Redes 802.11 em Centros Urbanos: Varredura, Estatísticas e Aplicações

Ulysses Cardoso Vilela[1], **Kleber Vieira Cardoso**[1], **José Ferreira de Rezende**[1]

[1]GTA - PEE - COPPE – Universidade Federal do Rio de Janeiro (UFRJ)
Caixa Postal 68.504 – 21.945-970 – Rio de Janeiro – RJ – Brasil

{ulysses,kleber,rezende}@gta.ufrj.br

Abstract. *We are witnessing today an exponential growth of the use of 802.11 networks by users with different individual backgrounds on the technology. This leads to a disordered growth that has been mapped by different initiatives thanks to a technique known as wardriving. This technique consists of using computers equipped with 802.11 interfaces, GPS and a software able to scan the channels used by these networks. When in motion, such equipments collect information about the encountered networks together with the geographic position of the equipment performing the scanning. With this information, it is possible to carry through statistics related to the penetration and behavior of the users in the use of the technology. These statistics can provide valuable information that can be used to improve the performance of such networks. This article describes the methodology used to scan 802.11 networks located in Rio de Janeiro, then it provides and evaluates statistics of more than 4,000 networks and, finally, exemplifies the use of these results in the conception of new applications and mechanisms for these networks.*

Resumo. *Assistimos hoje a um crescimento exponencial do uso de redes 802.11 por usuários com diferentes níveis de conhecimento da tecnologia. Esse crescimento desordenado vem sendo mapeado por diferentes iniciativas graças a uma técnica conhecida como wardriving. Essa técnica consiste na utilização de computadores equipados com interfaces 802.11, GPS e um software capaz de efetuar uma varredura nos canais utilizados por essas redes. Ao se movimentarem, tais equipamentos coletam informações sobre as redes encontradas juntamente com a posição geográfica do equipamento em deslocamento. A partir dessas informações, é possível realizar estatísticas relacionadas à penetração da tecnologia e ao comportamento dos seus usuários. Estas estatísticas podem fornecer valiosas informações para a melhoria do desempenho de tais redes. Esse artigo descreve a metodologia usada na varredura de redes 802.11 localizadas no Rio de Janeiro, fornece e avalia estatísticas sobre as mais de 4 mil redes encontradas e, por fim, exemplifica o uso desses resultados na concepção de novas aplicações e mecanismos para essas redes.*

1. Introdução

Nos últimos anos, temos observado um crescimento vertiginoso e desordenado do uso de redes IEEE 802.11, principalmente em ambientes domiciliares. Diferentemente das redes cabeadas, as redes sem fio, mesmo que instaladas de forma independente e administradas

por usuários distintos, compartilham escassos recursos de banda entre elas e interferem uma nas outras. Isso ocorre porque as redes sem fio geralmente se estendem além da área física que define o domicílio de um usuário, podendo alcançar algumas dezenas de metros para fora de uma casa ou apartamento. Assim, torna-se importante para a continuidade do seu sucesso e crescimento que o comportamento do usuário na implantação desse tipo de rede seja conhecido, permitindo que ele seja alterado de forma a melhorar o desempenho e a segurança no uso dessa tecnologia.

Nos últimos cinco anos, diversas iniciativas surgiram em países desenvolvidos no intuito de mapear as redes em uso, permitindo estudar e entender o comportamento de uso da tecnologia por parte dos usuários [WiGLE.net , WiFiMaps.com , Wi-Fi-Zones.com , WiFinder]. Nessas iniciativas, esse mapeamento é alcançado graças à contribuição de milhares de voluntários em todo o mundo utilizando uma técnica batizada de *wardriving*. Apesar do nome ter origem em uma atitude maliciosa de procurar redes vulneráveis a ataques, de fato, essa técnica oferece uma poderosa ferramenta para o recenseamento ou pesquisa de campo (*site survey*) em larga escala. A técnica de *wardriving*, ainda pouco explorada no Brasil, consiste na utilização em veículos automotivos de computadores dos mais variados tipos (*laptops, palmtops* e até mesmo celulares) equipados com interfaces de rede IEEE 802.11, GPS e um software capaz de efetuar uma varredura nos canais utilizados pelas redes 802.11. Ao se movimentarem durante a varredura, tais equipamentos coletam um certo número de informações sobre as redes encontradas juntamente com a posição geográfica do equipamento em deslocamento. De posse dessas informações, torna-se possível extrair, com um certo nível de detalhe, dados tais como densidade de pontos de acesso numa determinada região, grau de compartilhamento de canais, nível de segurança adotado, entre outros. Essas informações, mesmo que incompletas e imprecisas, permitem aos pesquisadores estudarem o problema da alocação de canal em topologias de rede mais próximas do real [Mishra et al. 2006], estudar a viabilidade do uso de redes IEEE 802.11 em aplicações veiculares [Bychkovsky et al. 2006], etc..

Uma importante informação coletada através do *wardriving* é a localização geográfica dos APs encontrados. Na prática, essa localização é estimada a partir das informações coletadas em múltiplas varreduras de um mesmo AP e diferentes métodos podem ser usados para estimá-la. Um método bastante simples considera apenas que o AP está localizado na posição onde o equipamento de varredura recebeu o sinal mais forte vindo daquele AP. No entanto, varreduras realizadas de diferentes posições, ou seja, a obtenção de diversas tuplas $posicao, sinal$, podem ser usadas para realizar uma triangulação e melhor prever o posicionamento de um determinado AP. Diferentes algoritmos são apresentados em [Cheng et al. 2005] e brevemente descritos a seguir. No entanto, essas estimativas podem ser bastante imprecisas como demonstrado em [Kim et al. 2006], mas isso não impede que tais informações sejam ainda bastante valiosas para a concepção de novas aplicações e mecanismos para essas redes.

Este artigo descreve, na Seção 2, a base de funcionamento do *wardriving*, assim como os dispositivos e o software usados, neste trabalho, para realizar a varredura de redes 802.11 localizadas em alguns bairros da cidade do Rio de Janeiro. Ainda nessa seção, são descritos brevemente os algoritmos usados para estimar o posicionamento dos APs e as divergências decorrentes da aplicação dos mesmos nos dados coletados. Na Seção 3, várias estatísticas sobre as mais de quatro mil redes mapeadas por *wardriving*

são mostradas e avaliadas. Por fim, a Seção 4 exemplifica o uso desses resultados na concepção de novas aplicações e mecanismos para a melhoria do desempenho dessas redes. A Seção 5 apresenta as conclusões tiradas da realização desse trabalho.

2. Varredura de Redes 802.11

A base de funcionamento da varredura de redes 802.11 consiste no envio de quadros de gerenciamento, definidos no protocolo IEEE 802.11, chamados `Probe Request`. O envio desses quadros permite à estação móvel determinar quais pontos de acesso (APs - *Access Points*) estão dentro do seu alcance, podendo assim realizar operações de associação ou de mudança de ponto de acesso, estas últimas chamadas de *handoff*. Ao receberem um quadro `Probe Request`, os APs respondem com um quadro `Probe Response` que contém informações de funcionalidades do AP e as taxas suportadas pelos mesmos. Esse procedimento de envio de quadros `Probe Request`, em todos os canais utilizados pela tecnologia IEEE 802.11, e a espera por quadros `Probe Response` é conhecido por varredura ativa (*active scanning*).

Pelo processo de varredura ativa, é possível detectar todos os APs ativos dentro do alcance da estação móvel, independentemente do canal em que ele esteja operando. No entanto, algumas condições devem ser respeitadas para que seja possível detectar um determinado AP. Primeiramente, é necessário que o AP esteja habilitado a responder a quadros de `Probe Request`. Alguns fabricantes de APs permitem, através de suas interfaces de gerenciamento, desabilitar essa funcionalidade. Segundo, é necessário que o AP esteja dentro do raio de alcance da estação móvel e também que a estação móvel esteja dentro do raio de alcance do AP, uma vez que os enlaces podem ser assimétricos. Múltiplos fatores afetam essa segunda condição. Como ambos os quadros `Probe Request` e `Probe Response` são transmitidos em difusão (*broadcast*), o padrão 802.11 define que eles devem ser transmitidos em taxa básica que dependendo do equipamento utilizado pode ser de 1 ou 2 Mbps. Nessas taxas, onde uma modulação mais imune a ruído é utilizada, é necessário uma potência de sinal muito inferior [1] àquela necessária em taxas mais altas para que o receptor possa detectar e demodular corretamente a informação recebida. Desta forma, é possível detectar, através do processo de varredura, um grande número de APs.

Em interfaces de rede 802.11 encontradas geralmente no mercado, é necessária uma potência da ordem de -90 dBm para que um quadro transmitido em 1 Mbps seja corretamente recebido. Essa potência é duas ordens de grandeza inferior à potência necessária para se detectar um quadro transmitido em 11 Mbps. Ao considerarmos a propagação do sinal na freqüência de 2.4GHz e o que foi explicado anteriormente, o sinal transmitido em uma taxa de 1 Mbps pode alcançar uma distância muito superior àquelas alcançadas em taxas superiores. Um outro fator que afeta esse alcance é a potência do sinal transmitido por ambos os equipamentos (AP e estação móvel) que depende da potência de saída das interfaces de rede utilizadas e a existência ou não de antenas em tais equipamentos.

2.1. Hardware e Software usados na Coleta de Dados

Para utilizar a técnica de *wardriving* e, conseqüentemente, de varredura ativa, foi utilizado um computador de mão Dell Axim X50v (Figura 1), o qual já vem equipado com uma

[1] O valor dessa potência depende da sensibilidade do hardware do receptor do sinal.

interface de rede 802.11 (com antena interna) e também com um receptor GPS Compact Flash: modelo GlobalSat BC-337, com 20 canais, antena externa e capacidade WAAS (*Wide Area Augmentation System*). O Dell Axim X50v tem um processador Intel PXA270 de 624MHz, 64MB de RAM, 128 MB de ROM e utiliza o sistema operacional *Windows Mobile 2003 Second Edition* versão 4.21.1088. O software utilizado para a varredura ativa foi o WiFiFoFum versão 2.1.1 desenvolvido pela Aspecto Software. Esse software coleta informações de localização do receptor GPS por uma porta serial, a qual é emulada pelo *driver* que controla o receptor GPS Compact Flash.

(a) Dell Axim X50v e receptor GPS (b) Dell Axim X50v no veículo

Figura 1. Equipamento utilizado na varredura.

Para cada quadro `Probe Response` recebido corretamente, o software registra tanto informações locais ao equipamento, como a localização geográfica extraída do receptor GPS e o nível do sinal recebido durante a recepção do quadro, quanto extraídas de campos do quadro de gerenciamento recebido. As seguintes informações são coletadas e armazenadas em arquivos no computador de mão:

- $RSSI$ (*Received Signal Strength Indicator*)[2] - o $RSSI$ indicado pela interface de rede do Dell Axim assume valores entre 59 (MinRSSI) e 139 (MaxRSSI). Esses valores correspondem a -90 dBm e -10 dBm de potência de sinal, respectivamente.
- $SSID$ - fornece o identificador atribuído a um determinado AP pelo próprio fabricante (configuração *default*) ou pelo proprietário do mesmo.
- Canal utilizado pelo AP - em geral, um valor entre 1 e 11, representando as faixas de freqüência utilizadas. Alguns equipamentos podem apresentar um valor de canal acima de 11, conforme será discutido posteriormente.
- Latitude e longitude - coordenadas do equipamento que realiza a varredura.
- Tipo da rede - infra-estruturada ou *ad hoc*.

[2]De acordo com o padrão 802.11, o RSSI refere-se à energia de radio-freqüência medida por um circuito na interface de rede cujo valor numérico é representado por um inteiro de um byte podendo assumir valores arbitrários entre 0 e 255.

- WEP (On/Off) - a variável booleana WEP indica se o AP em questão utiliza criptografia nessa rede [3].

Para realizar o *wardriving* descrito nesse artigo, foram percorridos aproximadamente 500 Km entre o Centro e bairros da Zona Sul do Rio de Janeiro (Copacabana, Flamengo, Botafogo, Humaitá, Ipanema, Leblon, Jardim Botânico, Gávea e Lagoa). Esse trecho foi percorrido entre outubro e dezembro de 2006, em diferentes dias da semana e horários variados. Foram registradas mais de quatro mil redes 802.11 infra-estruturadas (APs) num total de aproximadamente 150 mil varreduras. A Figura 2 mostra a distribuição desses APs sobrepostos ao mapa da cidade do Rio de Janeiro disponibilizado pelo GoogleMaps [Google].

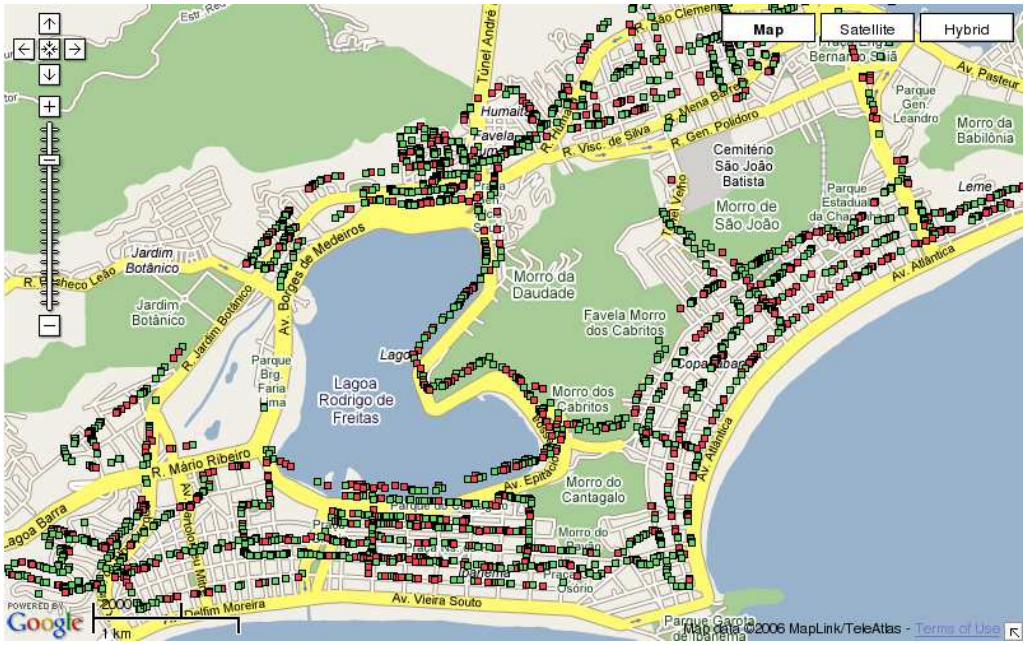


Figura 2. Distribuição de APs na cidade do Rio de Janeiro.

2.2. Análise das Varreduras

O gráfico da Figura 3 mostra as funções densidade de probabilidade (PDF) e distribuição de probabilidade (CDF) do número de varreduras para cada AP. A PDF está em escala logarítmica e mostra que 18,24% dos APs têm apenas uma amostra de informação, enquanto que 2.7% dos APs contam com 10 amostras. A CDF mostra que 50% dos APs têm pelo menos 10 amostras.

Na Figura 4 são apresentadas a PDF e a CDF do número de APs por varredura, ou seja, o número de `Probe Responses` recebidos a partir de um único `Probe Request`. Esse resultado pode ser visto como a densidade de APs observada por um equipamento móvel. Como pode ser visto, 99% das varreduras retornam 6 ou menos APs, enquanto em torno de 70% das varreduras foram detectados apenas um AP e o maior número de APs em um mesma varredura foi 12.

[3]Pelas informações presentes no quadro `Probe Response` não é possível identificar qual protocolo de segurança (WEP, WPA, TKIP, AES) é utilizado pelo AP. Esta booleana indica apenas se ela usa ou não tais protocolos.

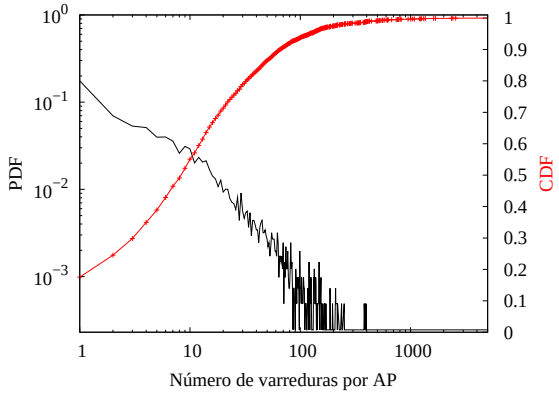


Figura 3. PDF e CDF do número de varreduras por AP.

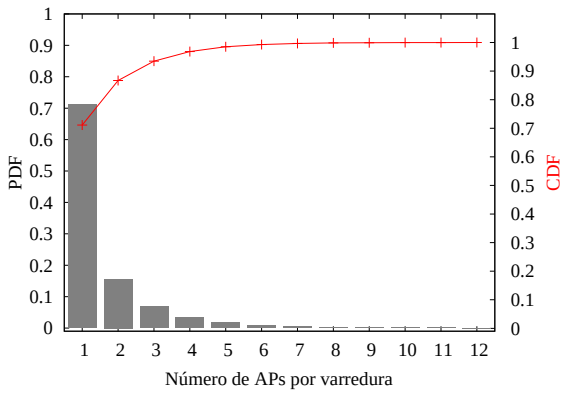


Figura 4. PDF e CDF do número de APs por varredura.

2.3. Estimativa do Posicionamento dos APs

Como foi visto anteriormente, um AP pode aparecer uma ou múltiplas vezes nos *traces* coletados durante o *wardriving*. Cada amostra de um mesmo AP contém uma posição geográfica e a potência do sinal recebido do AP nessa posição. A partir dessas informações, é possível calcular uma posição aproximada do equipamento em questão. A acurácia desse posicionamento é importante para algumas estatísticas, como a densidade de APs numa determinada região, e para algumas aplicações, como aquelas que fornecem a localização de um nó móvel a partir do conhecimento prévio do posicionamento dos APs.

Para estimar a posição em que um AP está localizado podem ser usados diferentes algoritmos. Dentre os mais comuns estão o baseado no **sinal mais forte recebido**, o **centróide** e o **centróide ponderado**. O centróide, também chamado de triangulação, consiste em calcular o centro geométrico[4] de todas as posições em que um dado AP foi observado, enquanto o centróide ponderado considera o nível de sinal recebido em cada posição e utiliza esse valor para ponderar cada amostra. Obviamente, quando há apenas uma amostra de um determinado AP, as três soluções fornecem o mesmo resultado.

Na Figura 5 são mostradas as diferenças entre o posicionamento obtido, dos mais de quatro mil APs coletados, ao se usar essas três abordagens. Como pode ser observado, a divergência é relativamente alta entre a posição obtida pelo sinal mais forte e os dois tipos de centróide, pois em torno de 60% das amostras a diferença está acima de 10 metros. Por outro lado, a diferença entre os dois tipos de centróide é baixa, sendo que mais de 98% das divergências estão abaixo de 10 metros. De acordo com [Kim et al. 2006], os melhores resultados quanto ao posicionamento dos APs são obtidos com o centróide ponderado. Por esse motivo, todas as informações relativas ao posicionamento dos APs, utilizadas neste trabalho, levam em conta a utilização desse algoritmo de estimativa.

[4]De fato, é calculado o centro geodésico dos APs.

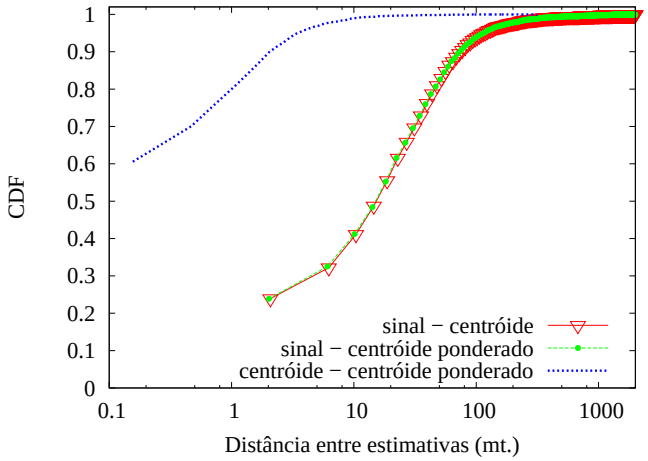
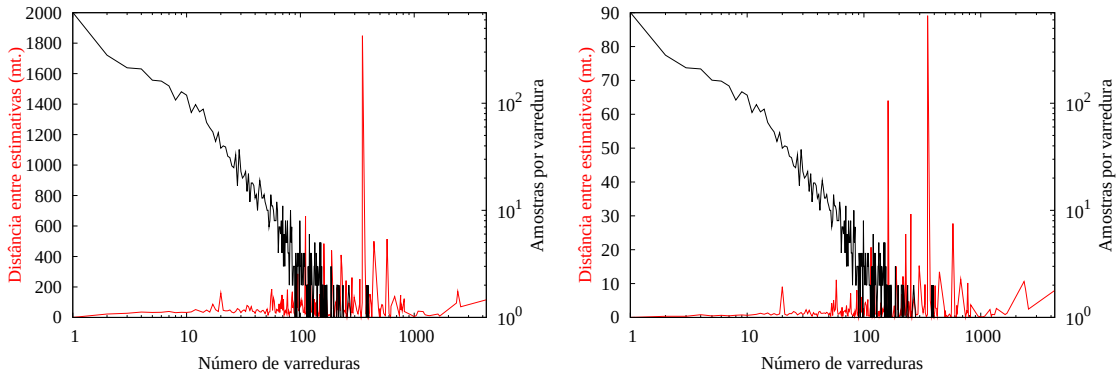


Figura 5. CDF das divergências entre os algoritmos de posicionamento.

A Figura 6 ilustra a relação entre a divergência média e o número de amostras por número de varreduras. É esperado que a divergência média aumente à medida que o número de amostras diminui. Até 10 varreduras, a média da diferença entre os algoritmos sinal mais forte recebido e o centróide ponderado é baixa, ficando inferior a 34 metros. O mesmo ocorre com a divergência média entre centróide e centróide ponderado, a qual fica inferior a 70 centímetros. Entre 10 e 100 varreduras as diferenças médias aumentam significativamente nos dois gráficos, alcançando acima de 200 metros para sinal mais forte versus centróide ponderado e acima de 10 metros para centróide versus centróide ponderado.



(a) Sinal - centróide ponderado (b) Centróide - centróide ponderado

Figura 6. Divergências dos posicionamentos usando diferentes algoritmos.

Acima de 100 varreduras, o comportamento é de difícil descrição, uma vez que o número de amostras cai abaixo de 10. É interessante observar que o aumento do número de varreduras não implica em uma diminuição da divergência entre as abordagens de posicionamento. Esse resultado era previsto para a diferença entre sinal mais forte e centróide ponderado, pois cada nova varredura pode identificar uma nova posição do AP se houver um sinal mais forte, enquanto o centróide ponderado é pouco afetado. No entanto, esse resultado também ocorre entre os dois tipos de centróide, ou seja, mesmo

para um grande número de varreduras (acima de 100), a diferença chega a dezenas de metros.

3. Resultados Estatísticos

Uma vez coletadas as informações, vários *scripts* foram criados para realizar um tratamento estatístico dessas informações. Uma estatística importante é a distribuição dos APs nos canais de operação disponibilizados pelo padrão IEEE 802.11. De acordo com as normas da FCC definidas na América do Norte, que acabam sendo seguidas na maior parte do mundo, 11 canais estão disponíveis para operação do padrão. No entanto, existem alguns países que utilizam um número diferente de canais disponíveis. No Japão, por exemplo, são disponibilizados 14 canais na banda ISM [Hills and Friday 2004]. Na varredura realizada, encontramos alguns APs utilizando canais de operação acima de 11, o que supõe que esses equipamentos foram adquiridos em países que utilizam os 14 canais ou então que os usuários desses dispositivos utilizam um software capaz de configurá-los nesses canais.

A Figura 7 mostra a percentagem do total de APs encontrados em cada um dos 14 canais. Como pode ser visto no gráfico, uma grande parcela dos APs (89,9%) utilizam os canais 1, 6 ou 11. Esses canais não se sobrepõem no espectro de freqüência, ou seja, não causam interferência mútua. No entanto, essa distribuição não é feita de forma homogênea uma vez que 69,2% dos APs utilizam o canal 6. Isto se deve ao fato da maioria dos fabricantes utilizar esse canal como padrão (*default*) e os usuários não se preocuparem em modificá-lo de forma a evitar interferência com outros APs na sua vizinhança. Na Seção 4, alguns experimentos serão realizados para demonstrar a perda de desempenho de determinadas redes considerando-se essa alocação de canal.

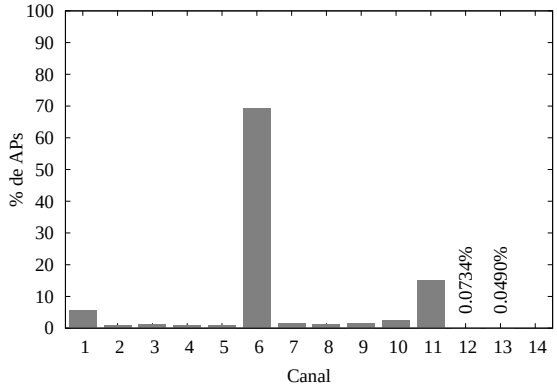


Figura 7. Distribuição dos Canais de Operação.

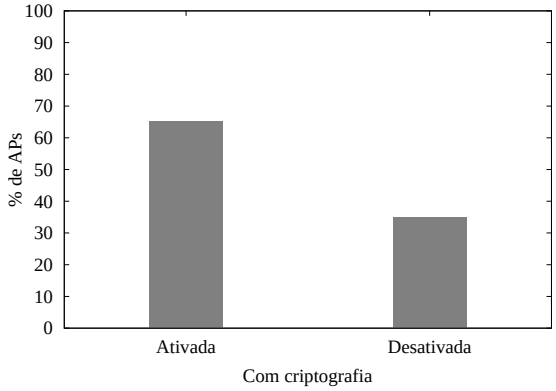


Figura 8. APs protegidos por criptografia.

A Figura 8 mostra a percentagem do total de APs que utilizam algum mecanismo de segurança ou não na camada de enlace do 802.11. O percentual de APs com criptografia desativada é próximo de 35%, o qual é inferior ao valor observado nas estatísticas apresentadas em [WiGLE.net], no qual a quantidade de APs sem criptografia fica em torno de 43%. Uma vez que essa não é opção padrão dos equipamentos, essa estatística sugere que os usuários de rede sem fio no Brasil tem uma preocupação maior com segurança. A estatística da Figura 10 aventa que a maior parte dos usuários brasileiros têm pelo menos

uma preocupação mínima com a customização de seus equipamentos, uma vez que mais de 70% dos SSIDs não são os padrões dos fabricantes.

A partir dos quadros de `Probe Response`, é possível extrair o endereço MAC dos APs coletados. Os três primeiros bytes desse campo representam um identificador único associado a seu fabricante, fornecida pelo IEEE [IEEE Registration Authority]. De fato, um mesmo fabricante pode ser proprietário de faixas não contíguas de endereços. Com base nesses dados, a Figura 9 mostra alguns dos fabricantes mais encontrados nas varreduras executadas. Como pode ser visto pela figura, o fabricante D-Link possui a maior parte do mercado de APs na cidade do Rio de Janeiro, seguido pelo fabricante Cisco-Linksys. Essa estatística é diferente da média mundial, onde Cisco-Linksys é quem mais comercializa pontos de acesso, seguida pela empresa D-Link, como pode ser visto em [WiGLE.net]. Essa inversão de posições não é um fato atípico, uma vez que os produtos D-Link tenham, em geral, um custo mais baixo que os equivalentes da Cisco-Linksys, motivando sua aquisição em países cujo valor de bens de tecnologia é elevado, como o Brasil. Porém, nesse caso, mais importante que as causas, são os efeitos dessa maior adoção por um determinado fabricante em detrimento de outro. Normalmente, todos os fabricantes seguem os padrões IEEE, porém as normas IEEE 802.11 deixam margem para divergência nas implementações. Sendo assim, ter mais equipamentos de um fabricante X do que de um fabricante Y, pode significar ter mais equipamentos com uma determinada falha de segurança, algum recurso extra para obtenção de mais banda, suporte a monitoramento de enlace, protocolos de roteamento *ad-hoc*, possibilidade de substituição de *firmware*, etc. Ou seja, há trabalhos científicos em redes sem fio 802.11 que podem ser motivados ou desmotivados pela simples estatística de quais são os equipamentos mais adotados e, portanto, o que se espera encontrar no ambiente real.

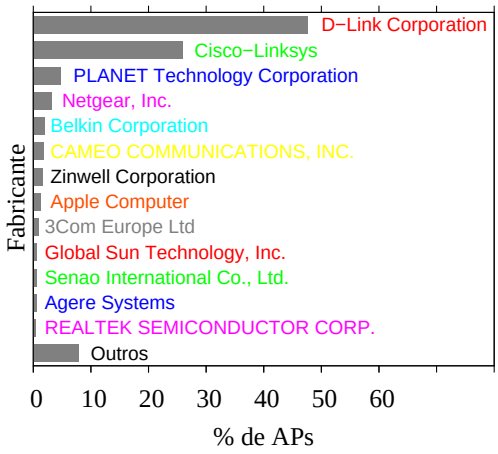


Figura 9. Fabricantes mais encontrados nas varreduras.

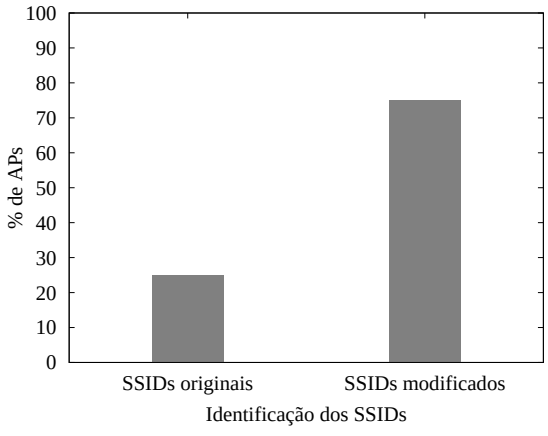


Figura 10. Conteúdo dos SSIDs.

3.1. Densidade e Vizinhança de APs

A Figura 11 apresenta a densidade do número de APs medida em diferentes áreas. A área que cobre todos os APs identificados durante o *wardriving* é de aproximadamente 123.846.453 m^2, porém uma parte significativa compreende o mar, morros, áreas verdes, etc. ou simplesmente não foi percorrida durante as medições. A área total foi dividida em

sub-áreas menores, conforme ilustra cada curva do gráfico, e todas as sub-áreas que não tivessem pelo menos um AP foram removidas do cálculo da densidade.

Como era esperado, a densidade aumentou à medida que se diminuiu o tamanho das sub-áreas, pois a quantidade de espaço vazio que é eliminada aumenta. No entanto, o eixo X está em escala logarítmica e, portanto, podemos concluir que as áreas menores apresentaram densidade significativamente mais alta. Para ilustrar, podemos verificar que menos de 5% das sub-áreas de 10.000 m^2 tiveram densidade superior a 0.001 AP/m^2, enquanto mais de 30% das sub-áreas de 2.500 m^2 alcançaram densidades acima desse valor. Esses dados confirmam a informação visual que havia sido obtida no mapa, o qual mostra alguns bairros ou partes de bairros com intensas aglomerações de APs. Ou seja, a distribuição dos APs nos bairros e dentro dos mesmos está longe de ser uniforme. Foi notada ainda uma densidade atipicamente alta em partes de alguns bairros, onde podem ser encontrados até 6 APs em uma sub-área de 100 m^2. Os bairros que apresentam essas altas densidades foram alguns dos mais nobres da cidade, a saber: Alto Leblon, Ipanema e Lagoa. A única exceção foi uma área no centro da cidade, na qual se encontra um grande centro de compras de produtos de informática. Ou seja, a menos de casos especiais que demandam grande número de APs (como um centro de compras ou um provedor de acesso), em geral, a aquisição de equipamentos 802.11 parece estar associada à renda dos usuários.

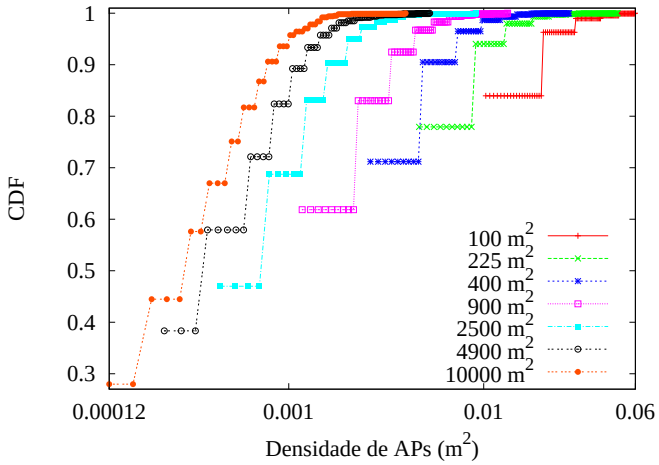
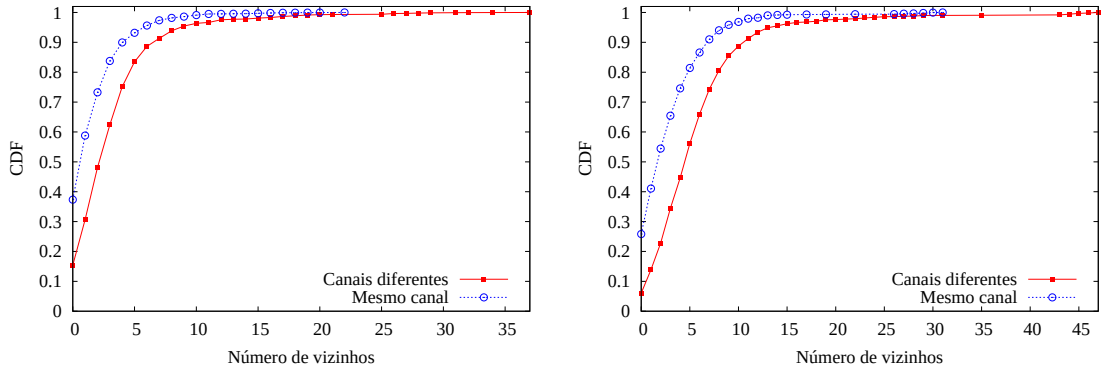


Figura 11. CDF da densidade de APs.

Os fabricantes de equipamentos 802.11 convencionais anunciam, geralmente, um alcance em ambiente *indoor* entre 30 e 50 metros. Ambientes *outdoor* apresentam distâncias maiores, podendo chegar a centenas de metros. No entanto, em ambientes urbanos densos, como os bairros do Rio de Janeiro que foram pesquisados nesse trabalho, essas faixas de alcance são compatíveis. Na Figura 12 é apresentada a função de distribuição da quantidade de vizinhos dos APs considerando-se os alcances de 30 e 50 metros. Foram avaliados dois tipos de vizinhanças, aquela formada por quaisquer APs dentro da faixa de alcance, mesmo que em **canais diferentes**, e APs que estão dentro da faixa de alcance e no **mesmo canal**.

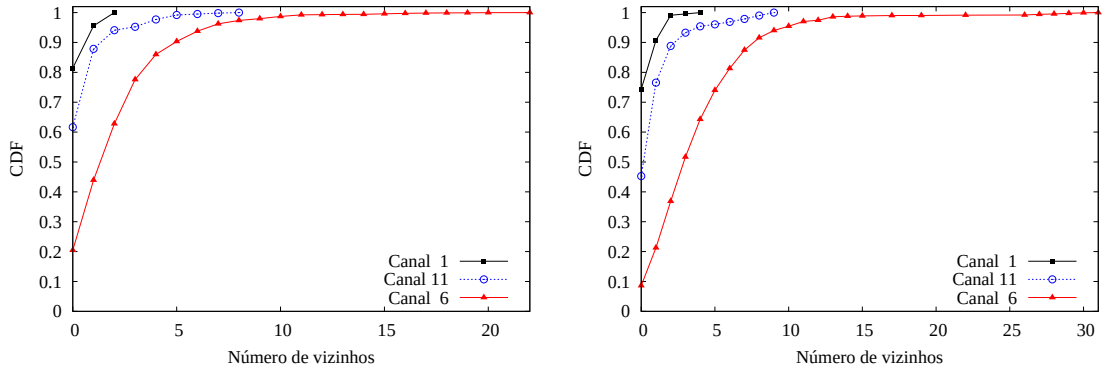
A Figura 12 confirma a alta densidade APs que havia sido comentada anteriormente. Para o alcance de 30 metros, mais de 50% dos APs têm pelo menos dois vizinhos,



(a) Alcance de 30 metros (b) Alcance de 50 metros

Figura 12. Grau de vizinhança dos APs.

subindo para 4 APs quando o alcance é de 50 metros. Ainda que consideremos apenas APs no mesmo canal, a uma distância de até 30 metros mais de 40% dos APs têm pelo menos 1 vizinho. A uma distância de até 50 metros, há mais de 58% dos APs com pelo menos 1 vizinho. Conforme havia sido dito antes, foram observadas intensas aglomerações de APs na maior parte das regiões pesquisadas, essa informação pode ser verificada pelo baixo percentual de APs com nenhum vizinho: menos de 7%, considerando-se um alcance de 50 metros.



(a) Alcance de 30 metros (b) Alcance de 50 metros

Figura 13. Quantidade de vizinhos no mesmo canal.

Na Figura 13 é mostrada a vizinhança dos APs por canal, considerando-se os três canais que não se sobrepõem: 1, 6 e 11. Na Seção 3, havíamos verificado que o canal mais utilizado é o 6, seguido do 11 e por fim o 1. Era esperado que esses canais mantivessem a mesma classificação em termos de vizinhança concorrente, ou seja, número de vizinhos no mesmo canal. As razões principais para essa previsibilidade são a ausência de coordenação entre os APs instalados e não preocupação (ou conhecimento) dos usuários na realização de uma pesquisa de campo antes da implantação de um novo equipamento, de forma a evitar concorrência do meio com vizinhos. No pior caso considerado, ou seja, a uma distância de 50 metros, menos de 11% dos APs no canal 1 encontram algum vizinho e no máximo 4 vizinhos podem ser encontrados a essa distância nesse canal. No outro extremo está o canal 6, no qual apenas 21% dos APs não encontram nenhum vizi-

nho a uma distância de 30 metros, caindo para 9% se considerarmos uma distância de 50 metros.

Esses resultados mostram que muitos usuários podem estar experimentando problemas de desempenho em suas redes locais sem fio por não realizarem um procedimento básico de pesquisa de campo. Por outro lado, apesar de simples, não é razoável esperar que usuários leigos tenham esse tipo de preocupação. Para lidar com esse tipo de problema um solução é proposta em [da Silva and de Rezende 2007], a qual permite uma alocação ótima dos canais usando um algoritmo distribuído.

4. Aplicações e Mecanismos

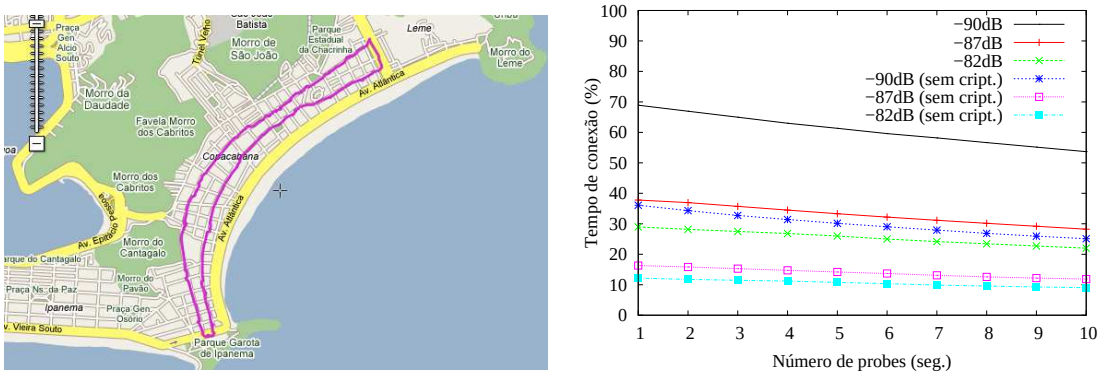
Há uma grande variedade de usos para as informações coletadas nesse trabalho e nessa serão detalhadas duas delas. A primeira é uma aplicação veicular, na qual é analisada a cobertura oferecida pelas redes 802.11 a um usuário que se move dentro de um automóvel. A segunda é uma avaliação de capacidade da rede, empregando os dados reais de posição e canal dos APs.

Para demonstrar a viabilidade de uma aplicação veicular utilizando-se as redes 802.11 instaladas, foi realizado um percurso de 7,4 Km no bairro de Copacabana (Figura 14(a)) num tempo aproximado de 50 minutos. Durante esse percurso, uma varredura das redes 802.11 instaladas na região permitiu estimar o tempo de conectividade conseguido dadas algumas restrições de taxa de transmissão e nível de segurança. O gráfico da Figura 14(b) mostra a parcela do tempo total em que o equipamento permaneceria conectado em função da quantidade de tempo em que permaneceu em contato com algum AP.

Como seria esperado, a Figura 14(b) mostra que quanto maior é o tempo necessário de contato do equipamento móvel com o AP para que seja estabelecida uma associação, menor é o tempo de conectividade. Foram considerados APs com três níveis de potência, equivalendo a três taxas distintas de transmissão (2, 5,5 e 11Mbps), e com o uso ou não de mecanismos de proteção. Podemos observar que, considerando a densidade de redes instaladas nesse percurso, é possível se obter algo próximo a 70% de conectividade ao longo do trajeto quando a taxa mínima de conexão é utilizada e nenhum dos APs possui mecanismos de proteção. Quando uma taxa de conexão maior é necessária e apenas os APs sem criptografia são considerados, essa parcela de tempo pode cair a 10%, sendo que o fator que mais afeta esse tempo de conectividade é a taxa com que se deseja conectar ao AP.

A capacidade mais baixa avaliada (2Mbps) é considerada satisfatória para uma ampla variedade de aplicações como *web* e *e-mail*, mesmo levando em conta a taxa de perda de pacotes em redes 802.11, a qual é tipicamente alta. Como foi visto, é possível que em determinadas situações o usuário tenha acesso à rede por pouco mais que 10% do tempo, o que é inapropriado para a maior parte das aplicações. Por outro lado, vem sendo desenvolvidas novas aplicações torelantes a atrasos como [Seth et al. 2006] ou oportunísticas como [Jiang et al. 2004], as quais conseguem usufruir dos recursos escassos de banda.

No Brasil, ainda são raras as redes 802.11 de acesso público, mas iniciativas como [FON] são comuns nos EUA e Europa. Logo, a aplicação ilustrada e outras semelhantes podem se tornar viáveis quando nossa infra-estrutura estiver mais próxima a dos países desenvolvidos.



(a) Trajetória (b) Conectividade

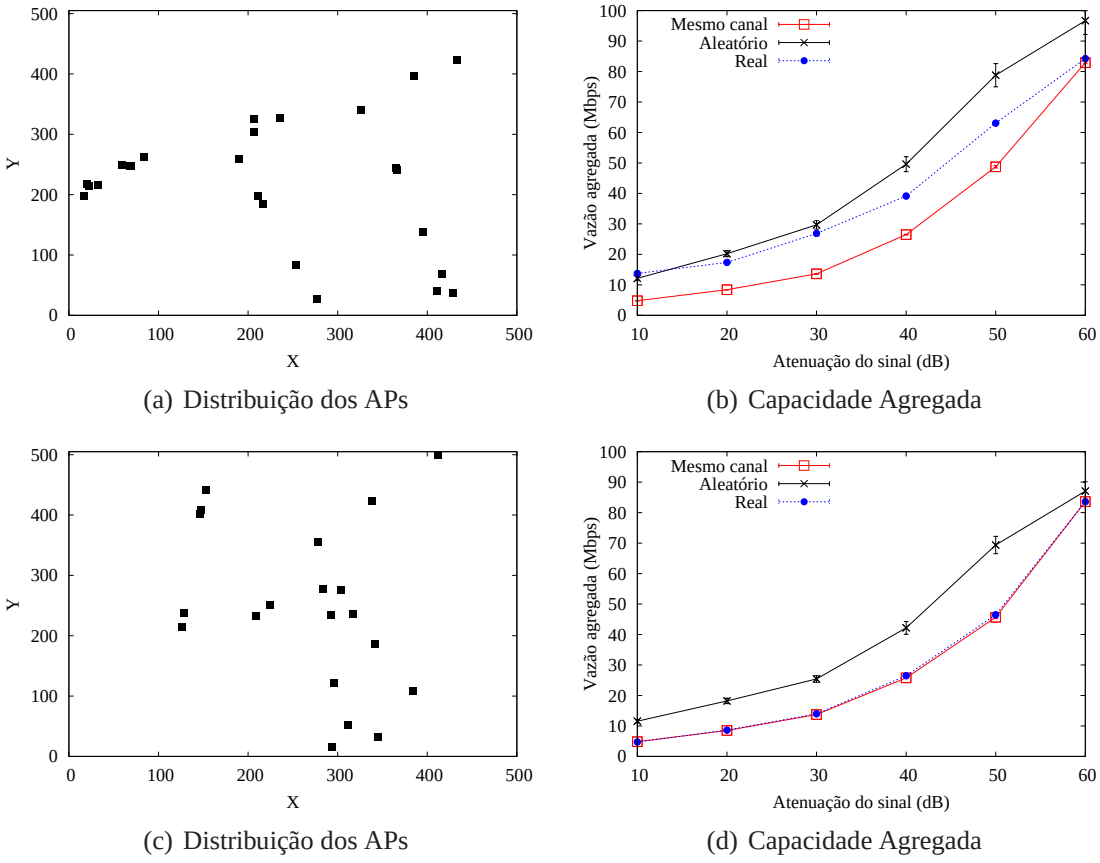
Figura 14. Aplicação Veicular.

Ao se realizar avaliações usando um simulador de rede, um problema comumente encontrado é a descrição da topologia da rede. É desejável que a topologia usada descreva o mais próximo possível o ambiente real que almeja analisar. O posicionamento dos APs controlados por diferentes entidades (ou pessoas) é uma incógnita. Muitas vezes são usados algoritmos de posicionamento aleatório ou que o distribuem os APs de acordo com algumas restrições, mas não há nenhuma garantia que se esteja obtendo um ambiente simulado que represente o real. Dentro desse contexto, é apresentado a seguir mais um uso das informações coletadas.

A partir do conhecimento das posições dos equipamentos, é possível avaliar diferentes mecanismos utilizando-se de topologias mais próximas do caso real ao invés da geração de topologias sintéticas. Um exemplo de aplicação dessas topologias é no estudo do nível de interferência entre APs de uma determinada região. Para exemplificar um estudo desse tipo, a área do *wardriving* foi dividida em áreas menores de 500mX500m. As Figuras 15(a) e 15(c) apresentam dois exemplos dessas áreas com os seus respectivos APs nas posições estimadas pelo algoritmo de centróide ponderado. Os posicionamentos dos APs de ambas as topologias, assim como os seus canais de operação, foram utilizados no simulador ns-2 [Network Simulator (NS)] para avaliar a capacidade agregada dessas redes e compará-la àquelas obtidas com dois outros tipos de alocação: aleatória e no mesmo canal. É considerado que a alocação no mesmo canal, onde a interferência entre os APs é máxima, fornece um limite inferior para a capacidade agregada. Nestes cenários, foi utilizada uma única estação cliente associada a cada AP, realizando um *download* de um arquivo durante toda a simulação. A capacidade agregada corresponde ao somatório das vazões obtidas por todos os fluxos presentes no cenário.

As curvas das Figuras 15(b) e 15(d) apresentam a vazão agregada em função da atenuação do sinal em dB. Essa atenuação leva em conta que os APs estão dispostos em ambientes internos (*indoor*) e, desta forma, o sinal transmitido por um determinado AP deve atravessar paredes e obstáculos antes de atingir os demais. Quanto maior a atenuação, menor a interferência entre os APs. Desta forma, as curvas mostram que a capacidade agregada cresce com a diminuição da interferência. No caso da alocação real, extraída das próprias informações de *wardriving*, a capacidade agregada é superior àquela obtida pela alocação no mesmo canal e inferior a quando os canais de operação são

escolhidos aleatoriamente. Ou seja, se cada usuário resolvesse alterar (aleatoriamente) o canal de seu AP sem saber em qual canal estão os equipamentos de seus vizinhos, haveria uma melhoria global na distribuição dos canais. No entanto, essa não é uma abordagem correta, sendo a proposta apresentada em [da Silva and de Rezende 2007] uma solução mais apropriada.



(a) Distribuição dos APs (b) Capacidade Agregada

(c) Distribuição dos APs (d) Capacidade Agregada

Figura 15. Interferência entre os APs.

5. Conclusões

Neste trabalho foram coletadas informações a respeito das redes 802.11 instaladas em alguns bairros do Rio de Janeiro. Para isso, foi utilizada uma técnica conhecida por *wardriving* que consiste na utilização de computadores equipados com interfaces 802.11, GPS e um software capaz de efetuar uma varredura nos canais utilizados por essas redes. Este artigo fornece e avalia estatísticas sobre as mais de 4 mil redes encontradas. Os resultados estatísticos revelam que a alocação de canais nessas redes é realizada de forma desordenada com uma grande parcela dos APs utilizando o mesmo canal e que uma parcela considerável de usuários, em torno de 35%, não utilizam mecanismos de segurança para proteger suas redes ou sequer trocam o identificador do AP (SSID) padrão usado pelo fabricante. Além disso, diversas análises com relação à estimativa do posicionamento, da densidade dos APs e do grau de vizinhança foram realizadas.

As informações coletadas por técnicas de *wardriving*, mesmo que imprecisas, são valiosas para o entendimento dessas redes e do comportamento dos usuários no uso da tec-

nologia e para o desenvolvimento e avaliação de novos mecanismos. No artigo é exemplificado o uso desses resultados no estudo da viabilidade de aplicações veiculares e o impacto da alocação de canal no desempenho dessas redes.

As informações coletadas servirão como subsídio para trabalhos futuros em simulação e modelagem que lidem com redes 802.11 em modo infra-estruturado e necessitem de dados como posição e canal.

O presente trabalho apresenta algumas possibilidades de extensão que, devido à restrição de recursos, os autores não pretendem realizar. Uma delas é uma cobertura ainda mais abragente da cidade do Rio de Janeiro, com uso de antenas extenas com maior ganho e interfaces de comunicação como maior sensibilidade. Com mais dados e informações mais precisas haveria a possibilidade de definir melhor o cenário das redes 802.11 em um cenário urbano. Outra extensão interessante é a realização de *wardriving* em outros centros urbanos brasileiros e a criação de uma base de dados nacional semelhante a de outros projetos no exterior como [WiGLE.net]. Esses dados ajudariam, por exemplo, a planejar a instalação de redes públicas de acesso ou a implantação de redes comunitárias semelhantes a [FON].

Referências

Bychkovsky, V., Hull, B., Miu, A., Balakrishnan, H., and Madden, S. (2006). A measurement study of vehicular internet access using in situ wi-fi networks. In *Proceedings of the 12th Annual International Conference on Mobile Computing and Networking (MobiCom'06)*, pages 50–61.

Cheng, Y.-C., Chawathe, Y., LaMarca, A., and Krumm, J. (2005). Accuracy characterization for metropolitan-scalewi-fi localization. In *Proceedings of the 3rd international conference on Mobile systems, applications, and services (MobiSys'05)*, pages 233–245.

da Silva, M. W. R. and de Rezende, J. F. (2007). SDCD: Um Novo Mecanismo para a Seleção Automática de Canal em Redes IEEE 802.11 Independentes. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*.

FON. Fon community. `http://www.fon.com`. [Último acesso: 29-Março-2007].

Google. Google maps. `http://maps.google.com`. [Último acesso: 26-Novembro-2006].

Hills, A. and Friday, B. (2004). Radio resource management in wireless LANs. *IEEE Communications Magazine*, 42.

IEEE Registration Authority. IEEE OUI and Company_id Assignments. `http://standards.ieee.org/regauth/oui/oui.txt`. [Último acesso: 18-Dezembro-2006].

Jiang, N., Schmidt, C., Matossian, V., and Parashar, M. (2004). Opportunistic Application Flows in Pervasive Environments. In *IEEE/ACS International Conference on Pervasive Services (ICPS'04)*, pages 219–219.

Kim, M., Fielding, J. J., and Kotz, D. (2006). Risks of using ap locations discovered through war driving. In *Proceedings of the 4th International Conference on Pervasive Computing (PERVASIVE 2006)*, pages 67–82.

Mishra, A., Shrivastava, V., Agrawal, D., Banerjee, S., and Ganguly, S. (2006). Distributed channel management in uncoordinated wireless environments. In *Proceedings of the 12th Annual International Conference on Mobile Computing and Networking (MobiCom'06)*, pages 170–181.

Network Simulator (NS). `http://www.isi.edu/nsnam/`. [Último acesso: 26-Novembro-2006].

Seth, A., Kroeker, D., Zaharia, M., Guo, S., and Keshav, S. (2006). Low-cost Communication for Rural Internet Kiosks Using Mechanical Backhauls. In *Proceedings of the 12th annual international conference on Mobile computing and networking (MobiCom'06)*, pages 334–345.

Wi-Fi-Zones.com. Find more hotspot locations. `http://www.wi-fi-zones.com`. [Último acesso: 22-Novembro-2006].

WiFiMaps.com. Wardriving maps and hotspot locator. `http://www.wifimaps.com`. [Último acesso: 22-Novembro-2006].

WiFinder. `http://www.wifinder.com/`. [Último acesso: 22-Novembro-2006].

WiGLE.net. Wireless geographic logging engine. `http://wigle.net`. [Último acesso: 22-Novembro-2006].