UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM TECNOLOGIAS, GERÊNCIA E SEGURANÇA
DE REDES DE COMPUTADORES

LEONARDO PERES FAGUNDES

Técnicas de Localização de Dispositivos Móveis em Redes WiFi - TDOA

Trabalho de Conclusão apresentado como requisito parcial para a obtenção do grau de Especialista

Prof. Dr. João Netto
Orientador

Prof. Dr. Sérgio Luis Cechin
Prof. Dr. Luciano Paschoal Gaspary
Coordenadores do Curso

Porto Alegre, dezembro de 2008.

Agradecimentos

Bolivar, meu pai, e Eva, minha mãe, pelo exemplo de vida e o caminho mostrado a seguir, onde me proporcionaram a oportunidade de estudar, onde aprendi que só a busca pelo conhecimento é capaz de tornar realmente um ser humano livre. A minha filha Débora, que está comigo em todas as horas mesmo sem ela saber. A minha companheira Rose, pelo carinho e compreensão nas minhas horas de estudo. Aos meus irmãos que de certa forma também ajudaram-me a chegar até aqui, em especial a minha irmã Izar pela correções e sugestões. A todos meus amigos de perto e os de longe. Por fim, a Deus, nosso amigo maior, pela oportunidade de eu estar neste Planeta ainda, aprendendo e crescendo.

"Se você é capaz de tremer de indignação a cada vez que se comete uma injustiça no mundo, então somos companheiros." Ernesto Che Guevara

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

AOA *Angle Of Arrival*
AP *Access Point*
CDMA *Code Division Multiple Access*
Cell-ID *Cell Identification*
DSSS *Direct Sequence Spread Spectrum*
FHSS *Frequency Hopping Spread Spectrum*
GPS Global Positioning System
IDS *Intrusion Detection System*
IEEE *Institute of Electrical and Electronics Engineers*
IR *Infra Red*
LAN *Local Area Network*
LBS *Location Based Services*
LOS *Line of Sight*
LSM *Least Square Method*
M-AP *Master – Access Point*
OFDM *Orthogonal Frequency Division Multiplexing*
RF *Radio Frequency*
RFID *Radio Frequency Identification*
RSSI *Received Signal Strength Indication*
S-AP *Slave – Acess Point*
SSP *Spread Spectrum Transmission*
STA *Station*
TDOA *Time Difference of Arrival*
TOA Time of Arrival
UWB Ultra Wide Band
VAT Vulnerability Assessment Team
VPN Virtual Private Network
WCDMA Wide-Band Code Division Multiple Access
WEP Wired Equivalent Privacy
Wi-FI Wireless Fidelity
WPA Wi-Fi Protected Access

LISTA DE FIGURAS

LISTA DE TABELAS

Localização de Dispositivos Móveis em Redes Wi-Fi - TDOA

Resumo

Fagundes, Leonardo Peres. **LOCALIZAÇÃO DE DISPOSITIVOS MÓVEIS EM REDES Wi-Fi - TDOA.** Porto Alegre, Dezembro, 2008. 26p.

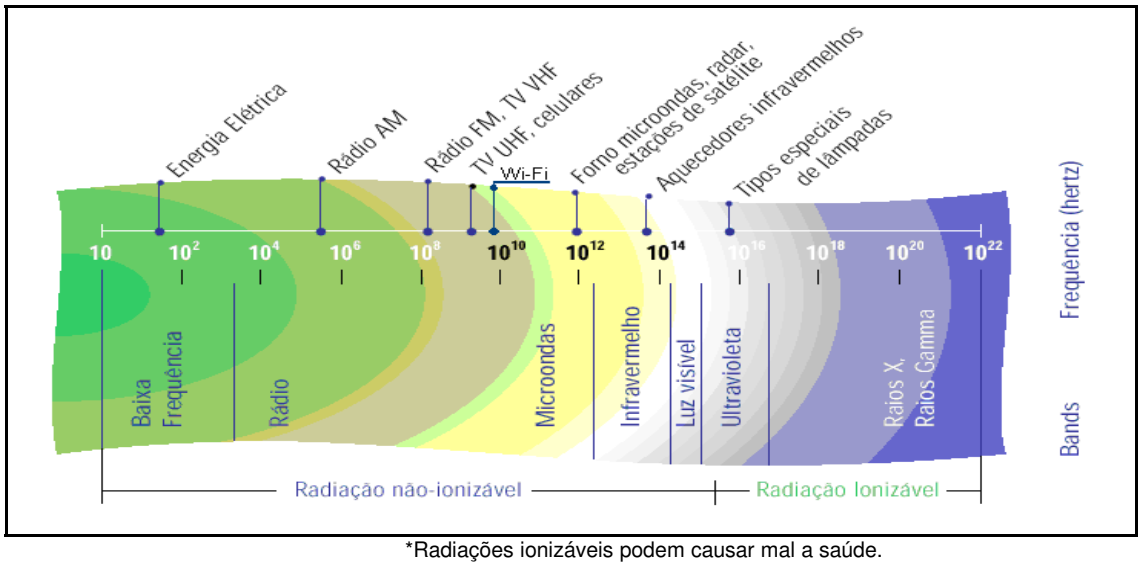
Trabalho de conclusão – Instituto de Informática, Universidade Federal do Rio Grande do Sul.

Com a popularização do uso das redes sem fio Wi-Fi, sistemas de localização de dispositivos móveis em ambientes fechados(*Indoor*) ou de menor cobertura estão ganhando importância no mundo atual, pois agregam valor às redes sem fio. Devido a sua arquitetura e ao crescente aumento de dispositivos portáteis sem fio inseridos em ambientes cobertos por estas redes, aliado ao aumento da demanda por informação a todo tempo e lugar, a localização é um importante diferencial que este tipo de sistema oferece aos usuários e administradores de rede. Técnicas mais utilizadas de localização por estes sistemas serão abordadas sucintamente neste trabalho, técnicas estas que na sua maioria, se baseiam em mensurar a potência do sinal de RF para estimar a posição de um dispositivo. Neste contexto, a possibilidade de um dispositivo sem fio hostil à rede Wi-Fi obter acesso indevido a mesma, o que consiste uma das grandes preocupações para os administradores de rede. Por isso, a técnica que utiliza o TDOA(*Time Difference of Arrival*), que está, ainda, sendo pouco estudada e implementada em sistemas de localização em ambientes *Indoor*, será objeto de estudo mais aprofundado devido à sua característica específica. Ela realiza um monitoramento do tempo que o sinal de RF leva entre o transmissor e o receptor e, por este motivo, vem contemplar um requisito importantíssimo relacionado à segurança do sistema, onde casos de acessos indesejados que provenham de distâncias maiores ou externas ao perímetro conhecido de uma rede sem fio. TDOA apresenta vantagem em relação as demais técnicas neste aspecto, pois este tipo de ataque pode ser mais facilmente detectado por ela.

1 INTRODUÇÃO

1.1 Histórico da Radiofrequência

O físico alemão Heinrich Hertz(1894), estudando a teoria do eletromagnetismo do também físico e matemático, o escocês James Clerk Maxwell(1879), descobre em 1887, analisando ondas eletromagnéticas, que estas possuíam características semelhantes às da luz: a mesma natureza vibracional e suscetibilidade de reflexão, refração e as ondas quentes.



*Radiações ionizáveis podem causar mal a saúde.

Figura 1.1: Radiofreqüência

Hertz através deste estudo, estava ajudando a formar a base para o desenvolvimento do rádio, televisão e do radar, ou seja, das comunicações através da radiofreqüência. Uma das primeiras aplicações do uso da RF, dá-se portanto no início do século XX. Em 1912, surgiu o primeiro dispositivo de radionavegação. De lá até os dias atuais, a utilização de sinais de RF em dispositivos e/ou sistemas de comunicação, localização e detecção tornou-se algo comum em diversas áreas do nosso cotidiano.

1.2 Tecnologia sem fio Wi-Fi

Redes de computadores, originalmente estruturadas através de cabeamento, passaram a usufruir desta tecnologia de comunicação sem fio por

sinais de RF e através de IR, infravermelho. Um destes tipos de redes mais importante, devido a sua velocidade de transmissão e popularização, é a denominada Wi-Fi (*Wireless Fidelity*), baseada nas implementações dos protocolos de comunicação 802.11x. O padrão 802.11x utiliza formas da técnica SSP (*Spread Spectrum Transmission)* que foi a base do seu desenvolvimento para comunicação sem fio por RF. Esta técnica foi patenteada nos EUA em 1942 por Hedwig Eva Maria Kiesler(1913) e George Antheil(1900) sob o título "*Secret Communications System*". A norma 802.11x baseia-se nas formas FHSS (*Frequency Hopping Spread Spectrum*), DSSS (*Direct Sequence Spread Spectrum*) e OFDM (*Orthogonal Frequency Division Multiplexing*). Atualmente, a pouca utilização do IR em relação a radiofrêqüencia deve-se principalmente à sua baixa largura de banda de 1 Mbps a 2 Mbps que alcança na transmissão de dados, taxa bem inferior à taxa mínima de RF que é 11 Mbps no padrão 802.11x.

1.3 Motivação

Quanto a segurança, sistemas que utilizam comunicação Wi-Fi precisam estar protegidos de acessos indesejados, pois podem facilmente sofrer ataques devido a sua arquitetura diversa das redes cabeadas. A proteção de uma rede cabeada através de *firewalls* nos roteadores de borda já limita o acesso indevido a este tipo de rede. Em redes sem fio, a segurança deve ser intensificada devido à possibilidade do fácil acesso, já que a característica do sinal de RF é trafegar em várias direções pelo ar. Implementações conhecidas visando à melhoria desta segurança, utilizam a criptografia para proteção, como WEP, WPA, WPA2 e uso de VPNs, possibilitando uma proteção mais efetiva. Sistemas de detecção de intrusão Wireless(*IDS-Wireless*), análogos aos IDS em redes cabeadas, também podem ajudar a detectar comportamentos anômalos da rede sem fio, podendo gerar alertas ao administrador da rede. Redes sem fio podem ainda sofrer ataques que partem de dispositivos a maiores distâncias, conectados a antenas direcionais de alto ganho. Mesmo sistemas GPS, por exemplo, não estão imunes a ataques semelhantes. Recentemente, testes realizados pelo grupo americano VAT(Vulnerability Assessment Team), observaram que um sistema GPS em um caminhão foi facilmente enganado por sinais de RF inseridos, propositadamente, no ambiente próximo ao veículo, confundindo o sistema e alterando a informação da sua verdadeira localização. Neste caso, o sistema de monitoramento receberia uma informação equivocada da localização do caminhão, facilitando a ação de ladrões. Em redes Wi-Fi, não é raro que este tipo de ataque provenha até mesmo de dispositivos como antenas caseiras, latas de batata frita, latas de óleo de cozinha, etc. A possibilidade de um dispositivo obter acesso à rede sem fio, através de uma antena com o sinal amplificado é também um grande problema de segurança.

Este trabalho visa estudar a técnica que utiliza o TDOA(*Time Difference of Arrival*), onde o tempo que o sinal de RF leva do dispositivo transmissor até o

receptor é considerado para estimar o posicionamento. Analisar as vantagens e desvantagens desta técnica, principalmente no que se refere a segurança do sistema, em relação às demais técnicas que utilizam, na sua maioria, a potência do sinal de RF para estimar a posição de dispositivos que compõem uma rede sem fio.

2 LOCALIZAÇÃO EM REDES SEM FIO

2.1 Aplicabilidade dos LBS

Atualmente discorrer sobre sistema de localização, remete-nos ao GPS (*Global Positioning System*) criado na década de 1970 pelo Departamento de Defesa Norte-Americano. O seu uso é largamente difundido através de pequenos dispositivos de localização, que já fazem parte do nosso cotidiano. Baseia-se o GPS em uma rede de informações via sinais de satélites, que permite que dispositivos aqui na Terra consigam estimar a sua localização por coordenadas de latitude e longitude, através de uma triangulação entre um receptor e as posições conhecidas de três ou mais satélites. Este sistema, porém, funciona satisfatoriamente bem apenas em ambientes externos, não possuindo uma boa acurácia em ambientes fechados(*Indoor*). Estudos demonstraram que sistemas de localização que utilizam redes Wi-Fi, conseguem excelentes resultados neste tipo de ambientes.

Sistemas de localização de dispositivos móveis estão cada vez mais sendo valorizados no mundo moderno, devido à ampliação e à popularização desse tipo de redes, e a grande gama de dispositivos portáteis. A possibilidade, em tempo real, da localização de um dispositivo dependendo do contexto em que está inserido, pode ser de vital importância para uma empresa ou organização. Já existem sistemas de localização sendo implantados em hospitais, onde a importância de localizar em tempo real médicos, por exemplo, é um grande diferencial na qualidade do atendimento aos pacientes. Em outras áreas, como grandes portos marítimos e fluviais, a localização de um *container* com carga sensível, pode significar uma importante informação que agregaria enorme qualidade ao serviço prestado pela administração portuária a seus clientes. Um sistema de localização baseado em Wireless pode auxiliar a identificação de obras em Museus, protegendo-as e informando aos visitantes dados sobre a localização das obras. Podemos ainda aplicá-lo em casas denominadas “inteligentes” onde poderia auxiliar nas tarefas comuns do morador, identificando rotinas e antecipando-as conforme o perfil do morador. Uma grande rede brasileira de lojas de departamentos e variedades, neste fim de ano, irá usar etiquetas RFID(*Radio-Frequency Identification*) em todos os seus produtos, agilizando o controle de estoque e evitando extravios. Outra grande rede de supermercados no Brasil está implantando, através de rede Wi-Fi, o “carrinho inteligente” que consulta num banco de dados a localização dos

produtos e os aponta num mapa da loja disponível no display do carrinho. Numa segunda etapa, a loja implementará o sistema de triangulação de antenas, o que permitirá ao carrinho, além de apontar a localização do produto, exibir onde o usuário está e traçar a rota para chegar até o item procurado. Enfim, nas mais diversas áreas estes sistemas podem hoje e num futuro próximo contribuírem na melhoria do dia-a-dia de pessoas e organizações .

2.2 Quanto as Técnicas mais Usadas

As técnicas de localização mais empregadas atualmente nos sistemas baseados em redes Wi-Fi, podem ser divididas em grupos.

As que se utilizam do ângulo de chegada do sinal de RF, conhecida como AoA(*Angle of Arrival*) utilizadas em sistemas que usam triangulação com antenas direcionais. Para estimar a posição, elas utilizam-se de três pontos de referência no raio de acesso ao dispositivo, calculando o ângulo e o tamanho das arestas do triângulo formado. Técnica semelhante, é outra técnica de triangulação, onde são necessários dois pontos distintos de medição em relação a um ponto fixo para estimar a posição do dispositivo.

As que se baseiam na potência do sinal de RF, RSSI(*Received Signal Strength Indicator*) mapeando o ambiente para posterior comparação em tempo real, com um banco de dados pré-armazenado. Na sua imensa maioria, estes sistemas usufruem da infra-estrutura préexistente das redes Wi-Fi, baixando muito os custos de sua implantação. Essas técnicas, porém, baseadas em mapas de RSSI podem dar uma estimativa equivocada no posicionamento de um dispositivo com o sinal de RF amplificado fora do perímetro conhecido. Desta forma, um dispositivo será enxergado pelo sistema como um componente da rede. Ele poderá, ainda, tentar obter acesso a esta rede, fazendo com que o sistema de localização baseado em mapas de RSSI se confunda e o considere numa posição mais próxima da que ele realmente está fisicamente.

Por fim, as técnicas que utilizam o TDOA(*Time Difference of Arrival*) onde a diferença do tempo de propagação do sinal RF é medida para estimar a posição do dispositivo.

3 TÉCNICAS DE LOCALIZAÇÃO

3.1 Técnicas Direcionais de Triangulação e Direcionais

A primeira delas é a que usa o AoA(*Angle of Arrival*) (HIGHTOWER;BORRIELLO, 2001;RUSSEL,2003), onde são necessárias duas medições em pontos distintos entre o transmissor e receptor. Em cada medição, é calculado o ângulo em que o sinal de RF é mais forte. Após a definição dos dois ângulos e sabendo o tamanho da aresta adjacente a ambos, define-se o triângulo. A interseção das linhas, portanto, determina a localização do dispositivo transmissor. O erro médio é proporcional ao produto do erro angular e a distância entre o AP e a estação. A medição do ângulo é realizada por diversas antenas, o que envolve um complexo sistema. (Figura 3.1)

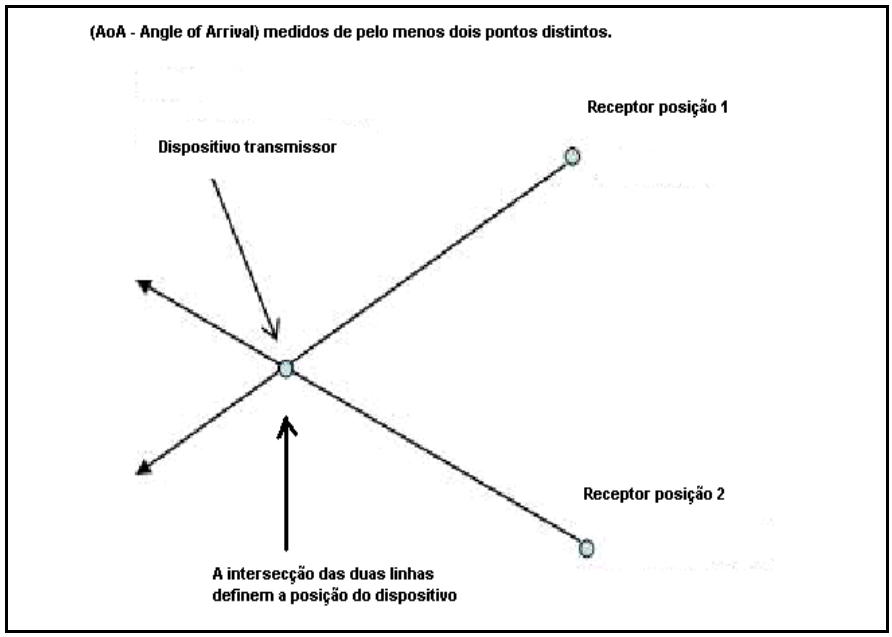


Figura 3.1:

As técnicas que utilizam triangulação funcionam muito bem em ambientes abertos, porém em ambientes internos(*indoor*) o sinal sofre com um problema de multipercurso, o que acaba comprometendo o resultado. Consequentemente, elas quase não são utilizadas em ambientes fechados.

3.2 Técnicas de mapeamento de RSSI

Em ambientes *indoor,* a técnica que mais tem se destacado nos sistemas de localização é a que faz uso do mapeamento de RSSI(*Received Signal Strength Indicator*) (BAHL;PADMANBHAM,2000;BERNA et al., 2003), onde são realizadas medições da potência do sinal de radiofreqüência em vários pontos do ambiente e o resultado é armazenado num banco de dados. Esses dados, posteriormente, são comparados com a medição em tempo real de um dispositivo a ser localizado no mesmo ambiente mapeado, onde o resultado mais aproximado dessa comparação determina a localização do dispositivo. Mapeamentos mais extensos podem causar erros dependendo da distância. A acurácia é comprometida em condições onde o sinal de RF sofre com o fenômeno de multipercurso, pois a variação do sinal pode chegar a 10dB.

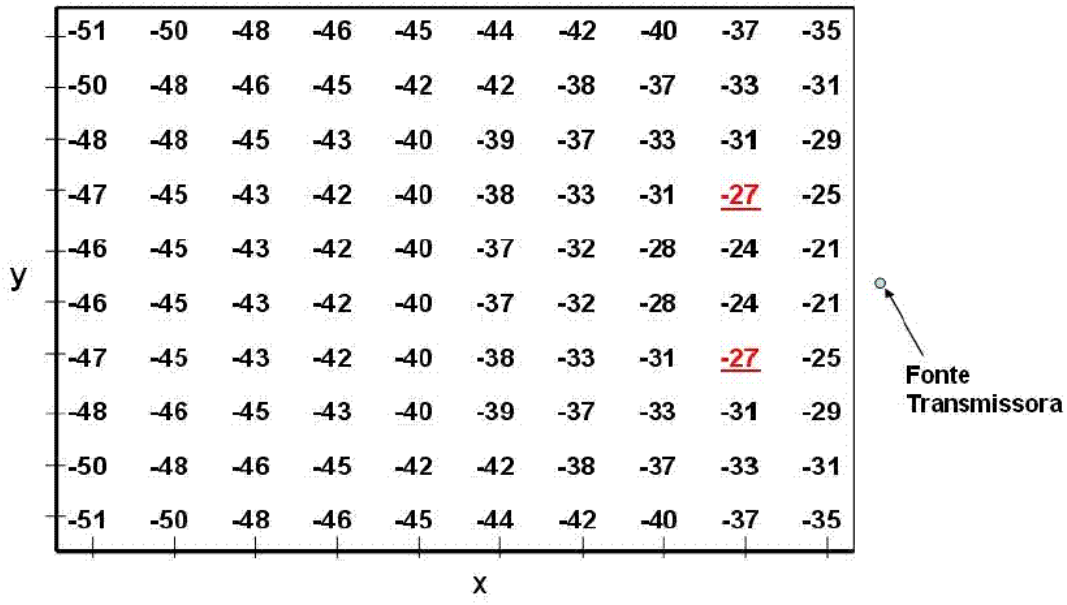


Figura 3.1: Exemplo de um mapa de RSSI

4 TDOA(*TIME DIFFERENCE OF ARRIVAL*)

4.1 Técnica de diferença de tempo de chegada do sinal de RF

A técnica analisada foi aplicada em um trabalho desenvolvido em 2005 de localização que utilizada o TDOA(*Time Difference of Arrival)* (YAMASAKI et al.,2005)e foi testada numa rede Wi-Fi IEEE 802.11b. Segundo os autores, na arquitetura da rede é necessário um bom posicionamento geográfico dos AP(*Access Point*) para melhorar os resultados desta técnica. E ainda que a acurácia de um LBS em ambientes Indoor sofre degradação devido a perda ou oscilação do sinal de RF pois desvios ou multipercursos que o sinal de RF pode sofrer sendo isso uma das características marcantes da sua propagação *Indoor*. O trabalho que foi desenvolvido neste sistema de localização com o técnica TDOA em IEEE 802.11b, incluiu vários procedimentos, como a sincronização dos APs(Access Point), através da observação de temporarização e medições de mais de uma fonte de recepção do sinal de RF. O Sistema foi testado num armazém, onde precisão do sistema atingiu, quando utilizado dez APs, foi de 2,4 mts a 67 percentil. O objetivo do trabalho desenvolvido com a técnica TDOA foi obter, com uma boa acurácia, um sistema de localização para ambiente internos e externos, pois o melhor resultado é o objetivo maior dos sistemas de localização atuais.

LBS são mais sujeitos a interferências em ambientes fechados do que em ambientes externos, por causa da perda de sinal de RF nesse tipo de ambiente.

Na tabela I vemos a comparação de técnicas de localização quanto a alguns aspectos importantes:

Tabela 4.1: Comparação entre Técnicas de localização

Técnica	**Perda da Confiabilidade**		**Complexidade do Access Point**
	Multipercurso	**Distância (AP-STA)**	
TOA(TDOA)	Pouca	Nenhuma	Média
AOA	Pouca	Pouca	Alta
RSSI	Severa	Pouca	Baixa
Cell-ID	Nenhuma	Severa	Baixa

Fonte: YAMASAKI et al.,2005

A técnica TDOA mede o atraso do tempo de chegada do sinal de RF, onde o erro médio é inversamente proporcional à largura de banda independente da distância entre o AP e a estação. TOA é outra técnica que utiliza a média do atraso de propagação do sinal. Para isso, é necessário sincronização precisa entre o APs e as estações.

Cell-ID é uma técnica simples para determinar a posição de uma estação. O AP com maior sinal é assumido com sendo a posição da estação. Sistemas que utilizam a técnica TDOA com banda suficiente são os mais confiáveis em ambientes *Indoor*.

A figura 1 mostra a relação entre os tamanhos de banda e os sistemas wireless padronizados por ano.

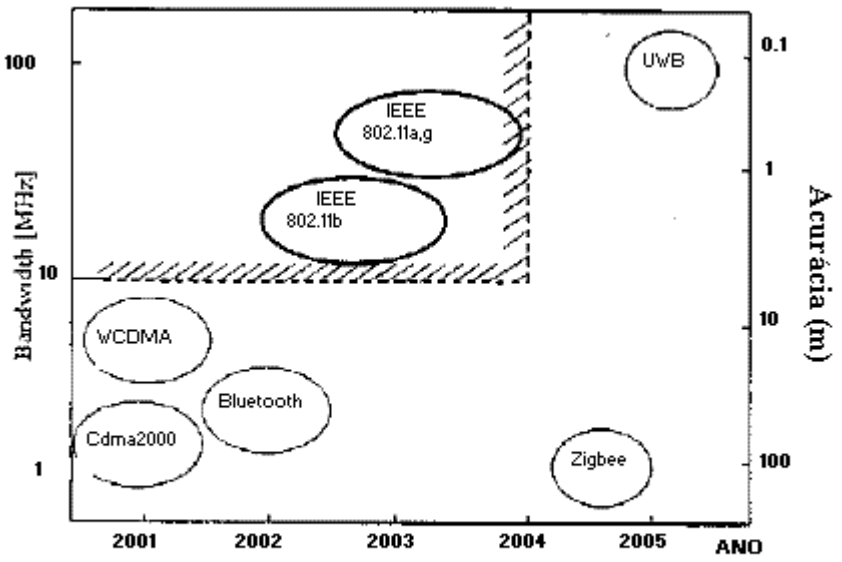


Figura 4.1: Comparação dos sistemas wireless (YAMASAKI et al.,2005)

A acurácia desejada para sistemas *Indoor* de localização deve ser menor que 10 mts. Para isso, o tamanho da banda deve ser maior que 10MHz. Por este motivo, redes baseadas em IEEE 802.11b ou superior que tem taxas superiores a 10MHz são as mais apropriadas para ambientes fechados.

O sistema testado é composto por receptores especiais, Tags e um servidor de localização. Os receptores especiais recebem um sinal da posição enviado por uma Tag e eles enviam ao servidor o tempo do recebimento. O servidor calcula a posição da Tag baseado nesses tempos de recebimento. O inconveniente é que este sistema precisa de Tags especiais.

4.2 Implementação do Sistema

Primeiramente, para estimarmos as coordenadas da estação, foram necessários mais que três APs para medirmos o tempo do recebimento dos

pacotes recebidos, enviados pela estação-alvo. Alguns pontos precisaram ser avaliados. O primeiro foi o método de medição do tempo do pacote recebido onde a solução convencional é similar ao método CDMA. O outro problema foi realizar o procedimento adequado em caso de ocorrer que mais que um AP receber pacotes idênticos enviados pela estação-alvo. A figura 2 mostra o problema de seleção de pacotes.

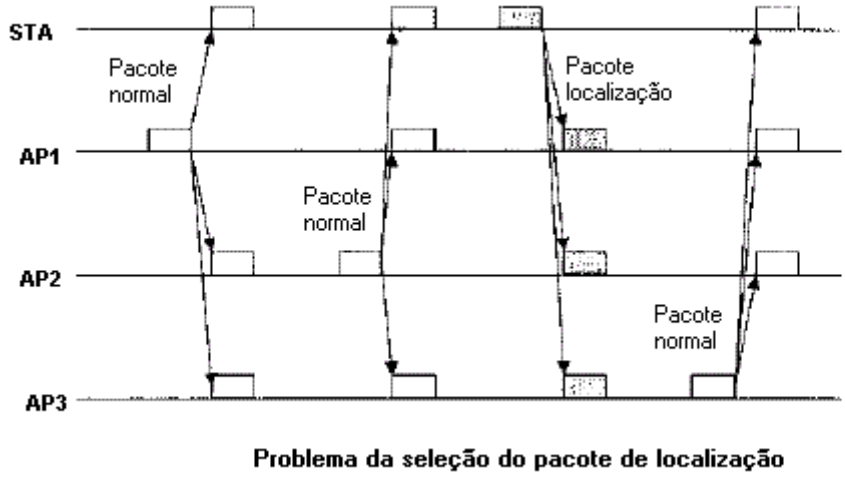


Figura 4.2: Problema da seleção do pacote de localização (YAMASAKI et al.,2005)

Na transmissão dos pacotes, o tempo em que cada estação envia um pacote é desconhecido pelos APs. Consequentemente, os APs precisam distinguir a localização dos pacotes de dados entre pacotes de controle e ainda gerenciar os pacotes de IEEE 802.11b. Outra questão muito importante é que os relógios do APs precisam estar perfeitamente sincronizados para poderem calcular a diferença do tempo dos pacotes recebidos. Como característica da IEEE 802.11b os APs não possuem mecanismos de sincronização, então é necessário um mecanismo de sincronização adicional para o sistema de localização wireless com a técnica TDOA.

4.3 Resultados Obtidos

O que diferencia os LBS é a precisão alcançada por cada um deles. Na tentativa de diminuir o efeito do multipercurso, otimizou-se o posicionamento dos APs. O multipercurso é um problema bem conhecido que afeta enormemente sistemas de localização *indoor*. A característica de propagação do sinal de RF em ambientes *indoor* é muito complexa, por isso todas as medições de tempo registradas provavelmente contêm erros. Na técnica TDOA, a medição do tempo exato do recebimento do sinal de RF é muito importante para a sobrevivência do sistema. A forma da disposição dos APs nesta técnica baseou-se nos cálculos de triangulação. Para um melhor resultado, este arranjo foi bem próximo de um triângulo regular.

4.4 Descrição do Sistema

Inicialmente, foi feita a seleção da localização de pacotes. A medição do tempo de recebimento de um pacote foi realizada por três módulos integrados no AP:Módulo Wireless, CPU e Módulo de localização. O diagrama do bloco funcional é mostrado na figura 3.

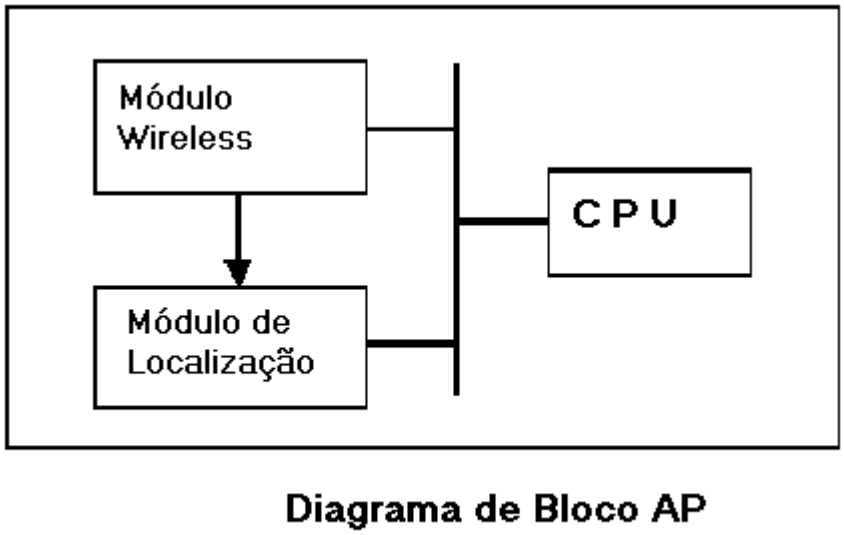


Figura 4.3: Diagrama de Bloco AP (YAMASAKI et al.,2005)

O módulo de localização possui um *buffer* de gravação de dados dos pacotes. Para medir o tempo de recebimento usa-se uma correlação com o sinal de RF, sendo que o AP precisa armazenar o sinal recebido no *buffer*. O módulo de localização então utiliza isso para calcular o tempo de recebimento. Conforme a IEEE 802.11b, por padrão, vários pacotes podem ser transmitidos randomicamente. O AP então, escolhe um pacote usando o método mostrado na figura 4.

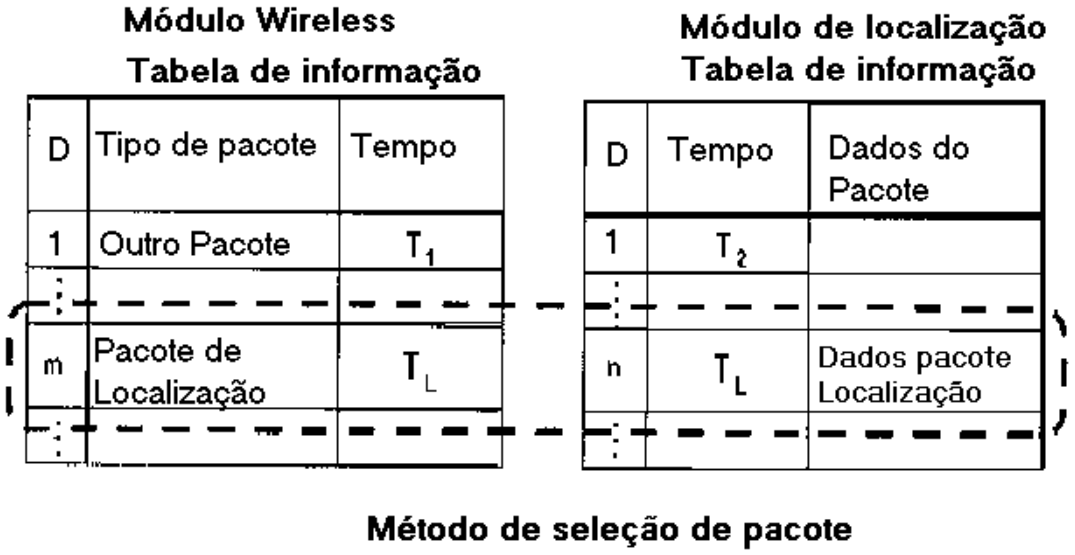


Figura 4.4: Método de seleção de pacote (YAMASAKI et al.,2005)

Quando o AP recebe o pacote, o módulo wireless grava o tipo do pacote e o tempo de recebimento numa tabela interna de informação. O módulo de localização grava dados do pacote recebido e o tempo de gravação na tabela de informações do módulo de localização. Caso o tipo de pacote seja o mesmo tipo do pacote de localização, o tempo de gravação é utilizado como uma chave de pesquisa na tabela. Se o tempo de gravação é igual ao valor mostrado na tabela, este pacote de dados é distinguido como pacote de dados de localização. Este pacote de dados de localização é então utilizado para calcular a correlação, estimando o tempo de recebimento.

4.5 Sincronização dos relógios dos APs

A rede wireless é um sistema assíncrono que não possui um relógio comum. Na técnica TDOA cada AP precisa medir e ajustar a diferença de tempo entre eles, para ser possível medir o "*receive timing*" com o seu próprio relógio, obtendo assim o TDOA exato. Para obter-se isso, a instalação em coordenadas conhecidas dos APs é muito importante. O método de sincronização é explanado na figura 5.

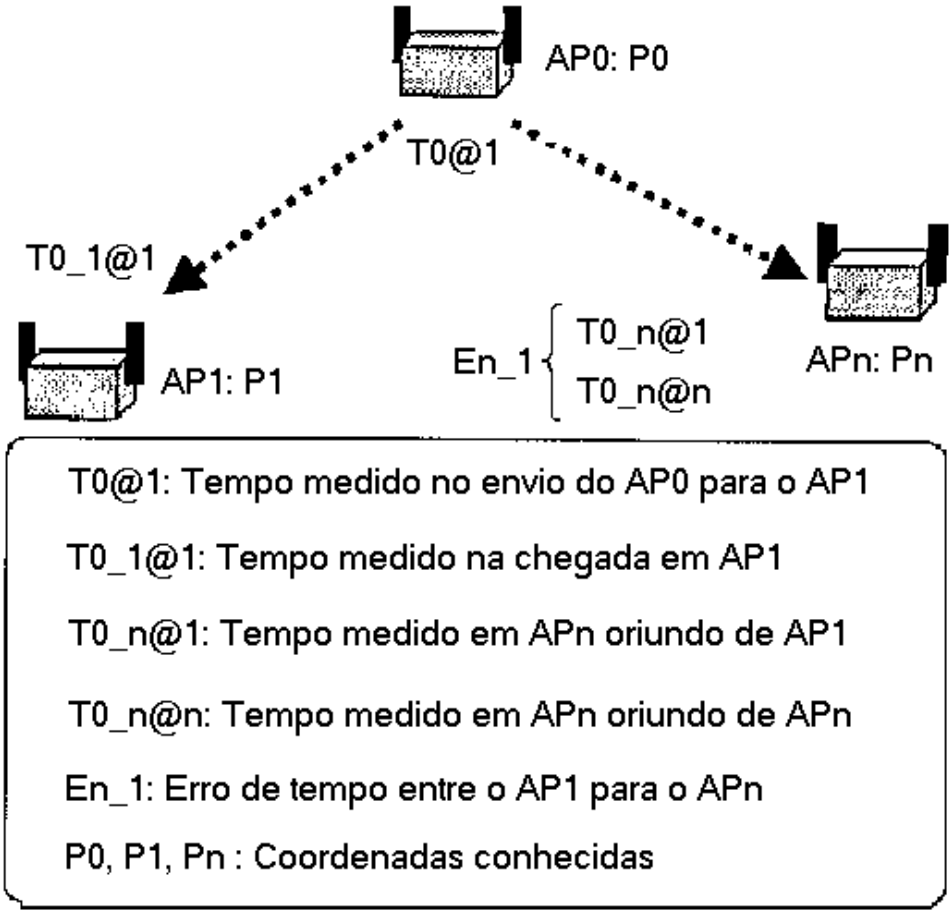


Figura 4.5: Método de sincronização de Aps (YAMASAKI et al.,2005)

T0_1@1 é observado em AP1. T0@1 é calculado usando a Eq.(1), porque P0 e P1 são conhecidas suas coordenadas. C é a velocidade da luz.

$$T0@1 = T0\_1@1 - | P1 - P0 | / C. \quad (1)$$

T0_n@1 é calculado pela Eq.(2), porque Pn e P0 também possuem coordenadas conhecidas.

$$T0\_n@1 = T0@1 + | Pn - P0 | / C. \quad (2)$$

T0_n@n é observado em APn. En_1 é calculado pela Eq.(3).

$$En\_1@1 = T0\_n@n - T0\_n@1. \quad (3)$$

En_1 é o erro de clock entre o AP1 e o APn. Através deste erro, é possível estabelecer uma sincronização entre os APs.

Para entender melhor como funciona a sincronização:

Quando chega um pacote vindo de AP0 para AP1, o T0_1@1 é o horário observado de chegada deste pacote em AP1. Calculamos então o T0@1(Horário de saída do pacote de AP0) através da fórmula:

T0@1 = T0_1@1 - | P1-P0|/C;

onde P1 e P2 são coordenadas conhecidas e C é a velocidade da Luz. Para chegar-se, portanto, ao valor de T0@1, diminui-se de T0_1@1 o tempo que levou o pacote para percorrer a distância entre P0 e P1, considerando que a velocidade de transmissão é C(velocidade da Luz), obtendo assim o tempo inicial da transmissão do pacote.

Através da fórmula:

T0_n@1 = T0@1 + | Pn - P0 | /C;

onde P1 e P2 são coordenadas conhecidas e C é a velocidade da Luz. Para chegar-se, portanto, ao valor de T0_n@1, soma-se o tempo da transmissão do pacote ao tempo que o pacote leva para percorrer a distância entre P0 e Pn considerando que a velocidade de transmissão é C, obtendo assim o tempo de chegada do pacote em APn.

Através do tempo estimado de AP0 até APn (T0_N@1), podemos estimar o erro de clock entre os APs envolvidos através da seguinte fórmula:

En_1@1 = T0_n@n - T0_n@1;

onde T0_n@n é o tempo observado da chegada do pacote de localização em APn. A diferença entre este tempo e o

tempo estimado, obtêm-se o En_1@1, que é a diferença entre os Clocks dos APs, que será utilizado na sincronização dos APs.

As coordenadas da estação foram estimadas usando o método LSM(*Least Square Method*). Neste método, admite-se que o sistema consiste em um conjunto de M APs. O tempo recebido pelo m-th AP como t_m. O AP que recebe o sinal mais forte é considerado o AP base do TDOA, e representamos o tempo de recebimento dele como t_{base}. A diferença entre os dois tempos é definida como $t_{diff,m} = t_m - t_{base}$. O valor de $t_{diff,m}$ é convertido para distância pela velocidade da luz C.

A representação das coordenadas estimadas (X_{cand}, Y_{cand}), e os m-th AP's como (X_m, Y_m). A distância entre as coordenadas é definida pela Eq.(4).

$$d_m = \sqrt{(X_m - X_{cand})^2 + (Y_m - Y_{cand})^2} \qquad (4)$$

As coordenadas do AP base é simbolizada por (X_{base}, Y_{base}). A distância entre o AP base e as coordenadas estimadas é definida pela equação 5.

$$d_{base} = \sqrt{(X_{base} - X_{cand})^2 + (Y_{base} - Y_{cand})^2} \qquad (5)$$

O resultado das diferenças entre eles é definido pela $d_{diff,m} = d_m - d_{base}$. O quadrado do erro das diferenças baseia-se na estimativa geométrica definida como $e_m = (c \times t_{diff,m} - d_{diff,m})^2$. O resultado do posicionamento é (X_{cand}, Y_{cand}), o qual chega-se em:

$$E = \sum_{m=1}^{M} e_m$$

4.6 Arquitetura do Sistema

A arquitetura interna do sistema é mostrada na figura 6. O sistema foi composto por um servidor de localização, access points e uma estação. O AP master(M-AP) é associado com a estação. No desenho, aparecem os APs slaves(S-APs), que recebem os pacotes entre o M-AP e a estação. O sistema necessita mais de três S-APs para duas dimensões e mais de quatro para posicionamento em três dimensões. O M-AP é usado para medir a diferença de clock entre os S-APs usados para medir o tempo de recebimento de pacotes enviados pela estação.

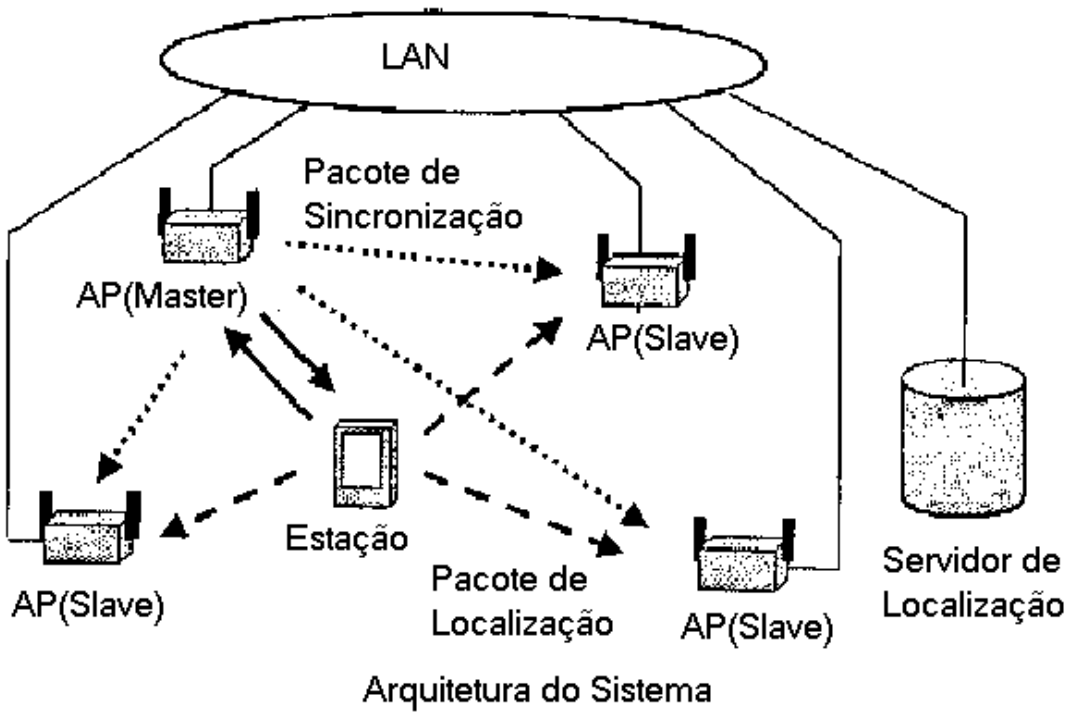


Figura 4.6: Arquitetura do sistema (YAMASAKI et al.,2005)

A figura 7 mostra graficamente o processo da detecção da posição. A aplicação de localização envia uma requisição de posicionamento ao servidor

de localização. O servidor envia uma requisição para os APs slaves para mudar para modo de recebimento. Os APs slave recebem a requisição e mudam para o modo de recebimento. No modo recebimento, os APs slaves capturam todos os pacotes no mesmo canal. O servidor envia um pacote de sincronização para a estação, e os APS slaves recebem e capturam o pacote de sincronização. A estação envia um pacote de localização para o servidor, e os APs slaves recebem e capturam o pacote de localização. Os APs slaves enviam o final do modo de captura e enviam o pacote de dados ao servidor. O servidor calcula o erro de clock dos APs slaves baseado na sincronização dos pacotes e dos valores de TDOA baseado nos pacotes de localização. O servidor calcula, então, a coordenada da estação usando estes valores. O servidor retorna os resultados para a aplicação.

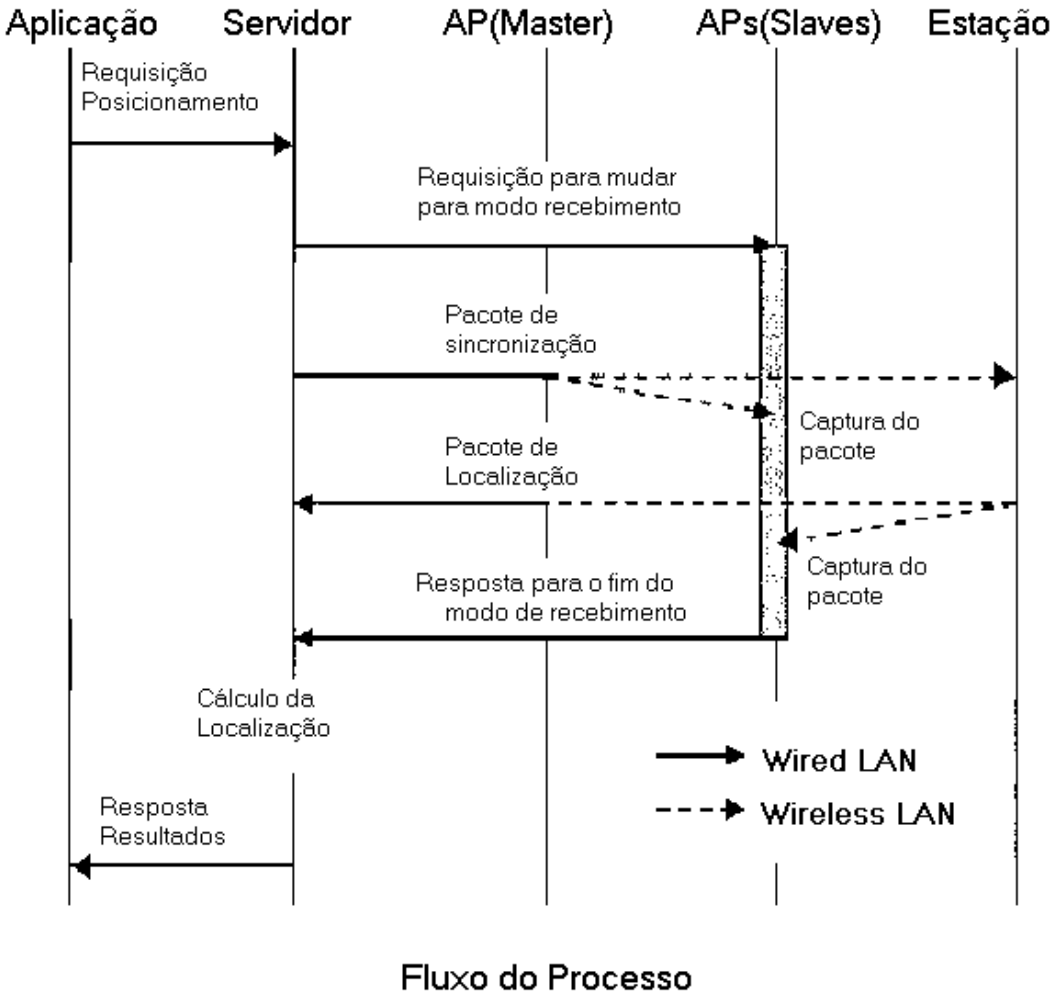


Figura 4.7: Fluxo do processo (YAMASAKI et al.,2005)

4.7 Aprimorando os Resultados

Para melhoria da precisão desta técnica é necessário: uma precisa medição do tempo de recebimento; uma boa síntese do tempo na utilização dos tipos de

pacotes recebidos e ainda um bom arranjo geométrico dos APs. A medição do tempo de recebimento do pacote baseia-se correlativamente CDMA(*Code Division Multiple Access*). Para IEEE 802.11b a taxa do chip é de 11 MHz. A resolução dessa taxa fica em 27m. Esta resolução não é suficiente para satisfazer as necessidades de aplicações indoor. Na técnica analisada consegue-se uma taxa erro de 21 cm usando uma alta amostragem de sinal de interpolação. Geralmente a acurácia do método é prejudicada pelo efeito de multipercurso do sinal, porque o pico de tempo é facilmente afetado pelo atraso causado pelo multipercurso da onda do sinal. A solução deste problema passa pela observação do "leading edge" do multipercurso da onda. Quando o efeito de multipercurso é grande, o erro do tempo do "leading edge" do nível do sinal é menor que o ponto do pico de tempo obtido entre os sinais observados.

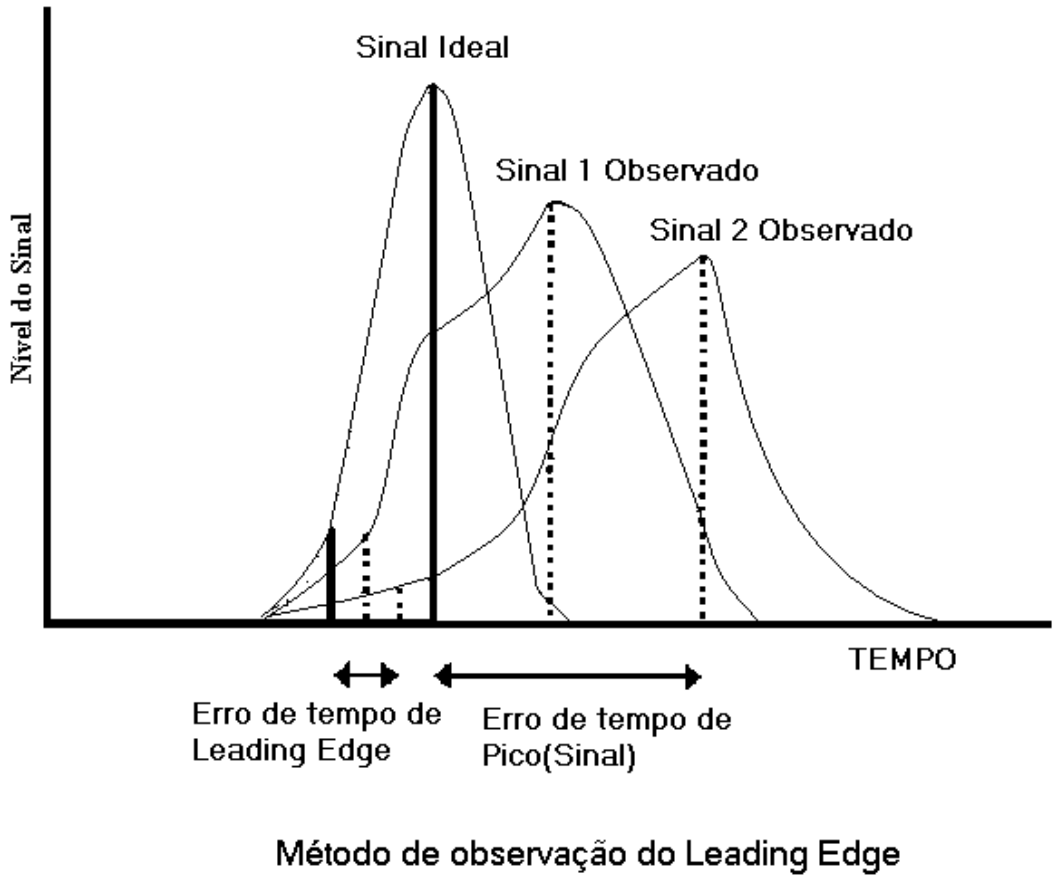


Figura 4.8: Método de observação do Leading Edge (YAMASAKI et al.,2005)

As diferentes técnicas de posicionamento sob diferentes condições ambientais são categorizadas em tempo, espaço e frequência. Por tempo, mede-se a posição sob intervalos de tempo. Como o passar do tempo, o efeito de multipercurso é alterado com as mudanças no ambiente. Por espaço, na medição da posição usam-se múltiplas antenas em diferentes coordenadas. Se as antenas forem separadas por meia-onda, o ambiente de multipercurso muda

consideravelmente, incrementando o efeito da média. Por frequência, mede-se o posicionamento utilizando múltiplos canais.

O terceiro método otimiza o arranjo geométrico dos APs. Na técnica TDOA, as coordenadas das estações são obtidas por triangulação. Para isso, a posição da estação deve ser coberta por três ou mais APs slaves. E ainda é importante assegurar o LOS(*Line of Sight*) linha de visada entre o AP principal e os APs slaves. O AP Master envia o sinal de sincronização para os APs slaves. Se a sincronização contiver um atraso de sinal, a sincronização conterá um erro. Consequentemente, o AP Master e os APs Slaves devem ser rearranjados até que os APs Slaves possam receber o sinal direto do AP Master. A causa do erro de sincronização é o tempo do erro observado da sincronização do pacote, e é identica a causa do erro de posicionamento praticamente. Portanto, no arranjo geométrico dos APs é muito importante ser preservada a linha de visada(LOS) entre o AP Master e os AP Slaves

5 CONCLUSÃO

Todas as técnicas utilizadas por LBS *Indoor* sofrem com o efeito mutipercurso do sinal em maior ou menor grau, comprometendo a acurácia do sistema. A vantagem da técnica TDOA em relação às demais é que ela ao estimar a posição mediante o tempo de propagação do sinal de RF, pode detectar tentativas de acesso ou invasão de dispositivos com sinal amplificado mais distantes ou fora do perímetro conhecido de uma rede Wi-Fi. Outra vantagem é que ela não necessita de um pré-mapeamento e armazenamento num banco de dados de informações, obtidas do ambiente no qual se quer implantar em relação às técnicas que utilizam mapeamento de RSSI. A desvantagem reside em que sua a implementação é muito mais complexa e onerosa em relação à técnica de mapeamento de RSSI, onde normalmente usa-se a infra-estrutura existente da rede e não são necessárias alterações de hardware nos APs como na técnica TDOA. Dependendo, porém, do nível de segurança que se deseja obter tanto numa rede Wireless quanto em um LBS, o custo da implantação da técnica TDOA compensaria, pois a rede tornar-se-ia mais protegida de acessos indesejados. Penso, portanto, que em uma rede sem fio em que a segurança da própria rede Wireless seja elevada ou de um LBS implantado necessite de segurança para operar, a técnica TDOA compensaria o seu custo inicial, pois ela contemplaria este quesito onde outras técnicas falham. O argumento que o TDOA não resulta em uma boa acurácia, não é justificável, pois por menores que sejam os resultados alcançados pela técnica TDOA, ainda assim, ela pode fornecer informações que as outras técnicas, baseadas apenas na potência do sinal de propagação de RF não conseguem fornecer ao administrador do sistema.

Dentro destas diversas técnicas, afirmo que um sistema de localização de dispositivos móveis que utilize TDOA, pode fornecer eficaz segurança ao sistema e ainda vir a complementar um sistema *IDS-WireLess*, pois auxiliará além da identificação de acessos indesejados, a localização de dispositivos que compõem a própria rede, detectando outros dispositivos estranhos ou indesejados à rede Wi-Fi.

REFERÊNCIAS

GUEDES, E. M. P. **Estudo de Técnica Híbrida de Localização de Estações Móveis baseada em TDOA e AOA**. 2003. 119 f. Dissertação (Mestrado em Engenharia Elétrica do Intituto Militar de Engenharia) – IME, Rio de Janeiro.

HIGHTOWER, J,; BORRIELLO, G. A survey and taxonomy os location sensing system for ubiquitous computing. Washington: Departament of Computer Science and Engineering, Univerty of Washington, 2001. (Technical Report UW-CSE 01-08-03)

MOURA, A. I. **WBLS: Um Sistema de Localização de Dispositivos Móveis em Redes Wi-Fi**. 2007 120 f. Dissertação (Mestrado na Escola Politécnica da Universidade de São Paulo) – Departamento de Engenharia de Computação e Sistemas Digitais, São Paulo.

NUNES, B. A. A. **Um Sistema de Localização para Redes Wi-Fi baseado em Níveis de Sinal e Modelo Referenciado de Propagação.** 2006 95 f. Dissertação (Mestrado em Ciências em Engenharia de Sistemas e Computação) – UFRJ, Rio de Janeiro.

RENNER, R, J. **Mecanismos de Localização de Estações Móveis 802.11 – Análise e Prototipagem**. 2008. 54 f. Trabalho de Conclusão (Curso de Sistemas de Informação) – Instituto de Ciências Exatas e Tecnológicas, FEEVALE, Novo Hamburgo.

RUSSEL,S. Detecting and locating rogue access point Ames, IO, US: Department of Eletrical and Computer Engineering, Iowa State University, 2003. (Technical Report CprE 537).

YAMASAKI R.; OGINO, A.; TAMAKI, T.; UTA, T.; MATSUZAWA, N. KATO, T. TDOA location system for IEEE 802.11b WLAN. In: WIRELESS COMMUNICATIONS AND NETWORKING CONFERENCE – WCNC, 2005, New Orlenans. Proceedings… Piscataway, NJ, US: IEEE,2005. p. 2338-2343