

Uma vez montado o ambiente descrito na seção anterior e de posse dos dados de localização gerados a partir dos experimentos descritos acima, foi necessário definir uma métrica para se avaliar a acurácia do estimador proposto e das técnicas de localização utilizadas. Assim, a métrica utilizada neste trabalho para avaliação do sistema foi, naturalmente, o erro na estimativa de localização. Este erro foi definido como a distância (em metros) entre o ponto $[x, y]$ indicado na saída do estimador e a real posição do dispositivo sem fio. Deseja-se assim que o erro seja o menor possível.

Parâmetro	Descrição	Valor
α	Atenuação por obstáculos	0
n_0	Const. de Decaimento[1]	2.6
T	Tempo de Reconstrução do MP	10 segundos
Res. do Grid	Espaçamento entre pontos do grid	1 metros
(X_{max}, Y_{max})	Dimensões do Local	$(16m, 10m)$
M	Número de *beacons* capturados	60
N	Número de Pontos utilizados no CoM	5
IC	Intervalo de Captura	1 segundos
$P(l)$	Probabilidade *a priori*	Uniforme

Tabela 6.1: Parâmetros utilizados nos experimentos para a geração dos resultados apresentados.

Foram traçadas então, de forma empírica, as funções de distribuição cumulativas (ECDF - *Empirical Cumulative Distribution Function*) do erro na estimativa de localização para cada uma das técnicas descritas na Seção 5.4. A Figura 6.3 mostra estas distribuições.

O comportamento de "escada" da curva W=1 e W=10, difere do comportamento mais suave da curva CoM, pois as duas primeiras são variações de um estimador discreto e a última mostra o resultado de um estimador contínuo, onde o erro pode assumir infinitos valores. No caso do estimador discreto, para o *grid* utilizado nestes experimentos com 160 pontos (16m x 10m = 160, para uma distância entre pontos de 1m), dada a posição real do transmissor, o valor de erro na estimativa poderá assumir 160 valores diferentes, uma vez que o erro é dado pela distância entre a posição real e o ponto indicado pelo estimador e que o estimador discreto só indica como saída pontos do *grid*.

É possível notar o ganho quando se utiliza o parâmetro W=10 no lugar de W=1. Esse ganho pode ser visto também nos valores mostrados na Tabela 6.2. Esta resume os resultados encontrados para as diferentes técnicas nos pontos 50, 75 e 90 percentil da ECDF do erro de localização. É possível perceber uma ligeira

vantagem para W=10 em relação as outras técnicas, quando se olha apenas o ponto de 90 percentil, mas nota-se que o CoM apresenta uma considerável vantagem em relação ao método da janela de estimativas para os pontos 50 e 75 percentil. Em média, nestas avaliações, W=10 e CoM apresentaram desempenhos semelhantes.

É importante citar que os experimentos foram realizados durante horário comercial onde existia constante movimentação de pessoas e alteração no número de presentes, dentro do local monitorado. Como visto nas Figuras 3.4 e 3.3, a simples presença e o trânsito de pessoas no local provoca alterações bruscas e constantes no nível de sinal recebido. Os resultados apresentados nesta seção demonstram a grande capacidade que o método de localização proposto tem para se adaptar as variações do RSSI. Mesmo com o trânsito de pessoas, o sistema apresenta 75% do tempo erro abaixo de 2 metros e 90% do tempo erro abaixo de 3.8 metros, quando se utiliza CoM.

Técnica	**50%**	**75%**	**90%**	**Erro Médio**
W = 1	2.0000	2.8284	4.0000	2.0650
W = 10	1.6124	2.7203	3.6056	1.8350
CoM	1.2341	1.9529	3.8203	1.6980

Tabela 6.2: Valores de 50, 75 e 90 percentil da distribuição cumulativa empírica do erro de localização, para cada técnica utilizada na escolha da saída do estimador. Os valores de erro reportados são dados nesta tabela, em metros.

Na Figura 6.4 pode-se observar a freqüência com que o erro ocorre para as diferentes técnicas utilizadas. Percebe-se que para erros menores ou iguais a 1 metro, W=10 leva certa vantagem com aproximadamente 37% das estimativas nesta faixa, contra 20% quando se utiliza CoM. No entanto, 77% das estimativas realizadas com CoM apresentaram erros menores ou iguais a 2 metros, enquanto que W=10 apresentou 54% das estimativas dentro desta faixa de erro. Para 77% das estimativas, W=10 apresenta erros menores ou iguais a 2.8284 metros.

É importante mencionar que antes de iniciados os experimentos descritos neste capítulo, propositalmente não foi realizado qualquer estudo com relação ao posicio-

namento de *sniffers* e pontos de acesso de referência, que proporcionassem resultados mais acurados. Os *sniffers* foram implantados em estações de trabalho utilizadas no cotidiano do laboratório onde o sistema foi implantado, sem que qualquer equipamento fosse movido de lugar. O objetivo por trás disso é mostrar que o sistema proposto pode alcançar bons resultados em termos de acurácia, utilizando-se uma infra-estrutura de rede (tanto com fio, quanto sem fio) já existente, sem que qualquer aspecto da rotina[2] de trabalho dos usuários desta rede fosse afetada e sem aumento de custos de implementação.

6.3 Comparação com Outros Mecanismos de Localização

Analisando as seções anteriores, fica claro que foi alcançado o objetivo de construir um modelo capaz de localizar um dispositivo sem fio com boa acurácia, de baixo custo, que utiliza uma infraestrutura de WLAN pré-existente e que funciona sem intervenção humana. Assim, nesta seção é possível observar de que forma o presente trabalho contribui com a pesquisa na área de localização, através de comparações entre o mecanismo proposto aqui e outros trabalhos semelhantes. Os pontos principais a serem considerados nesta comparação são: área monitorada, acurácia e custo da solução.

Utilizar custo como métrica de comparação, muitas vezes, pode parecer pouco objetivo, uma vez que algo que parece ter custo alto para alguém com poucos recursos, pode não ser tão caro para alguém com recursos abundantes. No entanto é sempre importante avaliar o custo de uma solução (em qualquer área de atuação), seja ele financeiro ou em termos de tempo consumido, dado que uma solução pode ser inviabilizada caso a relação custo/benefício seja considerada alta demais para uma determinada aplicação.

[2]Entenda-se por mudança na rotina novo software a ser instalado/utilizado, novo trabalho a ser realizado com na demorada fase de calibragem ou com movimentação de máquinas de seus locais de trabalho habituais.

É importante notar também que comparar sistemas de localização somente através de métricas de erro (50, 75, 90 percentil e/ou erro médio) pode levar a conclusões equivocadas. Devido a vasta diferença entre os ambientes onde os experimentos foram realizados (diferentes áreas, número de pessoas transitando e obstáculos), parâmetros utilizados e métricas reportadas, fica muito difícil fazer uma comparação direta entre técnicas.

Desta forma, dividiu-se esta seção em duas partes. A princípio será apresentada uma comparação qualitativa, onde será possível avaliar em quais soluções apresentam-se qualidades desejáveis e/ou desvantagens. Em uma segunda seção, uma métrica proposta em [8] é utilizada na avaliação. Esta métrica procura quantificar a relação custo/benefício, da implementação de cada técnica. Os trabalhos utilizados para este fim foram comentados no Capítulo 2 e são aqui novamente relacionados. São eles o RADAR [1], LEASE [8], Ref. [22], além da técnica proposta aqui. Os resultados das comparações são então comentados.

6.3.1 Comparação Qualitativa com Outros Mecanismos de Localização

Esta seção se dedica a comparar, de forma qualitativa, o método de localização proposto aqui com alguns dos sistemas mais referenciados na literatura. A Tabela 6.3 a seguir reúne algumas das características mais importantes encontradas e esperadas nestes trabalhos, tornando fácil uma comparação. As métricas que compõe a Tabela 6.3 são relacionadas abaixo junto a uma breve descrição das mesmas, o que torna mais claro o objetivo destas comparações.

- **Fase *off-line*** - Esta métrica indica o custo relacionado ao tempo gasto para construção do modelo de localização em cada solução. Este tempo, dado aqui em minutos, é função da área monitorada pelos sistemas e do número de pontos utilizados na fase *off-line*. Aqui é considerado apenas o tempo indicado em cada um dos trabalhos citados no melhor caso, ou seja, quanto tempo de calibragem foi necessário para atingir o melhor resultado de estimativa (menor

erro). Em poucas palavras, esta métrica indica o custo em tempo das soluções avaliadas.

- **Reconstrução do Modelo** - Indica se existe a necessidade de que o modelo de localização utilizado seja reconstruído periodicamente e se essa reconstrução é realizada de forma manual - *man* (com grande interação humana) ou automática - *auto*. Vale lembrar que uma reconstrução no modelo implica em nova fase de calibragem, para as técnicas que depemdem deste procedimento.

- **Número de Dispositivos** - Cada sistema necessita de um certo número de dispositivos sem fio para realizar as estimativas de localização. Estes dispositivos são APs, *sniffers* e emissores estáticos [8]. Esta métrica indica o custo financeiro das soluções avaliadas.

- **Usuário com Antena** - Muitas vezes, redes sem fio sofrem ataques que partem de dispositivos conectados a antenas com alto ganho. É comum, hoje em dia, que atacantes utilizem até mesmo antenas caseiras, confeccionadas dentro de latas de batata frita, latas de óleo de cozinha e até mesmo panelas e frigideiras. Desta forma, um atacante pode utilizar a rede sem fio a maiores distâncias, fazendo com que o sistema de localização estime sua posição, mais próximo do que ele realmente esta. Uma vez que o atacante está utilizando uma antena, o nível de sinal recebido por outros dispositivos será maior. Sistemas que utilizam a qualidade do sinal de RF (RSSI) para estimarem a posição física de dispositivos sem fio sofrem com este problema. Uma solução para isso seria a utilização de técnicas como *time difference o arrival* (TDOA).

- **Software no Cliente** - Algumas das soluções analisadas neste trabalho necessitam de software específico instalado nos clientes. Estes softwares coletam informações sobre o sinal de RF e utilizam-nas para auxiliar nas estimativas de posição dos próprios clientes. Esta métrica indica a necessidade de cada solução da utilização/instalação de software no cliente.

- **Detecta não Autorizados** - Indica apenas se o sistema é capaz de detectar a presença de dispositivos não autorizados, incluindo tentativas de ataque e

rogue access points[3]

- **Erro 50 percentil** - Indica o erro, em metros, reportado na referência bibliográfica do sistema indicado para o melhor caso no ponto da curva ECDF 50 percentil.

Método	Fase *off-line* (min.)	Reconst. do Modelo	No. de Disp.	Usuário com Antena	Software no Cliente	Detecta não Autoriz.	Erro 50 Percentil
RADAR	25	man	3	não	sim	não	2.94
Ref. [22]	550	man	4	não	sim	não	1.07
LEASE	0	auto	38	não	não	sim	3.17
Proposta	0	auto	4	não	não	sim	1.29

Tabela 6.3: Comparação qualitativa entre o modelo proposto e outros mecanismos de localização.

Como se pode ver pela Tabela 6.3, a exemplo do que acontece com todos os outros métodos de localização baseados em RF estudados, o mecanismo proposto não é capaz de localizar dispositivos que utilizam antenas diretivas, ou outros artifícios que possam alterar o valor RSSI recebido.

No entanto, ele é capaz de detectá-los, uma vez que utiliza *sniffers*. Tanto o sistema proposto quanto o sistema LEASE tem essa capacidade, pelo fato de trabalharem independentemente de ações realizadas nos clientes. Mesmo em ocasiões onde não é possível localizar o dispositivo transmissor, uma aplicação voltada para área de segurança da informação (um IDS - *Intrusion Detection System*, por exemplo) poderia utilizar o sistema de detecção do mecanismo proposto para acionar algum alarme para o administrador de rede.

[3] *Rogue access point* é um ponto de acesso conectado clandestinamente (sem o conhecimento dos administradores da rede) a rede de uma empresa e funciona como uma "porta dos fundos" para que atacantes possam ter acesso aos serviços de rede da empresa através desta infraestrutura sem fio.

Outra característica comum ao sistema proposto e ao sistema LEASE, perceptível através Tabela 6.3 é o fato de ambos não possuírem fase de calibragem. Mais uma vez, devido a utilização de *sniffers* em ambos os sistemas, o modelo de localização é construído automática e periodicamente. Essa característica peculiar, garante a ambos a habilidade de se auto-corrigirem a fim de minimizar o erro na estimativa de posicionamento. O mecanismo de auto-correção proposto neste trabalho foi descrito na Seção 4.4.

Em sistemas que dependem de fase de calibragem, em uma situação comum onde uma pessoa passa (ou qualquer anteparo é colocado) na frente do ponto de acesso que auxilia na localização, o impacto desta situação corriqueira seria arrasador em termos da acurácia nas estimativas de posição. Assim, um cliente sem fio passaria a fazer leituras de valores de RSSI mais baixos, uma vez que algum anteparo esteja posicionado entre o AP e o cliente que realiza essas medições de RSSI. Com leituras de RSSI alteradas (atenuadas pelo anteparo), o sistema de localização assumirá que a distância entre cliente e AP é maior do que na realidade é, contribuindo para um aumento no erro de posicionamento. Para resolver este problema, um novo processo de calibragem deveria ser realizado. Em alguns sistemas este processo poderia significar desde um pequeno atraso em alguma tarefa do dia-a-dia (aproximadamente meia hora no caso do RADAR), até a perda de um dia inteiro de trabalho (no caso da Ref. [22]). No sistema proposto, quando uma situação parecida ocorre, o modelo de localização é reconstruído e a interferência é levada em consideração, adaptando automaticamente o sistema ao novo ambiente.

Para os trabalhos estudados neste capítulo (com exceção do LEASE), dados de RSSI foram coletados em pontos (pontos do *grid* do modelo de localização) localizados apenas em corredores. A área aberta de corredores geralmente é mais amigável em relação a propagação de sinal. Não existem relatos nestes trabalhos (mais uma vez, com exceção do LEASE) de tentativas de localização dentro de salas e/ou laboratórios. Em [8] isso também é discutido. A Figura 6.5 mostra o *grid* utilizado na construção do modelo de localização proposto no RADAR e os pontos de acesso (BS - *Base Station*), também localizados nos corredores.

6.3.2 Comparação Quantitativa com Outros Mecanismos de Localização

De forma resumida, pode-se dizer que com o mecanismo proposto, foi possível chegar a resultados de acurácia próximos (melhores em muitos casos) aos dos melhores e mais referenciados mecanismos presentes na literatura, sem o custo adicional de tempo gasto e com pouquíssimo custo em equipamentos. No entanto, como dito anteriormente, fica muito difícil fazer uma comparação direta entre técnicas, olhando-se apenas para métricas de erro nas estimativas, devido a vasta diferença entre os locais onde os experimentos são realizados. Diferentes áreas, número de pessoas transitando, obstáculos, anteparos e outros equipamentos que causam interferência eletromagnética, são fatores que influenciam na acurácia das estimativas de localização.

Neste contexto, em [8] foi proposta uma métrica para se avaliar o quão efetiva é a técnica utilizada. Com esta métrica, os autores procuraram refletir os seguintes aspectos das soluções propostas:

- A extensão do trabalho realizado para construir o modelo;
- O erro na estimativa de localização obtido com a técnica utilizada;
- O quão dinâmico é a propagação de sinal no local monitorado;
- A capacidade de adaptação da solução proposta;

Com isso, foi definida em [8] uma quantidade chamada *"erro efetivo normalizado"* ε que procura levar em consideração algumas das questões relacionadas acima. Assim, ε foi definido como na Equação 6.1, onde m é uma métrica referente ao erro na estimativa tal como o erro a 50 percentil, A é a área do local monitorado e k é definido como o número de pontos utilizados para construir o modelo de localização. O valor de k indica o custo (em tempo e/ou dispositivos) na construção do modelo. Os parâmetros i e j permitem dar peso e enfatizar o custo na construção do modelo ou o erro associado a cada técnica.

$$\varepsilon(i,j) = \frac{ck^i m^j}{A}; \tag{6.1}$$

A Tabela 6.4 resume os dados utilizados para o cálculo da métrica de erro efetivo ε, assim como os valores calculados para ε. Para os valores de k indicados nesta tabela, foram utilizados os mesmos de acordo com as indicações de [8]. Para o sistema proposto aqui utilizou-se $k = 4$ (3 *sniffers* + 1 AP). Os valores dos parâmetros i e j utilizados aqui foram os mesmos das comparações realizadas em [8], $i = 1$ e $j = 3$. Para os mecanismos RADAR e Ref. [22], foram utilizados $k = 70$ e $k = 110$ respectivamente, pois são o número de pontos nos grids utilizados na fase de calibragem de ambos. Para o sistema LEASE [8], os autores experimentaram 3 variações do sistema, com quantidades diferentes de equipamentos (12, 28, 38). Estas quantidades incluem a soma do número de *sniffers* com emissores estáticos (dispositivos que apenas transmitem pacotes periodicamente) e pontos de acesso utilizados para auxiliar na localização.

Mecanismo	**Erro 50 percentil** (m)	**Valor** k	A (m^2)	ε
RADAR	2.94	70	978.75	1.81747
Ref. [22]	1.07	110	1767.51	0.07624
LEASE(12)	4.57	12	3009.97	0.38051
LEASE(28)	3.66	28	3009.97	0.45608
LEASE(38)	3.17	38	3009.97	0.40216
Proposta	1.29	4	160	0.00285

Tabela 6.4: Comparação quantitativa entre o modelo proposto e outros mecanismos de localização.

O valor mais baixo de ε calculado para o mecanismo apresentado aqui mostra que esta é uma proposta promissora. Ela também sugere que a técnica de reconstrução automática e periódica do modelo de localização realiza bem o trabalho de corrigir as flutuações de nível de sinal comuns em um ambiente sem fio.

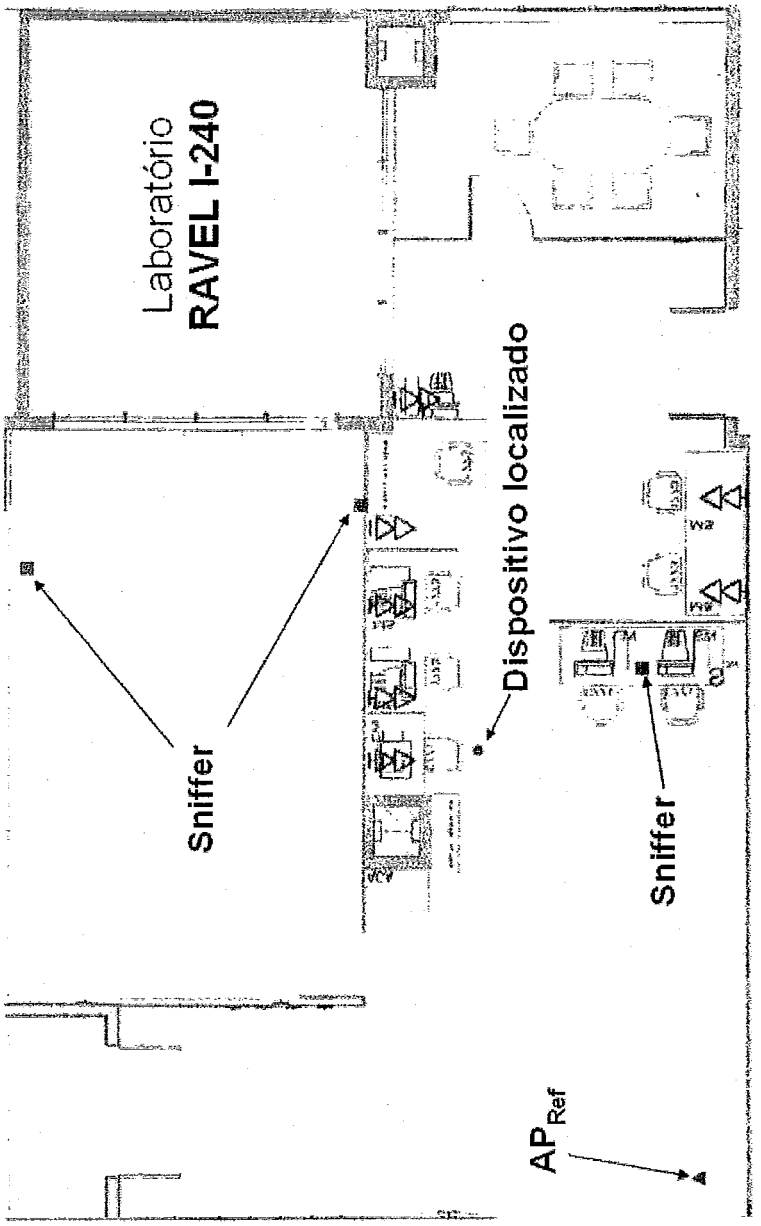

Figura 6.2: Mapa do local monitorado e disposição dos equipamentos sem fio.

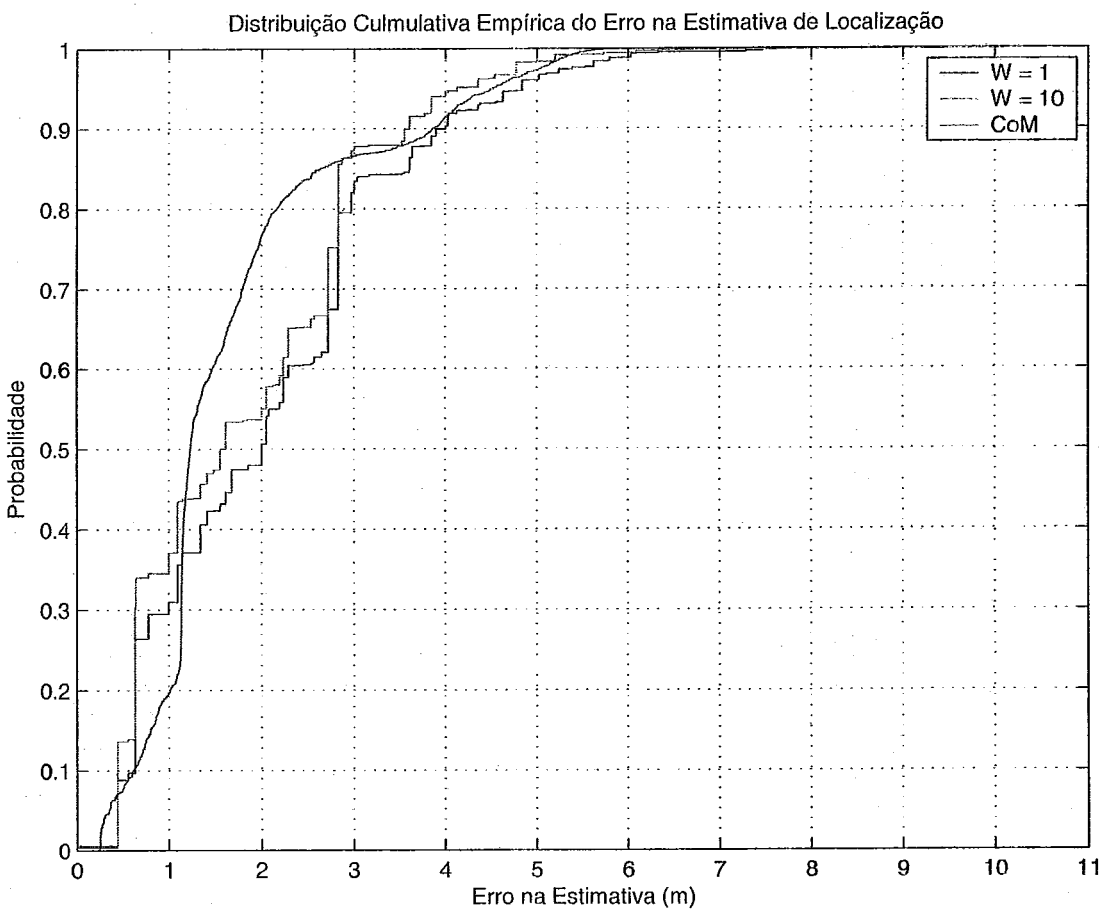

Figura 6.3: Distribuição cumulativa empírica de probabilidade do erro na estimativa de posição.

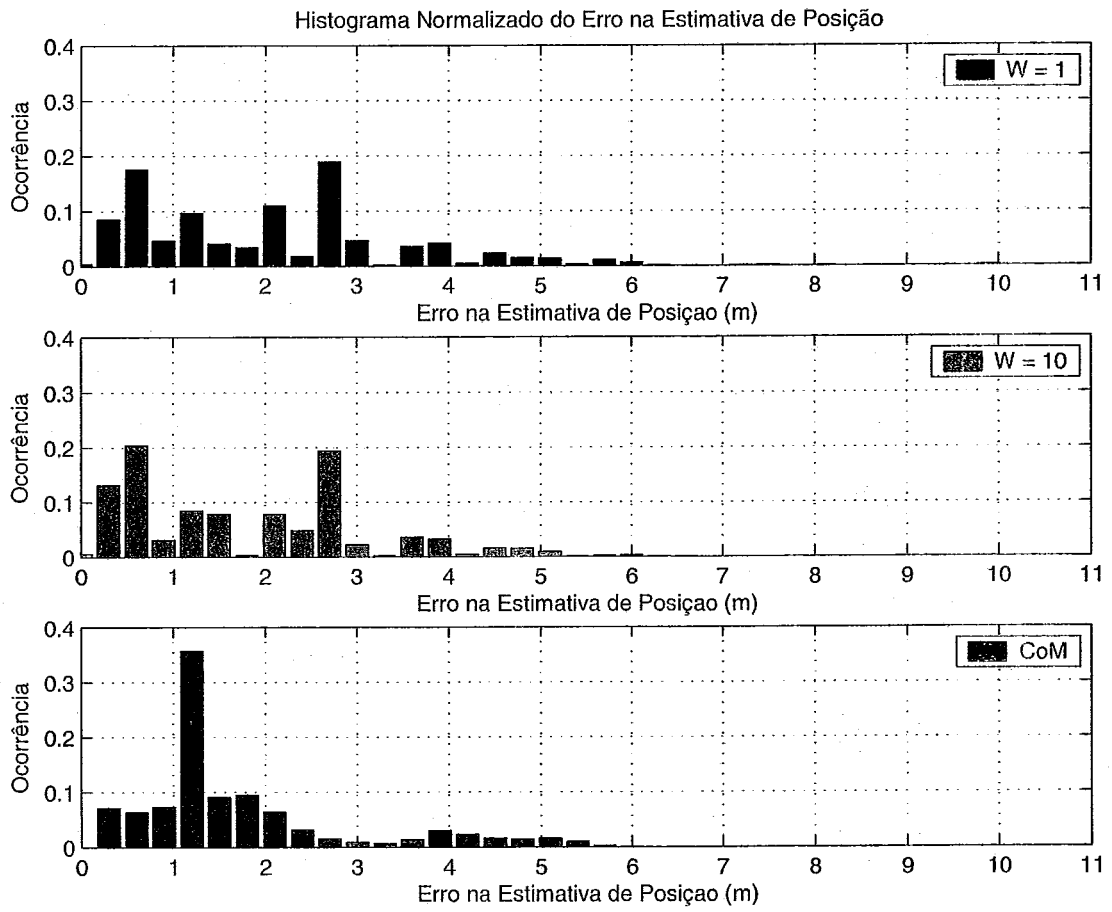

Figura 6.4: Histograma normalizado do erro na estimativa de posição para variações nas técnicas de estimativa.

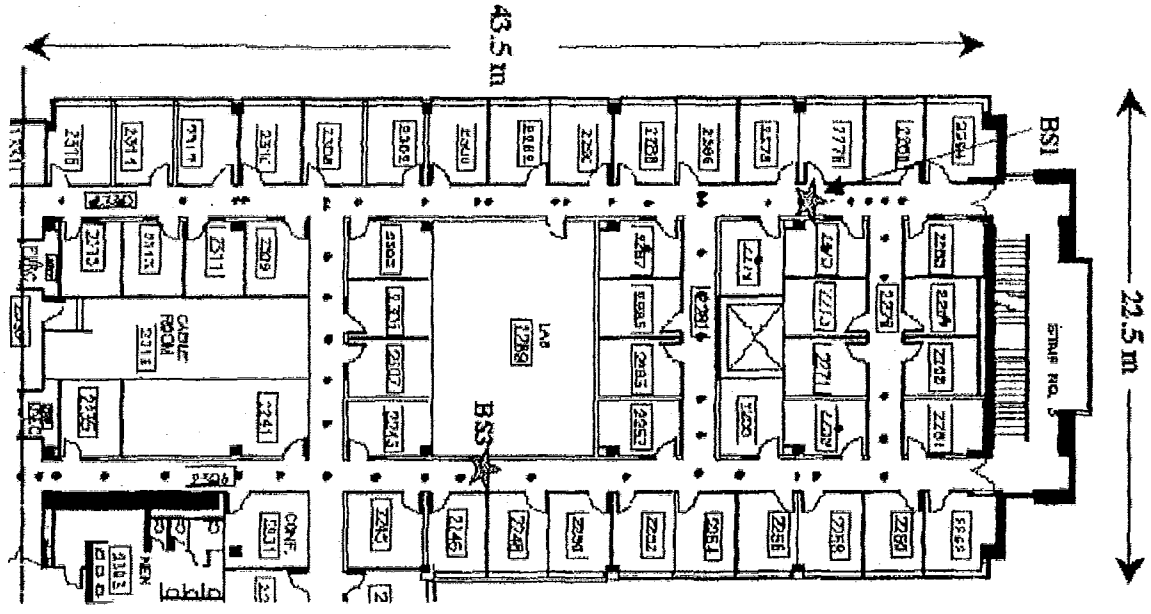

Figura 6.5: *Grid* utilizado na construção do modelo de localização proposto no RADAR. Pontos apenas nos corredores. Fonte:[1]

Capítulo 7

Conclusões e Sugestões Para Trabalhos Futuros

ESTE capítulo conclui o trabalho realizado, consolidando os resultados expostos anteriormente e extraindo as conclusões relevantes. Além disso, as principais contribuições alcançadas durante a pesquisa são apresentadas. Por fim, também são feitas algumas recomendações para pesquisas futuras.

7.1 Conclusões

O objetivo principal deste trabalho foi propor um novo método de localização de dispositivos sem fio para WLANs baseado em RF, livre de fase de calibragem e auto-suficiente. Esse método não depende de nenhum *hardware* especializado (dedicado somente a fins de localizar dispositivos sem fio) e é semelhante, em termos de acurácia, à outras técnicas de localização disponíveis no mercado e na literatura. Tais objetivos foram alcançados através da utilização de um modelo de propagação que descreve o decaimento do nível de sinal de RF recebido, de acordo com o aumento da distância entre transmissor e receptor. Este modelo de propagação foi utilizado na construção do modelo de localização (descrito no Capítulo 5) e seus parâmetros foram determinados dinâmicamente e em tempo real, através de medições de RSSI realizadas entre os pares "*sniffer* + AP de referência". Um método probabilístico foi utilizado para comparar os níveis de sinal medidos pelo sniffer, a partir do cliente sem fio, com o modelo de localização construído.

Uma nova arquitetura baseada em *sniffers* foi proposta de forma a permitir que aplicações de segurança e/ou gerenciamento possam também se beneficiar de informações de localização, diferente de outras soluções encontradas no mercado e na literatura, onde uma arquitetura baseada no paradigma cliente-servidor, impede a implantação destes tipos de serviço. Com a arquitetura proposta, a responsabilidade por capturar informações de RSSI para auxiliar na estimativa de posicionamento, não está mais sobre os clientes sem fio e sim sobre os *sniffers*.

A eficiência do método proposto foi avaliada objetivamente através de horas de medições experimentais e coletas de dados. Mostrou-se através de métricas bem definidas que o desempenho do sistema implementado atende aos requisitos de uma grande variedade de aplicações, não apenas por apresentar boa acurácia, mas também pela simplicidade na implantação e facilidade na manutenção do modelo de localização. Estes resultados contrastam com diversos outros trabalhos encontrados na literatura, onde um grande esforço de implantação muitas vezes representa uma barreira à sua adoção.

Uma vez alcançados os objetivos determinados no início desta pesquisa, futuramente será possível dar continuidade a mesma, investigando-se uma série de problemas relacionados à localização e que não foram atacados dentro do escopo do presente trabalho. Na seção seguinte, alguns destes pontos serão destacados, junto com aplicações do sistema desenvolvido junto a pesquisas atuais na área de redes móveis.

7.2 Sugestões Para Trabalhos Futuros

O sistema foi implementado em um ambiente real de produção, de forma que nenhum aspecto da rotina dos usuários tivesse sido afetado de qualquer maneira. A partir deste trabalho, torna-se interessante investigar o impacto do posicionamento de *sniffers* e pontos de acesso de referência na acurácia, bem como, a influência da quantidade destes dispositivos no desempenho do sistema.

Nos experimentos realizados neste trabalho, foi utilizado um modelo de propagação de sinal de RF para estimar a média de $P(s|l)$. No entanto, não foi levado em consideração neste estudo o valor do parâmetro α. Aqui, considerou-se $\alpha = 0$. É possível utilizar diferentes valores deste parâmetro para sintonizar o modelo de propagação e aproximá-lo ainda mais da realidade do canal sem fio, melhorando a acurácia do método. O estudo do impacto da mudança nos valores deste e de outros parâmetros do sistema, como o decaimento em espaço livre n_0 e a resolução do grid utilizada para montar o mapa de propagação, é alvo de trabalhos futuros.

A implementação de um mecanismo que utiliza fase de calibragem, como o RADAR por exemplo, no mesmo ambiente onde foi testado o método proposto seria interessante para que resultados de acurácia pudessem ser comparados efetivamente de forma quantitativa. O mapa de propagação gerado na fase de calibragem poderia também ser comparado com o mapa gerado dinamicamente através do uso de modelos de propagação em RF, e ainda utilizado para ajustar os parâmetros α e n_0, otimizando-os para um ambiente específico e contribuindo também para melhoria na acurácia.

Pesquisas na área de modelos de mobilidade podem se beneficiar de registros de movimentação (*traces*) fornecidos pelo sistema de localização desenvolvido aqui para validar modelos propostos [42] e/ou criar novos modelos. A área de pesquisa em protocolos de roteamento em sistemas móveis e redes auto-organizáveis pode também se beneficiar de informações de localização para atribuir endereços dinâmicos às estações móveis, sendo que esses endereços são dependentes de sua localização [43].

Bibliografia

[1] P. Bahl and V. N. Padmanabhan, "RADAR: An In-building RF-based User Location and Tracking System," *IEEE INFOCOM*, vol. 2, pp. 775-784, Março 2000.

[2] IEEE 802.11, *IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1999.

[3] *Wireless Ethernet Compatibility Alliance - WECA*. [Online]. Available: http://www.weca.net/OpenSection/index.asp

[4] J. Walker, "Unsafe at any key size: an analysis of the WEP encapsulation," IEEE 802.11 committee, Tech. Rep., Março 2000.

[5] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," *Eighth Annual Workshop on Selected Areas in Cryptography*, Agosto 2001.

[6] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html*, Janeiro 2001.

[7] W. A. Arbaugh, N. Shankar, and Y. C. J. Wan, "Your 802.11 Wireless Network has No Clothes," University of Maryland, Tech. Rep. 03628E, Março 2001.

[8] P. Krishnan, A. Krishnakumar, W.-H. Ju, C. Mallows, and S. Ganu, "A system for LEASE: location estimation assisted by stationary emitters for indoor RF wireless networks," *IEEE Infocom*, Março 2004.

[9] M. Hassan-Ali and K. Pahlavan, "A New Statistical Model for Site-Specific Indoor Radio Propagation Prediction Based on Geometric Optics and Geometric Probability," *IEEE Transactions on Wireless Communication*, vol. 1, no. 1, pp. 112–124, Janeiro 2002.

[10] D. B. Green and M. S. Obaidat, "An Accurate Line of Site Propagation Performance Model for Ad-Hoc 802.11 Wireless LAN (WLAN) Devices," *IEEE ICC 02*, Janeiro 2002.

[11] A. Hills, J. Schlegel, and B. Jenkins, "Estimating Signal Strengths in the Design of an Indoor Wireless Nestwork," *IEEE Transactions on Wireless Communications*, vol. 3, no. 1, pp. 17–19, Janeiro 2004.

[12] T. S. Rappaport, *Wireless Communications – Principles and Practice.* Prentice Hall, 2002.

[13] S.Y. Seidel and T.S. Rappaport, "914 MHz Path-Loss Prediction Models for Indoor Wireless Communications," *IEEE Trans. Antennas and Propagation*, Maio 1991.

[14] M. Youssef and A. K. Agrawala, "Handling samples correlation in the horus system," *IEEE Infocom*, Março 2004.

[15] A. Leon-Garcia, *Probability and random processes for electrical engineering.* Addison-Wesley, Reading, MA, 1994.

[16] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The Active Badge Location System," *ACM Transactions on Information Systems*, vol. 40, no. 1, pp. 91–102, Janeiro 1992.

[17] P. Prasithsangaree, P. Krishnamurthy, and P. K. Chrysanthis, "On indoor position location with wireless lans," *The 13th IEEE PIMRC*, Setembro 2002.

[18] Y. Gwon, R. Jain, and T. Kawahara, "Robust indoor location estimation of stationary and mobile users." in *INFOCOM*, Abril 2004.

[19] P. Bahl, A. Balachandran, and V. N. Padmanabhan, "Enhancements to the RADAR user location and tracking system," *Microsoft Technical Report*, 2000.

[20] V. Sacramento, M. Endler, H. Rubinsztejn, L. Lima, K. Gonçalves, F. Nascimento, and G. Bueno, "MoCA: A middleware for developing collaborative applications for mobile users," *ACM/IFIP/USENIX International Middleware Conference*, Outubro 2004.

[21] R. Battiti, T. L. Nhat, and A. Villani, "Location-aware computing: A neural network model for determinating location in wireless LANs," University of Trento, Tech. Rep. DIT-02-0083, Fevereiro 2002.

[22] M. Youssef and A. Agrawala, "WLAN location determination via clustering and probability distributions," *IEEE PerCom*, Fevereiro 2003.

[23] T. Roos, P. Myllymäki, H. Tirri, P. Misikangas, and J. Sievänen, "A probabilistic approach to wlan user location estimation," *International Journal of Wireless Information Networks*, vol. 9, no. 3, pp. 155–164, Julho 2002.

[24] C. Komar and C. Ersoy, "Location tracking and location based service using ieee 802.11 WLAN infrastructure," *European Wireless*, Fevereiro 2004.

[25] M. Youssef and A. K. Agrawala, "The horus wlan location determination system," *Proceedings of the Third International Conference on Mobile Systems, Applications, and Services - MobiSys*, Junho 2005.

[26] A. Taheri, A. Singh, and E. Agu, "Location fingerprinting on infrastructure 802.11 wireless local area networks (WLANs) using locus," *Fourth International IEEE Workshop on Wireless Local Networks*, Novembro 2004.

[27] S. Saha, K. Chaudhuri, D. Sanghi, and P. Bhagwat, "Location determination of a mobile device using IEEE 802.11b access point signals," *IEEE Wireless Communications and Networking Conference (WCNC)*, Março 2003.

[28] *Ekahau Positioning Engine.* [Online]. Available: http://www.ekahau.com/

[29] S. Ganu, A. S. Krishnakumar, and P. Krishnan, "Infrastructure-based location estimation in wlan networks," *IEEE Wireless Communications and Networking Conference (WCNC)*, Março 2004.

[30] T. W. Christ and P. A. Godwin, "A prison guard duress alarm location system," *IEEE International Carnahan Conference on Security Technology*, Outubro 1993.

[31] "Airdefense," 2005, http://www.airdefense.net.

[32] F. Adelstein, P. Alla, R. Joyce, and G. G. Richard III, "Physically locating wireless intruders," *Journal of Universal Computer Science (JUCS)*, pp. 4–19, Janeiro 2005.

[33] B. A. A. Nunes, C. A. V. Campos, L. F. M. de Moraes, and P. D. M. Jr., "Avaliando a Sobrecarga Introduzida nas Redes 802.11 pelos Mecanismos de Segurança WEP e VPN/IPSec," *WSeg2003 - XXI Simpósio Brasileiro de Redes de Computadores (SBRC'03)*, Maio 2003.

[34] W. Stallings, *Wireless Communications and Networks.* Prentice Hall, 2002.

[35] *Soekris Engineering.* [Online]. Available: http://www.soekris.com/

[36] Demetrio S. D. Carrión, "Implementação de um ponto de acesso seguro para redes 802.11b baseado no sistema operacional OpenBSD," *Projeto Final de Curso, Departamento de Engenharia Eletrônica e Computação - DEL/UFRJ*, 2003.

[37] *Wireless Tools for Linux.* [Online]. Available: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

[38] *Host AP driver for Intersil Prism2/2.5/3, hostapd, and WPA Supplicant.* [Online]. Available: http://hostap.epitest.fi/

[39] MYSQL, "Banco de dados mysql," http://www.mysql.com, Janeiro 2006.

[40] *Orinoco driver for wireless cards*, 2006, http://ozlabs.org/people/dgibson/dldwd/.

[41] *HOSTAP - driver for wireless cards*, 2006, http://hostap.epitest.fi/.

[42] C. A. V. Campos, D. C. Otero, and L. F. M. de Moraes, "Realistic Individual Mobility Markovian Models for Mobile ad hoc Networks," *IEEE Wireless Communications and Networking Conference - WCNC 2004*, Março 2004.

[43] A. C. Viana, M. D. de Amorim, Y. Viniotis, S. Fdida, and J. F. Rezende, "Easily-managed and topological-independent location service for self-organizing networks," *ACM MobiHoc*, Maio 2005.