Segurança em Redes Wireless

Fabrício R. A. Souza[1], Cristiano Maciel da Silva[2], Cayley Guimarães[3]
[1]Bacharel em Ciência da Computação pelo UNI-BH, [2]Mestre em Ciência da Computação pela UFMG, [3]Mestre em Ciência da Computação pela Virginia Tech.

Resumo – Este artigo tem como objetivo apresentar as redes sem fio, suas principais tecnologias e os padrões atualmente em uso. O texto contempla a rede, a segurança aplicada e uma análise sobre o uso popularizado dessa técnica de transmissão de dados. Realizou-se uma pesquisa de campo, em um dos grandes eixos comerciais da cidade de Belo Horizonte, com o objetivo de verificar quais os tipos de rede utilizados e os níveis de segurança apresentados. Foi verificado que a maioria das redes mapeadas é vulnerável a ataques sérios que podem prejudicar os usuários que não tem conhecimento pleno desse tipo de tecnologia.

palavras-chave – redes sem fio, segurança

Abstract – This article presents the main aspects of wireless networks security. A major economic section of the city of Belo Horizonte was researched, in order to determine the types of networs used and its security levels. It was found that most of the mapped network is vulnerable to serious attacks that may harm users who do not have full knowledge of such technology.

keywords – wireless networks, security

I. INTRODUÇÃO

As redes sem fio têm se popularizado principalmente pela mobilidade e praticidade oferecida aos seus usuários. Atualmente, tem-se observado um considerável aumento na quantidade de dispositivos portáteis com este tipo de suporte. Além disto, diversos estabelecimentos oferecem, hoje em dia, acesso à *Internet* a partir de seus dispositivos móveis como um requisito de negócio. Tanto em ambientes públicos, quanto em ambientes privados, estas redes estão cada vez mais difundidas, complementando as tradicionais áreas de redes locais (LANs[1]) [19].

A primeira rede sem fio foi criada em 1970, com o objetivo de conectar quatro ilhas na qual situavam os *campi* da universidade do Havaí. Mais tarde, na década de 80, as redes sem fio são inseridas na computação pessoal [21].

Inicialmente, as redes sem fio utilizavam transceptores infravermelhos ao invés de ondas de rádio, o que fazia com que os serviços fossem de baixa qualidade e confiabilidade (quedas constantes, interferências, etc.). As redes sem fio com tecnologia de ondas de rádio tiveram destaque no início da década de 90, quando os processadores evoluíram o suficiente para gerenciar os dados enviados e recebidos nesta tecnologia [1].

Em 1999, o Instituto de Engenharia Elétrica e Eletrônica (IEEE[2]) consolidou o padrão 802.11b. Já em 2002 o padrão 802.11a foi ratificado, superando o 802.11b em velocidade. Porém, devido à utilização da sua frequência de 5 GigaHertz (GHz)[3], o 802.11a não é compatível com demais dispositivos 802.11b utilizados, o que diminui significativamente a sua aceitação. Entretanto, no final de 2002 surge o 802.11g, completamente compatível com o 802.11b e com a mesma velocidade do 802.11a [16].

Engst & Fleischman (2005) teorizam que

> "*As redes wireless seguem as mesmas características de todos os dispositivos sem fio. Um transceptor envia sinais através de ondas de radiação eletromagnética, que se propagam a partir de uma antena que recebe estes sinais propagados nas freqüências corretas*" [1].

[1] *Local Area Network*

[2] *Institute of Eletrical and Electronics Engineers*

[3] *Hertz - Freqüência de um fenômeno periódico cujo período é de 1 segundo* [16]

Para as redes sem fio, temos como principal desvantagem, a segurança precária, o que torna possível a leitura maliciosa de informações trafegadas na rede, por exemplo [2].

Para superar os problemas de segurança, as organizações devem determinar processos específicos e bem definidos para o uso de dispositivos sem fio, desde as funções na qual ele será usado, o que será armazenado nesses dispositivos e qual a segurança aplicada a eles para evitar que os dados sejam comprometidos em uma situação de exceção. Desta forma, políticas e padrões são fundamentais, pois uma rede sem fio deve operar sobre o preceito de que existem nodos maliciosos dispostos a obter e manipular dados indevidos. [17, 21]

Uma rede sem fio operacional deve garantir a autenticidade do usuário, confiabilidade da transmissão, integridade dos dados e disponibilidade da rede [2]. Este artigo faz, primeiramente, uma revisão dos principais conceitos de redes sem fio. Em seguida, apresenta resultados de uma pesquisa de campo realizado em um dos principais eixos comerciais de Belo Horizonte, com o objetivo de determinar os tipos de redes usados e os níveis de segurança destas redes.

Desde o lançamento e a popularização das redes sem fio, os interessados nesse tipo de tecnologia têm feito uso indiscriminado, e pouco informado sobre a configuração de segurança. Além de desconhecimento e falta de treinamento, os dispositivos não forneciam aos usuários formas de auxílio na configuração da segurança da rede. Atualmente, os assistentes estão muito mais atentos à segurança, relacionando e instruindo os usuários iniciantes na melhor forma de fechar e criptografar a sua rede.

II. REDES

As redes sem fio, denominadas 801.11, necessitam de determinados componentes para sua adequada operação. A característica que se destaca neste tipo de rede é a utilização de ondas de rádio para a transmissão entre as estações, em que a presença de vários tipos de equipamentos permitem o acesso a estas redes, como placas de Interconexão de Componentes Periféricos (PCI[4]) (internas), placas de Barramento Serial Universal (USB[5]) (externas) e adaptadores de placas *ethernet*[6] [17].

Dos principais padrões de redes sem fio, se destacam a Interoperabilidade Mundial para Acesso por Microondas (*WiMax*[7]), *Bluetooth*, *Wi-Fi* e InfraVermelho (*InfraRed*)[17].

Tanto o *WiMax* como o *Bluetooth* são utilizados para comunicação entre pequenos dispositivos de uso pessoal. No *WiMax* as transmissões de dados podem alacançar 70 MegaBits por segundo (Mbps[8]) a uma distância de até 50 km - radial. O *Wimax* trabalha na faixa de frequência definida pela Indústria Científica e de Medicina (ISM[9]) centrada em 2,45 GHz[21].

A tecnologia *Bluetooth* é um padrão para comunicação sem-fio de baixo custo e curto alcance que permite a conexão de vários tipos de dispositivos de comunicação para a troca de dados, como os celulares, por exemplo. Da mesma forma que o *WiMax*, os dispositivos *Bluetooth* trabalham numa freqüência da faixa ISM, em 2,45 GHz. A comunicação entre esses dispositivos é feita através de um canal de Modulação de Freqüência-Acesso Múltiplo por Divisão de Código (FH-CDMA[10]). A comunicação se dá com o transmissor enviando um sinal sobre uma série randômica de freqüências de rádio. Logo após, um receptor identifica o sinal através de sincronismo com o transmissor. A mensagem somente é recebida se

---

[4] *Peripheral Component Interconnect*
[5] *Universal Serial Bus*
[6] *Tecnologia de interconexão para redes locais*
[7] *Worldwide Interoperability for Microwave Access*
[8] *Megabits per second*
[9] *Industrial Scientific and Medical*
[10] *Frequency Hopping - Code-Division Multiple Access*

o receptor conhecer a série de freqüências na qual o transmissor trabalhou para enviar o sinal [5, 21].

O *Wi-Fi* opera em faixas de freqüências que não necessitam de licença para instalação e/ou operação. Porém, para que seja utilizado comercialmente no Brasil é necessária licença da Agência Nacional de Telecomunicações (Anatel). O adaptador infravermelho é um padrão de comunicação sem fio para transmissão de dados. Ele não possui memória interna e, portanto, não armazena os dados; opera na transferência de um equipamento para outro, servindo apenas como uma ponte. Atualmente são disponíveis em dois padrões: 1.0 com taxas de transmissão de até 115.200 bps e 1.1 com taxas de transmissão de até 4 Mbps [21].

Da mesma forma que as redes cabeadas, as redes sem fio são classificadas como: Redes Locais (WLAN[11]), redes metropolitanas (WMAN[12]), redes de longa distância (WWAN[13]) e redes pessoais (WPAN[14]) [19].

Uma rede local sem fio (WLAN) se dá com base em um conjunto de padrões definidos pelo IEEE, representados da seguinte forma:

IEEE 802.11a é o padrão que especifica a camada de enlace e física para redes sem fio que operam na freqüência de 5 GHz. Apesar de ter sido confirmado em 1999, não existem muitos dispositivos que atuam nesta freqüência. [17]

IEEE 802.11b descreve a implementação dos produtos WLAN mais comuns em uso atualmente, incluindo aspectos da implementação do sistema de rádio e também de segurança através do protocolo WEP[15]. Sua operação é baseada na ISM, sem necessidade de licença para utilização, na freqüência de 2.4GHz e 11 Mbps. Aprovado em julho de 2003 pelo IEEE permite o número de 32 clientes conectados [17].

IEEE 802.11g atua na frequência ISM de 2.4 GHz e provê taxas de transferências de até 54 Mbps. É compatível com o padrão 802.11b, permitindo que trabalhem no mesmo ambiente [17].

IEEE 802.11i trata-se um grupo de trabalho que está ativamente definindo uma nova arquitetura de segurança para WLANs de forma a cobrir as gerações de soluções WLAN, tais como a 802.11a e 802.11g. Define mecanismos de autenticação e privacidade e várias de suas características podem ser implementadas nos protocolos existentes. O padrão inclui o protocolo *Wi-Fi* de Acesso Protegido (WPA[16]) que foi desenvolvido para oferecer soluções com maior segurança [17].

IEEE 802.11e fornece melhoramentos ao protocolo 802.11, sendo também compatível com o 802.11b e 802.11a. Os avanços incluem a capacidade multimídia, sendo possível com a adesão da funcionalidade de qualidade de serviços (QoS[17]), como também atualização em aspectos de segurança. Isto significa a habilidade de oferecer vídeo e áudio sob demanda, serviços de acesso de alta velocidade à *Internet* e Voz sobre IP - VoIP[18]. QoS é a chave da funcionalidade do 802.11e. Ele fornece a funcionalidade necessária para acomodar aplicações sensíveis a tempo com vídeo e áudio [17].

Os grupos do IEEE que estão desenvolvendo outros protocolos são:

[11] *Wireless Local Area Network*
[12] *Wireless Metropolitan Area Network*
[13] *Wireless Wide Area Network*
[14] *Wireless Personal Area Network*
[15] *Wired Equivalency Privacy*
[16] *Wi-fi Protected Access*
[17] *Quality of Service*
[18] *Voicer Over Internet Protocol*

Grupo 802.11d – Está concentrado no desenvolvimento de equipamentos para definir 802.11 WLAN para funcionar em mercados não suportados pelo protocolo corrente - O corrente protocolo 802.11 só define operações WLAN em alguns países [17].

Grupo 802.11f – Desenvolve o Protocolo de acesso entre pontos (*Inter-Access Point Protocol*), pela corrente limitação de migração (*roaming*) entre pontos de acesso de diferentes fabricantes. Este protocolo permitirá que dispositivos sem fios passem por vários pontos de acesso de diferentes fabricantes [17].

Grupo 802.11h – Em desenvolvimento do espectro e gestão das extensões de potência para 802.11a do IEEE para utilização na Europa com uma frequência de 5 GHz [17].

IEEE 802.11n – descreve o mais recente padrão para redes sem fio. Conhecido também como Espectro de Eficiência Mundial (WwiSE[19]), seu principal objetivo é alcançar maiores velocidades de transmissão, aproximadamente de 100 a 500 Mbps [17].

A topologia de uma rede IEEE 802.11 é completa pelos seguintes elementos:

O **Conjunto de Serviços Básicos** (BSS ou *Basic Service Set*) corresponde a uma célula de comunicação sem fio [17].

As **Estações** (STA ou *Stations*) são as estações de trabalho que se comunica entre si dentro do Conjunto de Serviços Básicos [17].

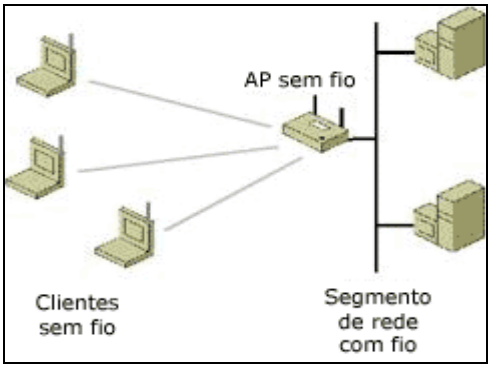
O **Ponto de Acesso** (AP ou *Access Point*) funciona como uma ponte entre a rede sem fio e a rede tradicional. Ele coordena a comunicação entre as Estações dentro do Conjunto de Serviços Básicos. Existem Pontos de Acesso que também atuam como roteadores, possibilitando o compartilhamento de *Internet* pelos outros usuários da rede e servidores com Protocolo com Configuração de Host Dinâmico (DHCP[20]), oferecendo a obtenção de um endereço IP na rede [17].

Ponte (*Bridge*) faz a ligação entre diferentes redes.

O **Conjunto Extendido de Serviços** (ESS ou *Extended Service Set)* consiste de várias células do Conjunto Básico de Serviços vizinhas entre si, cujos Pontos de Acesso encontram-se conectados em uma mesma rede tradicional. Nestas condições, uma Estação pode se movimentar de um Conjunto de Serviços Básicos para outro permanecendo conectada à rede, processo denominado de Migração (*Roaming)* [17].

São previstos dois modos de operação: (a) No modo Infraestruturado (vide Figura 1) existe a presença de um Ponto de Acesso coordenando a comunicação entre as estações de uma célula de Conjunto Básico de Serviços. (b) No modo onde todos os terminais funcionam como roteadores (*Ad-Hoc*) (vide Figura 2) as estações se comunicam diretamente entre si.

Figura 1: Rede sem fio no modo de infra-estrutura

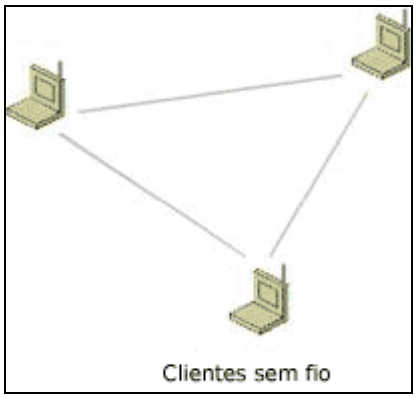


Fonte: Microsoft Brasil (2005)

[19] *World Wide Spectrum Efficiency*

[20] *Dynamic Host Configuration Protocol*

Figura 2: Rede sem fio no modo *Ad-Hoc*



Fonte: Microsoft Brasil (2005)

III. A SEGURANÇA

A proteção dos dados trafegados na rede pode ser realizada com base em diversas estrategias, destacando-se a criptografia, que permite que os dados trafeguem fora de uma ordem lógica e compreensível.

Computacionalmente, a criptografia garante:

- Sigilo: apenas os usuários autorizados e autenticados têm acesso a informação;
- Integridade: garante para o usuário que a informação está correta e sem interferência externa;
- Autenticação: é a forma que o sistema garante a identidade do usuário ou dispositivo com quem se comunica [17, 18].

Ao mesmo tempo em que as WLANs proporcionam flexibilidade, elas também representam riscos à segurança. Qualquer computador que possua um adaptador compatível (estando a uma distância adequada do transmissor) consegue detectar e capturar todos os dados enviados para o Ponto de Acesso. A melhora da segurança pode ser obtida através de configuração e técnicas aplicadas a essas redes [21].

Uma rede é compreendida como vulnerável ou deficiente quando acessos mal intencionados conseguem sucesso ao tentar invadir, alterar ou excluir informações confidenciais e, até mesmo, inutilizar o sistema [21].

As redes sem fio oferecem várias formas de proteção, exigindo domínio técnico para sua instalação e configuração, com o objetivo de minimizar os riscos de invasões. Como exemplo, o posicionamento físico dos equipamentos na rede determina um melhor desempenho do sistema, diminuindo a probabilidade de acessos não autorizados e demais tipos de ataque. Durante sua configuração e disposição dos equipamentos, devem ser observados os padrões em uso e a potência dos equipamentos.

A maioria dos concentradores possibilita a seleção de valores intermediários de alcance, o que facilita encontrar um ponto de configuração mais precisa. Ainda assim, usuários mal intencionados com uma interface mais potente, podem interceptar um sinal que não estava previsto pelo implementador. De forma geral, quanto mais centralizado estiver o concentrador, melhor será o sinal às estações que o recepcionam [21].

Para aprimorar a segurança das redes sem fio foram propostos alguns protocolos que serão apresentados a seguir.

O algoritmo de criptografia Privacidade Equivalente (WEP[21]) é parte do padrão IEEE 802.11 - ratificado em Setembro de 1999 e se utilizava para proteger redes sem fios do tipo, *Wi-Fi*. Este algoritmo opera na camada de enlace e utiliza o método criptográfico Roteamento Coloniale 4 (RC4[22]) da Empresa RSA Data Security, Inc [16].

Trata-se de um Algoritmo para Criptografia de Chave Pública que usa um vetor

[21] *Wired Equivalent Privacy*
[22] *Route Coloniale 4*

de inicialização (IV) de 24 bits e uma chave secreta compartilhada (*secret shared key*) de 40 ou 104 bits. O IV é concatenado à *secret shared key* e forma uma chave de 64 ou 128 bits, que é utilizado para criptografar as informações [16].

O WEP também utiliza o Ciclo de Checagem de Redundância (CRC-32[23]) para calcular a Soma de Verificação (checksum) da mensagem que é inclusa no pacote, o que garante a integridade dos dados. Então, o receptor recalcula o checksum para garantir que a mensagem não foi alterada. Provê recursos de criptografia de 128 bits integrados com os equipamentos da rede 802.11. As chaves criptográficas são simétricas, porém não são gerenciáveis e podem ser descobertas por usuários mal-intencionados. Como prevenção a esta situação, existe um mecanismo que permite que estas chaves sejam atualizadas em intervalos regulares, dificultando seu processo de quebra [16].

A principal desvantagem do WEP é possibilitar que um atacante que deseja ter acesso à rede possa, por meio de escuta, obter a chave, tornando possível a desencriptação dos dados da rede. Outra desvantagem observada é que a chave deve ser conhecida por todos que acessam a rede, o que pode facilitar a distribuição não autorizada da chave [12, 13].

Apesar da suas vulnerabilidades, o WEP é uma camada adicional na segurança da rede sem fio. Para corrigir as falhas no WEP, foi criado outro protocolo de criptografia mais robusto, o WPA [12, 13].

O *Wi-Fi* de Acesso Protegido (WPA[24]) é um subconjunto do padrão de segurança 802.11i baseado no 802.11. A Wi-Fi Alliance, em parceria com o IEEE, criou o protocolo WPA para fornecer um tratamento mais seguro e ao mesmo tempo compatível com o hardware utilizado pelo WEP. Desta forma, a atualização do *firmware* dos dispositivos *wi-fi* que utilizam o WEP pode ser migrada para WPA sem mudanças em sua arquitetura [21].

O WPA possui formas de autenticação, privacidade e controle de integridade das informações mais sofisticada que o WEP. Porém, no WPA, ao contrário do WEP, inexiste suporte para conexões Ad-Hoc[12, 13].

O WPA é implementado para atender a substituição do WEP, cifrando as informações e garantindo a privacidade do tráfego, e autenticar o usuário via padrões 802.1x e Protocolo de Autenticação Extensiva (EAP[25]) [10].

Para cifrar os dados, o WPA utiliza duas técnicas. A primeira é direcionada para pequenas redes através de uma chave previamente compartilhada (*pré-shared key* ou WPA-PSK), que é responsável por reconhecer o dispositivo pelo concentrador. A outra técnica utiliza um Servidor de Autenticação Remota (RADIUS[26]). O sistema de compartilhamento da chave é semelhante ao WEP, cuja troca das chaves é feita manualmente, o que caracteriza sua melhor indicação para redes de pequeno porte, onde os dispositivos estão acessíveis na maior parte do tempo [9, 10].

Junto com as novas implementações do WPA, está o Protocolo de Integridade de Chave Temporária (TKIP[27]), que faz as trocas dinâmicas das chaves. Já no WEP as chaves eram estáticas e seu IV era de 24 bits, passando para 48 bits. Este protocolo utiliza chave base de 128 bits chamada de Chave Temporária (TK[28]).

[23] *Cyclic Redundancy Check-32*
[24] *Wi-Fi Protected Access*
[25] *Extensible Authentication Protocol*
[26] *Remote Authentication Dial-In User Server*
[27] *Temporal Key Integrity Protocol*
[28] *Temporary Key*

Esta chave, em conjunto o endereço do Controle de Acesso de Mídia (MAC[29]) do transmissor, forma outra chave chamada Chave de Endereço Temporária e Transmissão (TTAK[30]), conhecida como "Chave da 1ª fase" [21].

A TTAK combinada com o IV do RC4, cria chaves diferenciadas para cada pacote do tráfego. Com isso, o TKIP espera que cada dispositivo da rede tenha uma chave diferente para se comunicar com o ponto de aceso, uma vez que essa chave é gerada de acordo com o endereço MAC das estações. Inclusive, pode ser programado para alterar o IV a cada pacote trafegado na rede, por sessão ou período, o que torna a captura mais difícil da transmissão [9, 10, 21].

O EAP é um modelo para autenticação também definido no WPA, que utiliza o padrão 802.1x e possibilita inúmeras formas de autenticação, inclusive certificação digital. Este padrão pode trabalhar em conjunto com outras tecnologias, como o servidor de autenticação RADIUS [8].

O 802.1x utilizam o protocolo EAP para gerenciar a forma como a autenticação mútua será feita na rede. Ele possibilita a escolha de um método específico de autenticação a ser utilizado como senhas, certificado digital ou tokens de autenticação. O autenticador não precisa entender o método de autenticação, ele simplesmente transmite os pacotes EAP do usuário a ser autenticado para o servidor de autenticação e vice-versa.

Os Pontos de Acesso 802.1X sem fio podem ser configurados como clientes RADIUS para que possam ser enviadas solicitações de contas e acesso para os servidores RADIUS que executam o Servidor de Autenticação Interna (IAS[31]).

O IAS controla a autenticação dos usuários e dispositivos à rede por meio de diretivas de acesso remoto centralizado. São vários os tipos de EAP que suportam os diversos métodos de autenticação:

• EAP-LEAP[32] (Cisco de pouco peso - EAP): Elaborado pela CISCO Systems– Fabricante de dispositivos de rede, usa o conhecido método de usuário e senha para enviar a identidade do usuário à ser autenticado no servidor;

• EAP-TLS[33] (Camada de Segurança de Transporte): Utiliza o certificado X.509 que é o padrão que especifica os certificados digitais para autenticação. Foi especificado no padrão de especificação para *Internet* RFC[34] 2716;

• PEAP[35] (EAP Protegido): Mais popularizado pela Microsoft nos sistemas operacionais Windows XP e Server 2003, oferece autenticação baseada em senha e exige que o servidor de autenticação possua um certificado digital, porém não exige certificados nos clientes [7, 8, 9, 10].

Entre o WPA e o WPA2, a principal diferença está no método criptográfico. O WPA utiliza o TKIP com RC4, enquanto o WPA2 utiliza Norma de Encriptação Avançada (AES[36]) em conjunto com o TKIP e chave de 256 bits, que é um método de criptografia mais seguro. O AES permite chaves de 128, 192 e 256 bits, tendo então uma ferramenta criptográfica muito mais poderosa. Já no WPA2, a chave de 256 bits é padrão. Com o AES no mercado, houve uma necessidade de computadores com hardware

[29] *Media Access Control*
[30] *Temporal and Transmitter Address Key*
[31] *Internal Authentication Server*
[32] *LightWeight – EAP*
[33] *Transport Layer Security*
[34] *Request for Comments*
[35] *Protected EAP*
[36] *Advanced Encryption Standard*

mais evoluído, capazes de realizar o processamento criptográfico. Os dispositivos WPA2 são integrados por um co-processador para realizar os cálculos da criptografia AES [7, 8, 9, 10].

IV. METODOLOGIA

Esse Estudo de Caso foi realizado em um trecho de grande concentração de comércio da cidade de Belo Horizonte - MG, no intuito de demonstrar a forma como essas redes têm sido utilizadas.

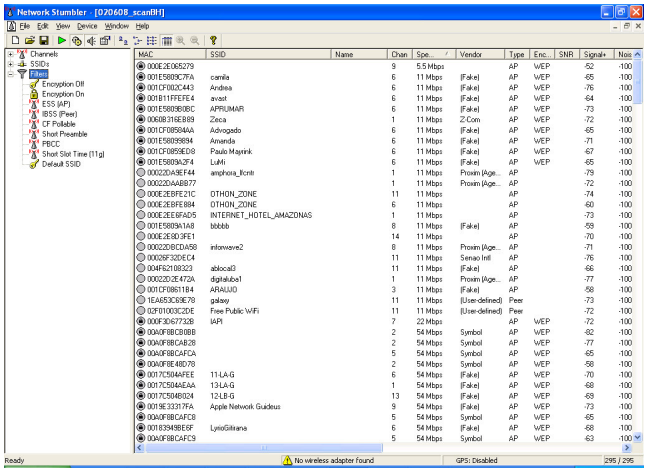
Foi feita uma coleta de campo na cidade de Belo Horizonte, na Avenida Afonso Pena, em toda a sua extensão. A Avenida Afonso Pena é considerada uma das mais importantes de Belo Horizonte, além de ser o coração econômico e um dos referenciais urbanos belo-horizontinos, com 4,3Km[20]. Foram capturadas as redes sem fio durante o trajeto, que ocorreu no dia 02 de Junho de 2008 entre 07h20min e 08h00min da manhã.

Esta coleta se deu com o auxílio de um notebook IBM, contendo de rede wireless externa produzida pela Sony Ericcson. A placa foi ativada no início da avenida e desativada em seu percurso final. A coleta se deu em um veículo, que se manteve em movimento com velocidade média de 20 kilômetros por hora, com alguns pontos de retenção.

Utilizou-se o programa Network Stumbler 0.4.0 do fabricante NetStumbler. [22]. Este software permite identificar, (inclusive com auxílio de um GPS (Posicionamento global via satélite – tradução livre)), integrando a longitude e latitude do ponto de acesso, caracterizar e fornecer todas as informações da rede encontrada. O programa fornece as seguintes informações sobre a rede encontrada. Como por exemplo, o endereço da placa MAC, o Serviço de Identificação (SSID), nome, canal, velocidade e fabricante da rede.

Na Figura 3, apresentamos a tela inicial do software utilizado, contendo as informações.

Figura 3: Tela principal do NetStumbler em modo de varredura.



V. RESULTADOS OBTIDOS

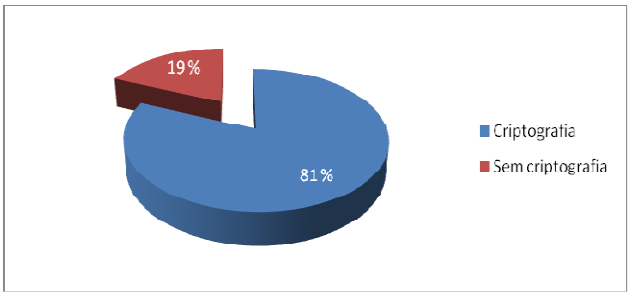
Foram encontrados vários tipos de redes sem fio com as mais diversas formas de segurança ou até mesmo com a falta dela.

Dentre as redes encontradas, podemos citar, como exemplo, redes abertas, fechadas e fechadas com criptografia. As redes criptografadas, na maioria dos casos, como representado nos gráficos 1 e 2 abaixo, utilizam o método WEP, cuja segurança é falha e facilmente quebrável com um programa especialista[37].

Das 295 redes encontradas no trajeto, 240 eram criptografadas, 55 sem qualquer tipo de segurança e 3 dessas 55 eram redes ad-hoc. As velocidades variavam entre 5.5 Mbps e 54 Mbps, ficando a grande maioria com a maior taxa de transmissão. Com os dados coletados, foi montado um infográfico demonstrado os resultados detalhadamente.

Gráfico 1: Redes criptografadas

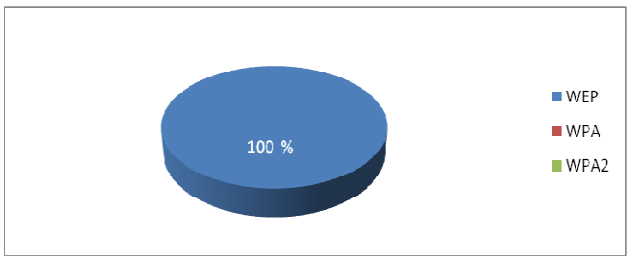
[37] *AirSnort, WepCrack, WepAttack e AirCrack[21]*



Como verificado no gráfico 1, 81% das redes encontradas estão criptografadas com algum método e apenas 19% está sem nenhum tipo de método criptográfico aplicado.

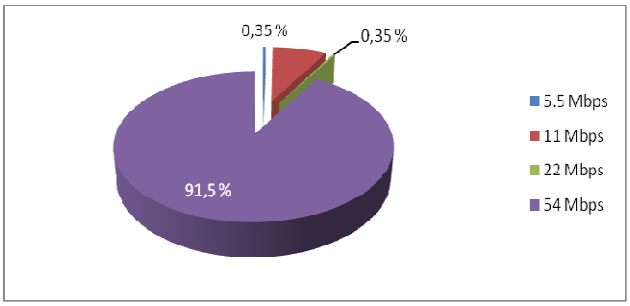
Isso demonstra que a maioria dos usuários se preocupa com os seus dados trafegados na rede, mas não fazem ideia se o nível de segurança que eles aplicaram os atende completamente.

Gráfico 2: Métodos Criptográficos aplicados



Apenas o método criptográfico WEP foi encontrado nas redes criptografadas. O que prova a falta de entendimento entre os métodos existentes e o que cada um faz.

Gráfico 3: Taxa de transmissão aplicada ás redes



Essas taxas se devem ao dispositivo utilizado para cada rede encontrada. Nesse caso, mais de 90% dos equipamentos são mais recentes e oferecem por padrão uma velocidade maior de transmissão que pode chegar a 54 Mbps.

VI. Análise dos resultados obtidos

Podemos ver, pelos dados obtidos, que a região da Avenida Afonso Pena, em Belo Horizonte, se utiliza das seguintes redes:

Mais de 80% é criptografada e 100% dessa criptografia é o protocolo WEP, cuja velocidade de transmissão de mais de 90% dessas redes mapeadas é de 54 Mbps.

Das redes encontradas, observamos um grande número que não possuíam nível de segurança adequado que pode provocar acessos maliciosos até mesmo por parte de usuários mal intencionados que sejam inexperientes.

À medida que a popularização de redes sem fio aumenta, e cada vez mais usuários inexperientes as configuram em casa ou no trabalho, observa-se uma falta de segurança preocupante.

Os assistentes de configuração têm se tornado a fonte usada pelos usuários para garantir a segurança dos dados. Entretanto, estes assistentes se valem, em sua maioria, da criptografia WEP, segundo os achados deste estudo. Ora, conforme vimos pela literatura, esta forma de segurança é a mais precária, tornando a rede vulnerável a ataques. Fica claro que os usuários de redes sem fio da região pesquisada não valorizam uma segurança maior em suas redes, provavelmente por falta de embasamento.

Mesmo com níveis de segurança implementados nas redes sem fio, elas sempre apresentarão riscos e vulnerabilidades. Em qualquer caso, o cliente e o concentrador são sempre alvo de ataques e possíveis falhas, devendo receber atenção especial e constante.

O avanço da tecnologia e a disseminação das redes sem fio, não resolveram alguns problemas, tais como o armazenamento da senha, tanto para o cliente quanto para servidor. Até mesmo os certificados digitais estão vulneráveis a ataques.

Ainda como uma solução para essa insegurança, tem-se os cartões e tokens processados, com objetivo de diminuir as possibilidades de fraude e cópia de informações confidenciais.

Uma das principais deficiências das redes sem fio está na autenticação, já que outros elementos desse enorme conjunto estão em constante evolução, como por exemplo, os algoritmos para criptografia do tráfego e protocolos. Mesmo com o uso de cartões e tokens, há dificuldade de implementação, problemas de escalabilidade e compatibilidade [11].

Outro sério problema é a facilidade em se praticar ataques do tipo negação de serviço. Não existe solução definitiva para esse problema, porém a origem do ataque pode ser monitorada com uso de ferramentas, podendo ser facilmente descoberta [21].

Com base nos padrões de protocolos atuais de segurança, por não atenderem completamente, recomenda-se a utilização de ferramentas de segurança adicionais para aumentar a confiabilidade dos ambientes sem fio. Dentre elas, destaca-se: Firewalls, VPNs[38] (Rede Privada Virtual) e AirMagnet.

Cada ferramenta tem um desempenho diferente com relação ao tipo de ambiente e recursos a serem utilizados pelos usuários da rede. Cada ambiente sem fio tem objetivos específicos, com isso, necessitam de mecanismos de segurança diferentes.

O AirMagnet produzido pela AirMagnet Enterprise, por exemplo, é uma ferramenta que é indicada para integrar diversos mecanismos de segurança, como a que realiza o monitoramento da rede e a detecção de dispositivos não autorizados na rede, além de incluir funcionalidades úteis, como a geração de relatórios. Sendo assim, muito valorizado por administradores de redes.

Cada rede sem fio implementada necessita de constante manutenção e monitoração do ambiente. Geralmente é utilizada uma configuração simples dos mecanismos básicos de segurança da rede, sem o posterior acompanhamento do seu estado. Assim a possibilidade de vulnerabilidades no ambiente aumenta gradativamente [4].

Quando uma rede está bem projetada, ela oferecerá segurança aos seus usuários, negando acessos indevidos e garantindo estabilidade na conexão. A única deficiência é a falta de criação de regras e políticas de segurança eficientes que considerem cada particularidade e pontos fracos que levem em consideração as características do ambiente onde a rede será implantada [4].

VII. CONCLUSÃO

Verificamos aproximadamente 300 redes durante todo o percurso. Destas, a maioria apresenta problemas de segurança, que as tornam vulneráveis a ataques.

Esta falta de segurança é conseqüência da falta de conhecimento dos usuários dos diversos protocolos, uma vez que, quando apresentam algum dispositivo de segurança, em sua maioria apresentam o protocolo WEP. Este protocolo é o que vem de padrão nos assistentes de instalação das redes, popularizando o seu uso. Contudo, este protocolo é precário, e faz-se necessário uma conscientização das empresas dos riscos de segurança a que elas estão sujeitas. Desta

[38] *Virtual Private Network*

conscientização, as empresas podem buscar conhecimento e optar por outros protocolos de segurança mais adequados ao seu negócio. Uma alternativa que está ao alcance dos usuários inexperientes é utilizar dispositivos que forneçam a encriptação dos dados através do protocolo WPA2, que como o citado no artigo, é o mais seguro para transmissão de dados em redes Wireles.

REFERÊNCIAS

[1]ENGST, Adam; FLEISHMAN, Glenn. Kit do Iniciante em Redes Sem Fio: O guia prático sobre redes Wi-Fi para Windows e Macintosh. 2ª ed.: São Paulo. Ed.: Pearson Makron Books. 2005.

[2]GIMENES, Eder Coral. Segurança de Redes Wireless. Mauá, SP. FATEC, 2005, 58p. Trabalho de Conclusão do Curso de Tecnólogo em Informática com ênfase em Gestão de Negócios.

[3]GOLEMBIEWSKI, H. S. D; LUCENA, V. F; SAMPAIO, R. B. Levantamento da área de cobertura de uma rede wireless 802.11: um estudo de caso na UNED de Manaus. I Congresso de Pesquisa e Inovação da Rede Norte Nordeste de Educação Tecnológica. Natal – RN, 2006, 15 p.

[4]GRÉGIO, A .R .A. Wireless Honeynets: Um Modelo de Topologia para Captura e Análise de Ataques a Redes sem Fio. São José do Rio Preto, SP. UNESP / IBILCE, 2005, 57p. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação.

[5]NUNES, Bruno. Bluetooth. 2001. Disponível em http://www.gta.ufrj.br/grad/01_2/bluetooth/index.htm. Acessado em: 17/04/2009.

[6]Infrared Data Association. InfraRed. 2007. Disponível em http://www.irda.org/. Acessado em: 17/04/2009.

[7]MICROSOFT. Configurando Redes Sem Fio IEEE 802.11 Com Windows XP Para Residências e Pequenas Empresas. 2005. Disponível em http://www.microsoft.com/brasil/security/guidance/prodtech/winxp/wifisoho.mspx. Acessado em: 17/04/2009.

[8]MICROSOFT. Decisão sobre uma Estratégia de Rede sem Fio Protegida. 2004. Disponível em: http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.mspx. Acessado em: 17/04/2009.

[9]MICROSOFT. Usando o 802.1X e a Criptografia Para Proteger WLANs. Disponível em: http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod172.mspx. Acessado em: 17/04/2009.

[10]MICROSOFT. Visão Geral da Atualização de Segurança WPA Sem Fio no Windows XP. 2005. Disponível em: http://support.microsoft.com/kb/815485/pt-br. Acessado em: 17/04/2009.

[11]CARRIÓN, Demetrio de Souza Diaz. Implementação De Um Ponto De Acesso Seguro Para Redes 802.11b Baseado No Sistema Operacional OPENBSD. Trabalho de Conclusão do Curso de Engenharia Elétrica, Universidade Federal do Rio de Janeiro. 2003. Disponível em: http://www.ravel.ufrj.br/arquivosPublicacoes/demetrio_projfinal.pdf. Acessado em: 17/04/2009.

[12]MACIEL, Paulo Ditarso et al. Influência dos Mecanismos de Segurança no Tráfego das Redes sem Fio 802.11b. Natal. Workshop de Segurança realizado durante o XXI Simpósio Brasileiro de Redes de Computadores (SBRC2003) em Natal, RN. 2003. Disponível

em: http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=79. Acessado em: 17/04/2009.

[13]ARTHAS, Kael. Tutorial Wireless. 2004. Disponível em: http://www.babooforum.com.br/idealbb/view.asp?topicID=269602. Acessado em: 17/04/2009.

[14]CARDOSO, Rogério. WLANS São Inseguras?. Disponível em: http://www.ciscoredacaovirtual.com/redacao/perfistecnologicos/conectividad.asp?Id=24. Acessado em: 17/04/2009.

[15]Governo do Estado de São Paulo, Instituto de Pesos e Medidas do Estado de São Paulo. Unidades Geométricas e Mecânicas. Disponível em: http://www.ipem.sp.gov.br/5mt/unidade.asp?vpro=mecanica. Acessado em: 28/05/2009.

[16] Institute of Electrical and Electronics Engineers, Inc. Disponível em: http://standards.ieee.org/reading/ieee/interp/802.11_interp.pdf. Acessado em: 28/05/2009.

[17]TORRES, Gabriel; Redes de Computadores. Curso Completo; Editora Axcel Books do Brasil, 2001; Pags. 258 a 271.

[18]SOUSA, Lindeberg Barros; Redes de Computadores. Dados Voz e Imagem; 6ª Edição; Editora Érica, 2002; Pags. 203 a 217 e 413 a 418.

[19]TANENBAUM, Andrew S. Redes de Computadores, 1997, 3ª Edição; Pags 08 à 19.

[20]Prefeitura de Belo Horizonte. Avenida Afonso Pena. Disponível em: http://portalpbh.pbh.gov.br/pbh/ecp/contents.do?evento=conteudo&idConteudo=23858&chPlc=23858&termos=afonso%20pena. Acessado em: 29/05/2009.

[21]LACERDA, Pablo de Souza. Análise de Segurança em Redes Wireless 802.11x. Universidade Federal de Juiz de Fora, 2007, 49 págs.

[22]NETSTUMBLER. Software de varredura de redes Wireless. Disponível em: www.netstumbler.com. Acessado em: 31/05/2009.