VARREDURA E ANÁLISE DAS REDES WI-FI EM IBIRAMA-SC UTILIZANDO O MÉTODO DO WARDRIVING

William Oliveira, Gedielson Souza, Alexandre Battisti
williamxd3@hotmail.com, gedisouza@hotmail.com, gthardrock@gmail.com

Resumo
Redes sem fio Wi-Fi vem ganhando cada vez mais espaço sobre as redes comums cabeadas devido a sua mobilidade e flexibilidade. Para investigar esta tendência, este presente artigo descreve um estudo da utilização de redes sem fio na cidade de Ibirama-SC, analizando e esquematizando dados como: os padrões de segurança, disposição de canais e padrões de radio utilizados, marcas de aparelhos de Pontos de Acesso Wi-Fi mais utilizados, dentre outros. Este trabalho apresenta o uso de *wardriving* como metodologia para mapear o uso de redes sem fio em uma dada região.
Palavras-chave: Redes sem fio. Wi-Fi. *Wardriving*.

1. Introdução

Até certo tempo, só era possível conectar-se a internet através de cabos, tipo de conexão de ótima qualidade, porém com certas limitações quanto a sua mobilidade e flexibilidade. Para amenizar estes problemas surgiram então as redes sem fio Wi-Fi tornando mais prática a conexão com a internet.

Uma característica das redes sem fio Wi-Fi é facilidade de suas ondas eletromagnéticas atravessarem edifícios e obstáculos podendo percorrer grandes distâncias. Utilizando desta facilidade na captura do sinal Wi-Fi surgiu a técnica do *wardriving*, que consiste no ato de mover-se por determinada região rastreando sinais *wireless* através de um computador ou aparelho com um software especifico a pratica.

Fazendo uso desta técnica fez-se uma varredura em uma determinada região da cidade de Ibirama-SC, no dia 3 de novembro de 2013, onde foi colocado uma série de dados a respeito as redes sem fio Wi-Fi de modo a analisa-los e estudá-los.

2. Redes Wi-Fi

As redes Wi-Fi são redes sem fio em conformidade com os padrões 802.11 do IEEE (*Institute of Electricaland Electronics Engineers*). Redes Wi-Fi são categorizadas como WLANs (*Wireless Local Areas Networks*), são redes sem fio de cobertura local de cerca de 20 metros. (TELECO, 2012)

A comunicação wireless é realizada por meio da tecnologia *Spread Spectrum* (Espectro espalhado) este método consistem em dividir a faixa de frequência em várias faixas menores, onde então os dados são transmitido em diversos pedaços e então juntados quando recebidos. O Wi-Fi usa 3 métodos para gerar o *Spread Spectrum*, são eles: DSSS (*Direct Sequence Spread Spectrum*), Utiliza 11 canais com largura de 22Mhz cada, dentro da banda de 2.4Ghz, possibilitando várias redes no mesmo local sem que elas interfiram entre si; FHSS (*Frequency Hopping Spread Spectrum*), utiliza 79 canais de 1Mhz de largura cada onde o transmissor e o receptor saltam por estes canais conforme uma sequência pseudoaleatória conhecida por ambos; OFDM (*Orthogonal Frequency Division Mutiplexing*), faz uso de 52 canais de frequência, sendo 48 delas pra envio de dados e 4 para sincronização, seu diferencia é poder enviar vários dados

paralelamente, sendo assim podendo transmitir uma maior quantidade de dados por segundo. (GALLO; HANCOCK, 2002)

Dentro da família de protocolos IEEE 802.11 as principais são: IEEE 802.11a, utiliza modulação OFDM para geração do sinal, trabalha na frequência 5Ghz com uma taxa de transferência máxima de 54 Mbps; IEEE 802.11b, utiliza da modulação DSSS, opera na frequência 2.4Ghz e possui uma taxa de transferência máxima de 11 Mbps; IEEE 802.11g, faz uso de OFDM ou DSSS para geração o *Spread Spectrum*, opera no intervalo de frequência 2.4Ghz com capacidade de transmissão máxima de 54 Mbps; IEEE 802.11n, o mais evoluído atualmente, usa modulação DSSS ou OFDM para a transmissão, pode operar em 2.4Ghz ou 5Ghz e com taxas de transmissão de até 600Mbps. (TELECO, 2012)

As redes Wi-Fi podem operar em dois modos: *Ad-Hoc*, onde vários dispositivos próximos se comunicam entre si sem necessidade de um termina central ou ponto de acesso ou Infra estruturado, que utiliza um equipamento gerenciador para a distribuição o sinal, conhecido como *Access Point* ou Ponto de acesso. (GALLO; HANCOCK, 2002)

Diferente das redes cabeadas as redes sem fio não possuem as proteções físicas, necessitando então de outros meios de segurança, os mais usados atualmente são: WEP (*Wired Equivalent Privacy*), criado em 1999, compatível com praticamente todos os dispositivos Wi-Fi, muito vulnerável por contar com um sistema de segurança baseado em apenas 40bits, fator que restringe a quantidade de caracteres da senha; WPA (*Wi-Fi Protected Access*), adotado em 2003 com uma encriptação de 265bits, ainda não totalmente seguro por contar ainda com algumas vulnerabilidades remanescentes do WEP; WPA2 (*Wi-Fi Protected Access II*), o protocolo mais atual e seguro, introduzido em 2006, praticamente invulnerável por utilizar os padrões de criptografias AES (*Advanced Encryption Standard*) e o CCMP (*Counter Sipher Mode*). (GALLO; HANCOCK, 2002)

3. Metodologia

Para coleta das informações utilizou-se de uma abordagem seguindo padrões de Gil(2007) de pesquisa quantitativa (onde os dados podem ser expressados em números) exploratória (de modo a investigar um fenômeno) através de um estudo de caso onde fez-se uso da técnica do *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." (VILELA; CARDOSO; REZENDE, 2006, p.1).

Os equipamentos usados foram um automóvel e um notebook "Acer Aspire 5733", com interface Wi-Fi integrada. Em termos de software foi utilizados o Vistumbler[1], ferramenta utilizada para mapeamento e identificação de redes sem fio, para a varredura dos sinais de redes sem fio da região de coleta para a obtenção geral dos dados.

Devido a inviabilidade da varredura ser feita na cidade inteira, utilizou-se então de uma amostra, o trajeto de amostragem iniciou-se na Rua Mq. Do Herval, próximo a ponte Castro Alves, até o Centro da cidade onde então retornou pelo outro lado da cidade através da Rua Getúlio Vargas e Rua Guarany chegando finalmente ao CEAVI. O trajeto todo teve a distância de 18Km e foi percorrido em cerca de 30 minutos a uma velocidade média de 50km/h, não houve necessidade de uma velocidade mais baixa já que o software é capaz de detectar os sinais muito rapidamente. A varredura foi feita no dia 3 de novembro de 2013 as 14horas.

4. Análise e discussão dos dados

Foram encontrados 399 redes Wi-Fi na varredura utilizando o método do *wardrivng*, no percurso

[1]Disponível em: http://vistumbler.com

de amostra na cidade de Ibirama-SC, na data de 3 de novembro de 2013. A partir do dados coletados foi então quantificados e analisados: modos de operação (*Ad-hoc* ou infra estrutura), principais canais, padrões de rádios, protocolos de segurança e marca de aparelhos de ponto de acesso.

4.1 Análise dos Modos de Operação

As redes sem fio residenciais e comerciais são em sua maioria no modo estruturado, servindo como uma última milha sem fio, para um provedor cabeado. Entretanto, pode-se encontrar eventualmente redes operando em malha ou ponte sem fio, que estejam operando em modo *Ad-Hoc*. Das 399 redes encontradas na coleta, 99% (394 redes) operavam em modo Ad-hoc, enquanto apenas 1% (5) operavam em modo Infra Estrutura.

4.2 Análise da utilização de canais

Outro dado capturado foram os canais utilizados pelos pontos de acessos. O padrão IEE 802.11 define 11 canais de 22MHz dentro da banda 2.4Ghz, considerando esta largura de canais o número de pontos de acesso ativos simultaneamente em um mesmo ambiente sem interferências é 3. O gráfico da Figura 1 abaixo mostra de uso dos canais de rede sem fio, nota-se que a grande maioria está dividida entre os canais 1, 6 e 11 o motivo disse deve-se ao fato desses canais serem configurados como padrão pelas fabricantes de aparelhos de Ponto de Acesso.

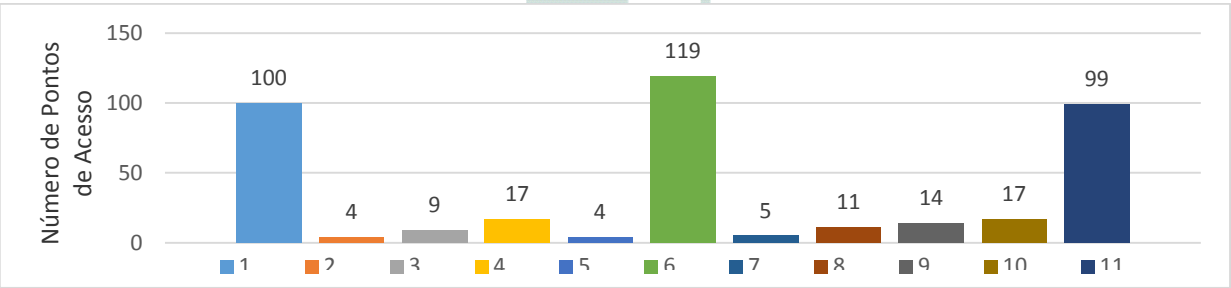

Figura 1 - Gráfico dos canais Wi-Fi (Originado dos dados coletados na varredura)

4.3 Análise dos padrões de rádios utilizados

Na varredura outra informação retida foram os padrões de rádios de rede sem fio, na Figura 10 é possível notar que o padrão IEEE 802.11n é o mais utilizado somando mais da metade dos pontos de acesso encontrados (53,5%), seguido do padrão IEEE 802.11g utilizado em 33,3% das amostras e por fim o padrão IEEE 802.11b contabilizando 12,7% das redes.

Nota-se, portanto, que a maioria dos Pontos de Acessos faz uso do padrão de transmissão Wi-Fi mais evoluído do mercado segundo Teleco(2012).

4.4 Análise dos tipos de Protocolos de segurança

Neste item analisamos os protocolos de segurança utilizados, nota-se uma preferência pelo uso do protocolo WPA2, somando uma parcela de 66,4% das amostras capturadas, os protocolos WPA e WEP contabilizam respectivamente 10,7% e 15,2% e as rede abertas (sem criptografia) somaram 6,7%.

4.5 Análise das marcas

Outro dado adquirido na varredura foram as marcas dos aparelhos de Ponto de Acesso Wi-Fi. Foi constatado que a marca mais utilizada é a TP-Link com uma parcela de 34%, seguido da

marca D-Link com 22%, fato que diverge a nível mundial onde a marca de aparelhos de transmissão Wi-Fi mais utilizada é a Cisco de acordo com o site de registro de informações sobre redes sem fio, WIGLE.net.

5. Conclusão

No presente artigo foi descrito o atual cenário das redes sem fio Wi-Fi na cidade de Ibirama, onde utilizamos da técnica o *wardriving*, para colocar as informações, na varredura foram capturadas 399 redes sem fio Wi-Fi num percurso de 20km.

Analisado os dados coletados foi notado que a quase todas (99%) das redes sem fio da região analisada faz uso do modo de operação Infraestrutura, fato que reflete a fácil aquisição dos aparelhos de Ponto de Acesso Wi-Fi, que vem se tornando cada vez mais baratos e acessíveis.

Foi observado que a maior parte dos canais de rede sem fio Wi-Fi estão divididos entre os canais 1,6 e 11, devido, muito provavelmente, por serem configuração padrão atribuídos pelos fabricantes do aparelho de Ponto de Acesso.

Outro fato positivo analisado foi em relação à segurança, foi visto que o protocolo com maior utilização foi o WPA2, o mais seguro no presente momento, no entanto uma parcela considerável (15%) ainda faz uso do protocolo WEP, sendo o mesmo ineficiente para garantir a privacidade dos dados que trafegam na rede.

Também foi notado que a marca de aparelho de Ponto de Acesso mais utilizado é a TP-Link com uma parcela de 34%, seguido da marca D-Link com 22%, fato que diverge a nível mundial onde a marca de Access Point mais usada é a Cisco.

Para trabalhos futuros, recomendamos a utilização de antenas mais potentes acopladas ao computador para uma maior área de captação de sinais Wi-Fi.

Referências

GALLO, Michael A.; HANCOCK, William M.. **Comunicação entre Computadores e Tecnologias de Rede.** São Paulo: Thomson Learning LTDA, 2002. 673 p.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 5.ed. São Paulo: Atlas, 2007.

LINHARES, André Guedes; GONÇAVELS, Paulo André da S. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11**. Universidade Federal de Pernambuco (UFPE), Recife – PE. 2006.

TANEMBAUM, Andrew S. **Redes de computadores - Quarta edição**. Amsterdam: Vrije Universiteit, 2003. Disponível em: http://www-usr.inf.ufsm.br/~rose/Tanenbaum.pdf. Acesso em: 2 de novembro de 2013.

TELECO, **Redes de Dados Wireless**. Disponível em: http://www.teleco.com.br/tutoriais/tutorialwifiiee/default.asp. Acesso em: 01 de dezembro de 2012.

VILELA, Ulysses Cardoso; CARDOSO, Kleber Vieira Cardoso; REZENDE Jose Ferreira de Rezende. **Redes 802.11 em Centros Urbanos: Varredura, Estatísticas e Aplicações**. GTA - PEE - COPPE – Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro – RJ.