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

MOISÉS BRANDALISE

Mapeamento Wireless na Cidade de Bento Gonçalves, RS.

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

Prof. Dr. Luciano Paschoal Gaspary.
Orientador

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

Porto Alegre, dezembro de 2008.

DEDICATÓRIA

Dedico esta obra a todos que colaboraram para o sucesso desta pesquisa. Meus familiares e amigos pelo incentivo e acima de tudo, pelo ser que despertou em mim o interesse profundo pelos estudos, que pelo custo do amor fez com que eu dispusesse de outra forma minha vida em relação ao meu futuro profissional.

AGRADECIMENTO

Ao meu orientador Luciano Paschoal Gaspary, pela eficácia de sua orientação apesar do curto espaço de tempo.

EPÍGRAFE

A magnitude torna-se atônita se mergulhada em um mar bravio.

LISTA DE ABREVIATURAS

AP	Acess Point, ou Ponto de Acesso.
CBC-MAC	Counter Mode Cipher Block Chaining-Message Authentication Code.
EAP	Protocolo Extensivo de Autenticação.
OFDM	Orthogonal Frequency Division Multiplexin.
SSID	Service set Indentifier, ou, Serviço para ajustar a Identificação.
TKIP	Temporal Key Integrity Protocol, algoritmo usado para criptografia.
WEP	Wired Equivalent Privacy.
WPA	WI–FI PROTECTED ACCESS, proteção de rede sem fio.
WLAN	Wireless Local Area Network, ou seja, Rede local sem fio.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

RESUMO

Este projeto tem como objetivo fazer uma análise das redes wireless na cidade de Bento Gonçalves, estado do Rio Grande do Sul, Brasil. Wireless são redes sem fio bastante utilizadas para transmissão de dados entre computadores. Incialmente será feito um estudo dos tipos de redes existentes como Ad-Hoc e Ap. Em seguida apresenta-se um capítulo sobre os protocolos de autenticação como WEP e WPA explicitando a diferença entre eles. Para finalizar a parte do embasamento teórico faz-se um estudo dos algoritmos de criptografia TKIP e AES. No capítulo 3, apresenta-se uma experiência feita capturando redes em 21 pontos da cidade, usando um notebook e um software de captura e análise de tráfego. Ao final, demonstra-se os números obtidos, gráficos, comparativos entre redes abertas e redes fechadas, intensidade do sinal dentre outros números.

Palavras Chave: redes, wireless, Bento Gonçalves, sem fio, segurança, wep, wpa.

Mapping Wireless in the city of Bento Goncalves, RS.

ABSTRACT

The present work has the objective of analyzing the wireless network in the city of Bento Gonçalves, in the state of RS, Brazil. Wireless is a network with no wire used to transmit data to other computers. Firstly, a study of kinds of net will be analyzed such as Ad-Hoc and Ad-Hoc and Ap. Afterwards it is showed a chapter about protocols authentication such as WEP and WPA explaining the difference between them. To finish the theoretical concept, it is necessary a study of the algorithm of the cryptography TKIP and AES. In chapter 3, it is showed an experiment capturing networks in 21 places in the city, using a notebook and software of captures and traffic analyses.At the end it is showed the numbers obtained, graphics, comparisons between open network and closed network, intensity of the signal among other numbers.

Keywords: networks, wireless, Bento Gonçalves, security, wep, wpa.

1 INTRODUÇÃO

Com o forte avanço da internet e necessidades de sigilo em redes computacionais, falar em segurança é algo justificável e sem sombra de dúvidas, muito importante. Noticia-se cotidianamente através dos veículos de comunicação, tentativas frustradas e também bem sucedidas de delitos realizados na grande rede de computadores, a internet.

A maioria das empresas, sejam públicas ou privadas, estão preocupadas com questões como sigilo de dados o que envolve diretamente a segurança de sua infra estrutura computacional. Algunas usuários domésticos hoje possuem informações relevantes em seus computadores pessoais, o que torna este problema não apenas corporativo. Após a chegada propriamente dita da internet, que inicialmente era mais conhecida pelo uso de cabos de cobre, cabos coaxiais dentre outros, algumas outras tecnologias de transmissão de dados foram sendo melhoradas. É o caso das redes sem fio as chamadas redes wireless, redes estas que se fazem presente em todos os lugares, disseminadas através de suas ondas que se propagam pelo ar.

Atualmente na cidade de Bento Gonçalves pode-se notar que de alguns pontos, muitas redes são detectadas pela antena sem fio usando um computador portátil. Surgiu diante disso a idéia em desenvolver um estudo mapeando diversos pontos da cidade de forma a fazer um levantamento da atual siutuação das redes wireless e do nível de preocupação que as empresas tem, enfim, o estudo será apresentado ao longo do projeto onde será apresentado de forma clara os números coletados.

O trabalho será dividido em duas partes. A primeira parte, ou seja, no capítulo 2 será feito uma busca na literatura como o objetivo de ambasar o estudo, ou seja, será abordado o resumo dos principais assuntos que envolva a segurança wireless, as tecnologias existentes hoje, como as formas de autenticação, padrões criptográficos, modelos de infra estrutura, padrões internacionais entre outros.

Na segunda parte do projeto, o capítulo 3, será apresentada a experiência realizada. Será feito uma varredura em busca de redes sem fio em diversos pontos da cidade,

com o objetivo de analisar padrões de segurança sem fio utilizados atualmente pelas empresas, usuários domésticos enfim, qualquer rede sem fio detectada. Por fim, serão apresentados os resultados de forma a mostrar o comportamente e o conhecimento por parte de empresas prestadoras de serviço, empresas estas responsáveis pela configuração do equipamento, de usuários domésticos que adquirem equipamentos em lojas de hardware dentre outros números.

2 SEGURANÇA WIRELESS

Com o advento das redes sem fio, as chamadas wireless[1], a segurança dos dados passou a ter outra visão no que tange a segurança. Analisar uma estrutura sem fio, seu raio de atuação é algo que preocupa, pois não temos noção de quem pode estar interceptando o sinal e ou inserindo um sinal malicioso. Pela razão deste projeto estar tratando de redes sem fio, este tópico é de muita importância uma vez que o foco principal desta pesquisa trata de redes wireless.

2.1 Funcionamento das WLANS

As redes sem fio cresceram muito nos ultimos anos, pois com ela é possível montar uma infraestrutura de rede em um ambiente corporativo sem o uso de cabos e sem a necessidade de perfurar paredes. Muitas são as vantagens de usar uma rede sem fio, mas da mesma forma, algumas desvantagens também podem ser apresentadas no seu uso, como por exemplo, a diminuição do sinal pelo fato de ter que passar por obstáculos como uma parede e consequentemente a perda de desempenho da rede. A segurança neste caso é o que mais preocupa o gerente de uma rede, uma vez que o sinal pode ter capturado do lado de fora da instituição ou da residência. Para nos proteger disso, foram criados alguns mecanismos de proteção os quais serão estudados ao longo deste projeto.

Segundo a RNP, através da utilização portadoras de rádio ou infravermelho, as WLANs estabelecem a comunicação de dados entre os pontos da rede. Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas. Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra. Para extrair os dados, o receptor sintoniza numa freqüência específica e rejeita as outras portadoras de freqüências diferentes. (RNP, 2008)

[1]Nome em inglês dado a rede de dados com comunicação sem fio.

Os sinais de rádio se propagam por todo o espectro, para testar isso, basta ligar seu notebook e percorrer a cidade, verás que este sinal está em toda a parte. Esta é a proposta deste projeto, sair em busca de redes aberta e fechadas.

As tecnologias de funcionamento em rede sem fios abrangem desde redes de voz e dados globais que permitem aos utilizadores estabelecer ligações sem fios através de longas distâncias, até tecnologias de luzes infravermelhas e frequências de rádio optimizadas para ligações sem fios de curto alcance. Os dispositivos normalmente utilizados para o funcionamento em rede sem fios incluem computadores portáteis, computadores de secretária, computadores de mão, assistentes digitais pessoais (PDA, Personal digital assistant), telemóveis, computadores com caneta e pagers. As tecnologias sem fios servem vários objectivos práticos. Por exemplo, os utilizadores móveis podem utilizar o telemóvel para aceder ao correio electrónico. Os viajantes com computadores portáteis podem ligar à Internet através de terminais instalados em aeroportos, estações de comboio e outros locais públicos. Em casa, os utilizadores podem ligar os dispositivos ao computador de secretária para sincronizar dados e transferir ficheiros. (TECHNET, 2008)

Como podemos ver as WLANs são sinais de rádio transmitidos a uma determinada frequência que podem ser capturados por qualquer receptor que use esta faixa. Sendo assim, foram necessárias algumas modificações no projeto inicial de forma que pudesse ser inserida uma segurança adicional a este sinal.

2.2 SSID

O espectro é composto por muitos sinais de rádio. Estes sinais de rádios estão em toda a parte, basta que tenha um transmissor capaz de emitir o mesmo. O fato das redes sem fio usar a mesma frequência, faz com que esta esteja repleta de sinais dos mais diversos transmissores. O projeto em estudo tem como um de seus objetivos analisar as redes sem fio, estas, identificadas pelo seu SSID.

De acordo com a Wikipidia, trata-se de um nome usado para identificar as redes do padrão 802.11 (será visto nos próximos capítulos). Esta identificação é configurada no Access Point e nas estações receptoras fazendo com que se oomuniquem entre si. (Wikipedia, 2008).

No estudo a ser relalizado, será feita a identificação de muitas redes pelo seu SSID, de forma a possibilitar um estudo sólido dos principais aspectos e pontos importantes.

2.3 Tipos de Redes sem Fio

Falar dos tipos de redes sem fio é algo importante uma vez que muitas são as tecnologias e padrões utilizados para a transmissão de dados sem fio.

Tal como com as redes com fios, as redes sem fios podem ser classificadas em diferentes tipos com base nas distâncias através das quais os dados podem ser transmitidos. (TECHNET, 2008)

As redes que serão analisados no experimento serão locais, ou seja, Wlans com pouco intensidade de sinal, algo que não ultrapasse raios de 100 metros. Estas redes geralmente são redes de empresas e usuários domésticos que fizerama instalação para uso privado.

2.3.1 Sem Fio Ad-hoc (ponto a ponto)

Trata-se de uma espécie de barramento de interconexão onde não existe um nó principal. A comunicação é feita entre os equipamentos, ou seja, ponto a ponto. Em nosso estudo, dificilmente poderá ser identificada se uma rede possui esta característica. De qualquer forma, seu sinal poderá estar presente nas capturas para posterior análise.

Vários computadores, cada um equipado com placas de interface de rede sem fio. Cada computador pode comunicar diretamente com todos os outros equipados com placas de interface. Eles podem compartilhar arquivos, impressoras, mas não acessar os recursos de uma rede fixa. (UFCAR, 2008)

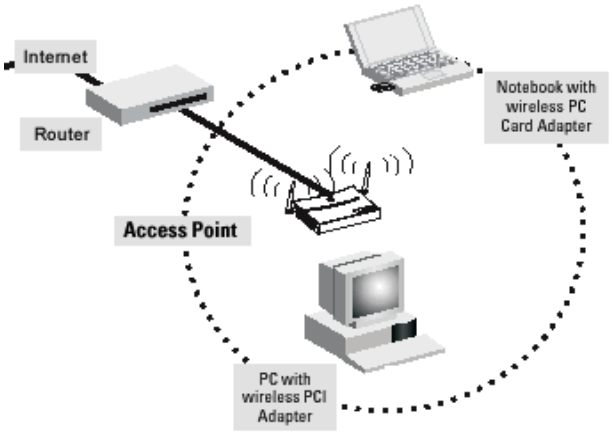
Também segundo a Wikipedia, o termo é empregado para designar o tipo de rede que não possui um nó ou terminal especial para o qual todas as comunicações convergem e que as encaminha para os respectivos destinos. (WIKIPEDIA, 2008)

Em resumo, trata-se de equipamentos com funções próprias que dispensam o uso de um nó principal, que é o caso do AP. Este será tratado a seguir.

2.3.2 Sem fio com uso de AP (ponto de Acesso)

As redes que utilizam Ponto de Acesso, os chamdos AP, são muito utilizados. Estes pontos de acesso emitem seu sinal o qual pode ser capturado por pontos pré configurados ou não, dependendo da segurança, o qual passa a se comunicar diretamente com este.

Uma rede local sem fio pode possuir um ponto de acesso, que funciona como os hubs das outras redes. Esses pontos de acesso podem conectar (como uma ponte) uma rede local sem fio a uma rede local fixa, permitindo aos computadores acessar os recursos dessa rede. (UFCAR, 2008)



Fonte: http://www.hp.com/sbso/images/oov/wireless/oov_access_point_diagram2.gif
Figura 2.1 – Infraestrutua de Funcionamento de um Access Point

Na figura acima, um unico ponto principal serve para distribuir seu sinal para diversos equipamentos, como por exemplo, computadores pessoais, notebooks dentre outros equipamentos. Basta que o equipamento possua o padrão 802.11 e este, estará apto para atuar na rede.

2.4 Protocolos

Protocolos são características em comum que permitem com que determinados indivíduos conversem entre si de maneira organizada. Em redes sem fio, veremos alguns protocolos de de segurança, estes se não o mais, mas um dos fatores mais importantes em termos de segurança sem fio.

São os protocolos que determinam as características e as técnicas usadas para sua aplicação. A seguir, veremos os três mais usados protocolos em redes wireless atualmente, são eles, WEP, WPA e WPA2.

2.4.1 WEP

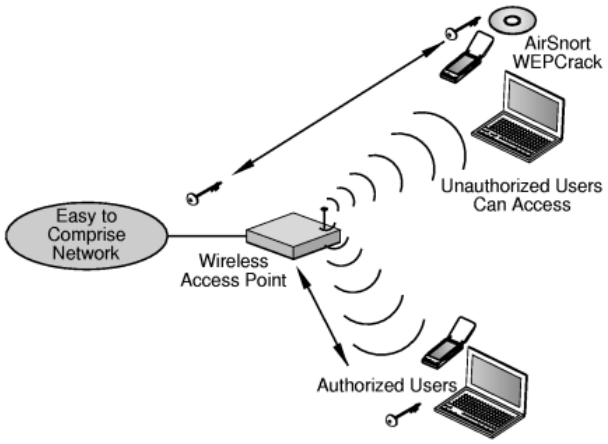
Este foi um dos primeiros protocolos a serem criados como forma de identificar e proteger as redes sem fio.

Segundo estudos feitos na universidade de Berkeley, o protocolo WEP depende de uma chave secreta que é compartilhada entre a estação móvel, por exemplo, um laptop com placa de rede sem fio e um ponto de acesso, seja estação (ad hoc) ou uma base de Acesso

(AP). A chave de acesso é usada para criptografar os pacotes antes de serem transmitidos. Estas técnicas são usadas para defender a rede de ataques externos. (BERKELEY, 2008)

Esta parte do texto descreve parcialmente a intenção deste projeto, em outras palavras, serão analisadas redes sem fio de forma a caracterizar as técnicas de cifragem usada.

Segundo BORISOV, cada uma das partes que desejam participar da comunicação deve possuir uma chave secreta k que será usada no processo de criptografia e no processo inverso também. Esta chave k será a mesma usada tanto para criptografar os dados a serem transmitidos como para recuperar os dados na recepção. O nome que se dá a este processo é criptografia simétrica devido ao fato da chave ser única para os dois processos. É importante lembrar que a troca de chaves deve ser feita de maneira segura, se possível pessoalmente, para que a segurança não seja comprometida. (BORISOV, 2001)



Fonte: http://docs.hp.com/en/T1428-90017/img/gfx1.gif
Figura 2.2 – Distribuição da chave WEP entre os equipamentos.

Podemos ver na figura 2, a distribuição de chaves entre o Wireless Access Point (AP) e os equipamentos a sua volta. Esta chave será usada para a cifragem dos pacotes transmitidos entre eles.

Através de algumas pesquisas feitas na internet, pode-se verificar que esta técnica de distribuição de chaves é algo que nos traz pouca segurança, pois muitas são as ferramentas disponíveis para quebrar esta chave.

2.4.2 WPA

A técnica WPA, trouxe um pouco mais de conforto em termos de segurancça uma vez que funciona de forma parecida com a WEP, porém, com algumas implementações e aperfeiçoamentos.

De acordo com o padrão IEEE 802.11, tendo em vista o grande número de vulnerabilidades apresentadas pelo protocolo WEP, um grupo de trabalho do IEEE 802.11 iniciou pesquisas para o desenvolvimento de um novo padrão de segurança denominado IEEE 802.11i. O intuito primordial era resolver todos os problemas de segurança encontrados no WEP. Enquanto o padrão estava sendo desenvolvido, a *Wi-Fi Alliance*[2], para responder às críticas geradas pelo meio corporativo em relação ao WEP, apresentou em 2003 um padrão denominado *Wi-Fi Protected Access* (WPA). (IEEE, 2008)

Segundo BULHMAN, a autenticação WPA é uma combinação de sistemas abertos e 802.1x e utiliza as seguintes fases:

- primeira fase usa uma autenticação de sistema aberto para indicar a um cliente sem fio que pode enviar quadro para o ponto de acesso;
- A segunda fase usa o 802.1x para executar a autenticação em nível de usuário.

Para ambientes sem infra–estrutura RADIUS[3], o WPA suporta o uso de chave pré–compartilhada. Já para ambientes com infra–estrutura de RADIUS o WPA suporta EAP e RADIUS (BULHMAN, 2008)

Ainda neste protocolo, encontramos o encapsulamento TKIP que foi umas das grandes mudanças em relação ao protocolo WEP. Segundo pesquisa, (RUFFINO, Nelson) a criptografia dos dados ao utilizar um protocolo de chave temporária TKIP, possibilita a criação de chaves por pacotes, além de possuir função que detecta erros de chamada. Possui um vetor de inicialização de 48 bits em contrapartida aos 24 do WEP e ainda possui um mecanismo de distribuição de chaves. Mas existem ainda vulnerabilidades que permitem a captura de informações para invasão em redes com este modelo adotado. (RUFFINO, 2005)

Este algoritmo será tratado com maiores detalhes nao próximo capítulo.

2.5 WPA2

Neste capítulo será visto mais uma variação do WPA, ou seja, uma melhoria em sua estrutura. Todas essa inovaçoes tem o intúito de siminuir os riscos em relação a segurança.

O Wi-Fi Protected Access 2 (WPA2) é baseado na norma IEEE 802.11i; oferece um mecanismo de encriptação utilizando o Protocolo AES-CCMP (Advanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). O que garante o nível de privacidade de dados exigido por muitas instituições financeiras e governamentais. (USR, 2008)

Segundo a (Wi-Fi Aliance), o futuro da segurança deverá seguir o padrão WPA2. A encriptação TKIP que será vista logo abaixo, a autenticação PSK e WPA são características apresentadas a partir da WPA e além disso, o uso da criptogradia AES (Advanced Encryption

[2]Associação internacional sem fins lucrativos formada em 1999 para certificar produtos Wi-Fi baseados no padrão IEEE 802.11. A certificação de produtos Wi-Fi teve início em março de 2000. Um dos principais objetivos é assegurar a interoperabilidade entre todos os equipamentos certificados pela Wi-Fi Alliance.

[3]É um protocolo AAA para aplicações para acesso à rede de computadores e mobilidade através de rede IP.

Standard). AES já foi adotado como padrão no Ministério do Comercio e no Instituto Nacional de Padrões e Tecnologia nos EUA. (WI-FI, Alliance)

Como notamos, a tendência da segurança tende a ser o padrão WPA2, porém, hoje em dia, muitas empresas e usuários domésticos ainda usam WEP e WPA. As razões podem ser as mais diversar, como por exemplo, equipamentos obsoltetos e até mesmo falta de conhecimento para reconfiguração.

2.6 Algoritmos de Criptografia

Neste capítulo será apresentada as principais formas de criptografia em comunicação de dados sem fio. Este estudo é julgado importante uma vez que dependemos diretamente de inteligências como estas para possibilitar o sigilo de informações.

Criptografia (Do Grego *kryptós*, "escondido", e *gráphein*, "escrita") segundo (TKOTZ, 2005) é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. (TKOTZ, 2008)

Por estarmos tratando de transmissão de dados sem fio e sabendo que este sinal por ser capturado por todos que estiverem ao alcance do sinal, transmitir dados de forma segura na marioria das vezes se faz necessário. Dentre inúmeras outras e esta, serão avaliados os algoritmos TKIP e AES, ambos citados em capítulos anteriores.

2.6.1 TKIP

De forma a eliminar as falhas do protocolo WEP, pesquisadores do grupo de trabalho do 802.11i definiram o uso do TKIP. O protocolo, que também pode ser chamado de WPA supera o WEP no seu processo de cifragem pelo fato de fazer uso de chaves temporárias.

De acordo com (TURATTO, 2002), o TKIP utiliza o tamanho de chaves de 128 bits, esse tamanho era opcional no WEP (padrão é de 64 bits) e também dobrou o tamanho do vetor de inicialização, o tamanho do vetor de inicalização ficou de 48 bits, ao contrário de 24 bits que era no WEP, possibilitando dessa forma um espaço maior de possibilidades de keystreams.

Outra característica muito importante ainda segundo (TURATTO, 2002), é que o TKIP é que a chave compartilhada entre os usuários Wireless e o ponto de acesso é alterada de tempo em tempo. Essa chave é trocada a cada 10.000 quadros. (TURATTO, 2002)

A afirmação de (MICHAEL, 2002), onde ele diz que para evitar ataque de repetição e inserção o TKIP implementa número de sequência e para integridade dos dados utiliza o algoritmo MIC - Message Integrity Checksum (MICHAEL, 2002).

2.6.2 AES

Nesta seção que serve como base teórica para a experiência do próximo capítulo, analisaremos algumas características do AES e sua forma de funcionamento.

Os algoritmos evolutivos ou evolucionários (*Aes*) são paradigmas computacionais da inteligência computacional para resolução de problemas, inspirados nos princípios da teoria evolutiva de Darwin e na genética de Mendel.(GOLDBERG, 1989).

Também segundo (TECHNET, 2008), o padrão IEEE 802.11i substitui formalmente o WEP (Wired Equivalent Privacy) no padrão IEEE 802.11 original com um modo específico do AES (Advanced Encryption Standard) conhecido como protocolo CBC-MAC (Counter Mode Cipher Block Chaining-Message Authentication Code) ou CCMP. O CCMP oferece confidencialidade (criptografia) e integridade dos dados. Este artigo descreve os detalhes da implementação WPA2 do CCMP do AES para criptografia, descriptografia e validação da integridade dos dados dos quadros sem fio 802.11. (TECHNET, 2008)

De acordo com (RUFFINO, 2005), a grande novidade do 802.11i é a substituição TKIP (RC4) pelo CCMP (AES). Desta forma, o novo padrão resolve o problema da criptografia fraca. O problema de performance é resolvido com a utilização de co-processadores criptográficos. Uma segunda novidade é a presença de tratamento para Roaming, mecanismo até então não presente nas soluções. (RUFFINO, 2005)

Como visto, o AES incorporou muitas vantagens em relação ao seu uso. A reutilização de equipamentos fica um pouco comprometida uma vez que o mesmo é considerado um algoritmo pesado o que demanda mais poder de processamento.

2.7 Padrão IEEE 802.11

Será feito agora um estudo sob o ponto de vista da segurança que contempla o padrão IEEE 802.11. Quando fala-se em padrão nos vem em mente a palavra padronização. Este é o papel do instituto IEEE o qual junto com entidades influentes definiram o padrão que será visto com mais detalhes a seguir.

Como cita a (INFOWESTER, 2008), o padrão 802.11 estabelece normas para a criação e para o uso de redes sem fio. A transmissão dessa rede é feita por sinais de radiofreqüência, que se propagam pelo ar e podem cobrir áreas na casa das centenas de metros. Como existem inúmeros serviços que podem utilizar sinais de rádio, é necessário que cada um opere de acordo com as exigências estabelecidas pelo governo de cada país. (INFOWESTER, 2008)

Será feito a seguir um estudo dos principais versões do 802.11:

- *802.11*. Segundo (EBIANCHI, 2000), em 1997, a primeira versão do padrão IEEE 02.11 foi lançada e especificava um padrão na faixa e operação de 2,4GHz alcançando taxas de até 2Mbps. Em 1999, o padrão recebeu uma atualização, passando a contar com duas novas PHY, IEEE 802.11a e IEEE 802.11b. O padrão IEEE 802.11a, que opera na faixa de 5GHz, especifica uma PHY baseada em OFDM (Orthogonal Frequency Division Multiplexing), alcançando taxas de até 54Mbps. (BIANCHI, 2000).

- 802.11i. Foi nesta versão que foram incluídos os protocolos de segurança discutidos anteriormente, como WEP, TKIP e AES. Segundo (WIKIPEDIA, 2008) O grupo de trabalho 802.11i vem trabalhando na integração do AES com a subcamada MAC, uma vez que o padrão até então utilizado pelo WEP e WPA, o RC4, não é robusto o suficiente para garantir a segurança das informações que circulam pelas redes de comunicação sem fio. O principal benefício do projeto do padrão 802.11i é sua extensibilidade permitida, porque se uma falha é descoberta numa técnica de criptografia usada, o padrão permite facilmente a adição de uma nova técnica sem a substituição do hardware. (WIKIPEDIA, 2008)

Este capítulo serviu para apresentar algumas particularidades do padrão 802.11 que serve como base para a pesquisa a ser desenvolvida. O embasamento teórico apresentado se fez necesário uma vez que o estudo a seguir, condiz e está fortemente ligado as especificações feitas. Será feito nas sequência uma pesquisa de um assunto de suma importância, a integração AES com endereço MAC.

2.7.1 Integração do AES com a subcamada MAC

A integração entre estas duas tecnologias certamente vem a colaborar com o aumento da segurança de redes sem fio.

Conforme cita (CASTRO, 2008), As redes locais usam topologia de difusão, o que significa que os nós de uma rede local compartilham um canal de comunicação único e precisam disputar o mesmo meio para transmitir os dados. A subcamada MAC oferece a forma como os nós compartilham o meio físico (quem, como, quando e por quanto tempo ocorrerá o uso do canal). Duas categorias amplas de métodos de acesso são mais apropriadas para redes locais: acesso não-sequencial (por vezes chamado de estocástico ou estatístico) e passagem de mensagens (denominado determinístico). (CASTRO, 2008)

No que se refere a não sequencial, diz (TANEMBAUM, 2003), os protocolos ditos de acesso não-seqüencial definem como um nó pode acessar um canal de comunicações de múltiplo acesso. Em princípio, um nó pode transmitir sempre que tiver dados para transmitir, o que pode provocar uma colisão, geralmente com a perda das mensagens. (TANEMBAUM, 2003).

Falando em passagem de mensagem, afirma (WIKIPEDIA, 2008) onde são transmitidas mensagens apenas através de conexões, canais virtuais que são, em geral, unidirecionais e não-confiáveis, anexáveis a um ponto de entrada e outro de saída (pontos de conexão). Conexões possuem identificadores únicos, e não estão associadas a um dispositivo de rede real, havendo um serviço de resolução de identificadores para dispositivos de rede. Também estão disponíveis conexões bidirecionais ou confiáveis, implementados sobre as conxões convencionais.(WIKIPEDIA., 2008)

Com esta base teórica, pode-se prosseguir com a experiencia. Todos os capítulos apresentados nas seções anteriores trazem em seu cerne conteúdos importantes que embasam fortemente a pesquisa e principalmente o foco do projeto.

3 EXPERIÊNCIA REALIZADA

3.1 Conceitos

O projeto realizado teve como base de dados as redes sem fio detectadas na cidade de Bento Gonçalves, estado do Rio Grande do Sul, Brasil. O projeto foi desenvolvido usando a técnica conhecida como Wardriving[4]. Trata-se de uma técnica conhecida no "mundo wireless" que consiste em percorrer a cidade utilizando-se de um carro ou qualquer outro meio móvel em busca de redes sem fio, abertas (sem segurança) ou fechadas (com criptografia). A idéia centrou-se em mapear a cidade de forma a identificar particularidades das redes wireless.

3.2 Ferramentas utilizadas

Para que o projeto fosse realizado, alguns recursos foram necessários para que a obtenção dos dados pudesse ser feita. Tais recursos, os quais serão detalhados na sequência são de fácil acesso e de baixo custo. Em se tratando de custos monetários, vale ressaltar que os custos foram baixos em termos de hardware, porém em termos humanos, muitas horas foram usadas para a realização das atividades.

Para que as práticas pudessem ser realizadas, foi necessário um computador pessoal (notebook) com uma interface wireless, alguns softwares e um carro para o deslocamento entre os pontos de coleta.

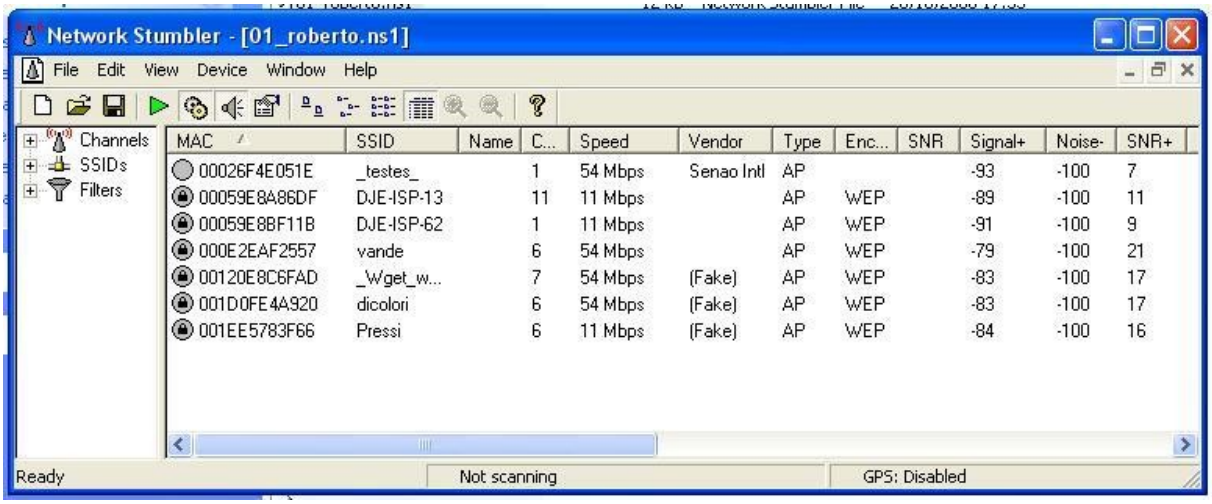
O computador utilizado foi um Notebook da marca Toshiba, composto de um processador "Pentium R 4", com "Cpu de 2,8Ghz", "memória Ram de 512MB" e Interface de rede "Atheros AR50001X+Wireless Network Adapter".

O sistema operacional utilizado foi o "Microsofot Windows XP professional", com SP2 instalado. Ainda em se tratando de software, a ferramenta principal utilizada foi o Netword Stumbler Versão 0.4.0. (Build 554), conhecido como "NetStumbler" . Trata-se de

[4]Wardriving – Utilizando-se de um veiculo automotor, percorrer a cidade em busca de redes sem fio.

um software utilizado para fazer captura de redes wireless bastante conhecido. Este software e capaz de capturar e armazenar informações sobre as redes que estiverem ao alcance do adaptador de rede. Com ele é possível fazer algumas análises gráficas e obter um número muito grande de informações das características das redes detectadas, como por exemplo, o SSID da rede, se possui ou não ciptografia, qual o endereço MAC do equipamento dentre outros.

Para ilustrar e tornar mais compreensível, segue abaixo uma figura ilustrativa de uma tela do NetStumbler e algumas redes capturadas.



Fonte: Própria.
Figura 3.1 – Captura de dados utilizando a ferramenta NetStumbler

Como podemos observar, o software exibe diversas colunas de dados, sao elas:

- MAC; endereco físico do equipamento transmissor dos dados.
- SSID; Identificação da rede.
- Name; Nome da rede para exibição.
- Channel; Canal utilizado para a transmissão dos dados.
- Speed; Velocidade em Mbps da transmissão dos dados.
- Vendor; Fabricante do Equipamento.
- Type; Base station connection, geralmente é AP.
- Encryption; Tipo de segurança implementada.
- SNR; Relação entre sinal e ruído.
- Signal; Intensidade do sinal.
- Noise; Intensidade de Ruído.
- SNR+; 100 - Relação entre sinal e ruído, ou seja, SNR positivo.

- Ip Addr; Endereco Ip do Equipamento.

Pode-se notar que temos diversas informações a respeito das redes.

Além desta ferramenta, foi usado uma planilha eletrônica e um veículo automotor de pequeno porte, ou seja, um veículo normal de passeio.

3.1 Coleta dos dados

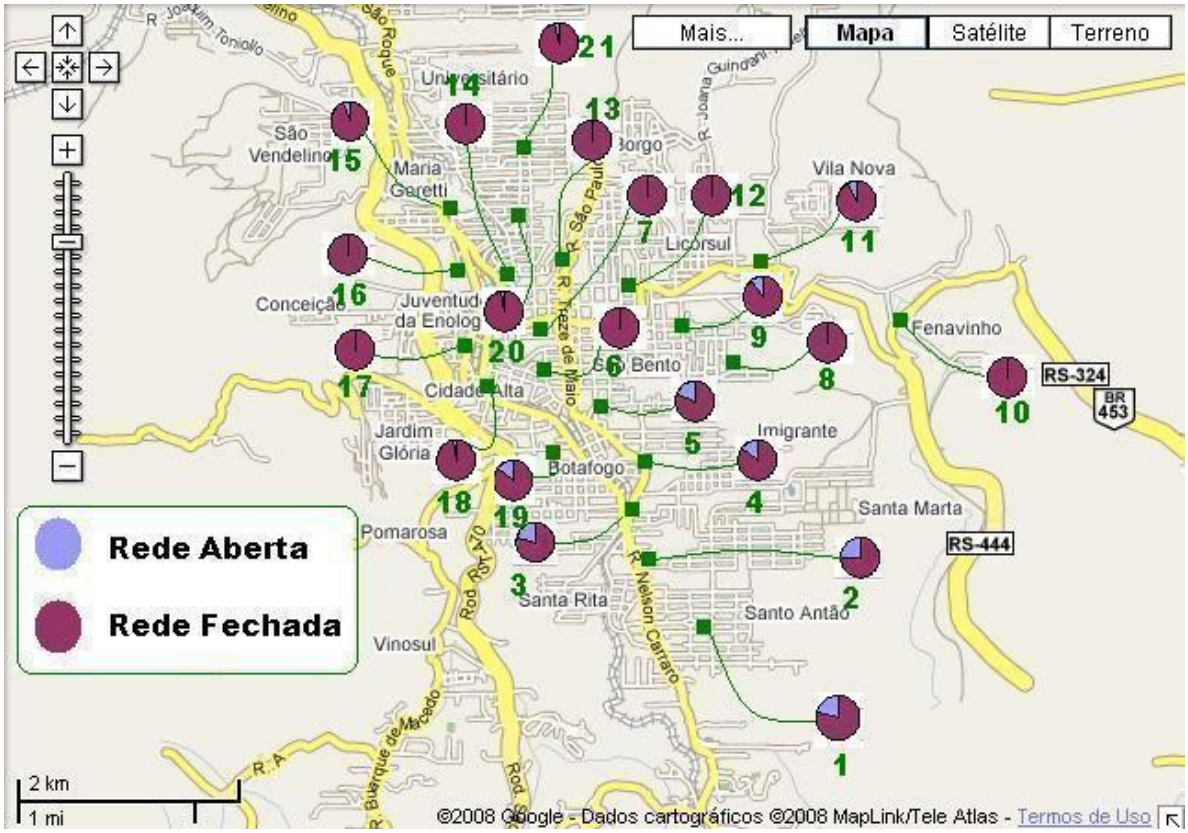
Tão importante quando os equipamentos é a coleta das informações. A coleta foi feita em diversos pontos da cidade os quais serão expostos a seguir. Para que a coleta fosse feita nos pontos abaixo, o veículo era estacionado e o computador pessoal colocado sobre ele durante 60 segundos. Neste tempo, o NetStumbler capturava todas as redes disponíveis e as exibia. O tempo de 60 segundos foi definido em função de duas capturas, onde ambas se aproximando dos 50 segundos, apresentaram duas novas redes apesar de seu sinal ser fraco. Diante destas duas experiências, foram padronizadas capturas de 60 segundos.

Os pontos de captura e seus respectivos endereços na cidade de Bento Gonçalves, Rio Grande do Sul são:

- Ponto 1; Rua Nelson Carraro, esquina com rua Ulisses Gasperi..
- Ponto 2; Rua Nelson Carraro, esquina com rua Marcos Valduga
- Ponto 3; Rua Nelson Carraro, esquina com rua Joao Estéfano.
- Ponto 4; Rua Vitorio Carraro, esquina com rua Rua Pinto Bandeira.
- Ponto 5; Rua 13 de maio, esquina com rua Vitória.
- Ponto 6; Rua 13 de maio, esquina com rua General Osório.
- Ponto 7; Rua Ramiro Barcelos, esquina com rua Marinho.
- Ponto 8; Rua planalto, esquina com rua Hmy Dreher.
- Ponto 9; Rua Hmy Dreher, esquina com rua 15 de novembro.
- Ponto 10; Rua Domingos Rubechini, em frente ao portão principal das pavilhões da Fenavinho.
- Ponto 11; Rua Marechal Castelo Branco, esquina com rua João Tomian.
- Ponto 12; Rua Eugênio Valduga, esquina com rua Gal Goes Monteiro.
- Ponto 13; Rua Gal Goes Monteiro, esquina com rua Cav Horácio Mônaco.
- Ponto 14; Rua Marechal Deodoro, esquina com rua Dr. Antunes.
- Ponto 15; Rua Gerenal Gomes Carneiro, esquina com rua Avaí.
- Ponto 16; Rua Osvaldo Aranha, esquina com rua Tupanciretã.
- Ponto 17; Rua Osvaldo Aranha, esquina com travessa Pelotas.
- Ponto 18; Rua 10 de novembro, esquina com travessa Bagé.

- Ponto 19; Rua 10 de novembro, esquina com travessa Curitiba.
- Ponto 20; Rua Saldanha Marinho, esquina com rua Barão do Rio Branco.
- Ponto 21; Rua Marechal Deodoro, esquina com rua Cândido Costa.

Conforme descrito acima, estes são os pontos de coleta e os endereços. Com esta captura, pode-se dizer que a área urbana de maior movimento foi mapeada. Segue abaixo mapa urbano da cidade, com os pontos de coleta e indicativos de redes seguras ou abertas.



Fonte: http://maps.google.com.br
Figura 3.2 – Mapa da cidade com pontos de coleta.

É possível observar na figura acima os pontos que determinam o local da coletas dos dados. Pode-se dizer que 70% da área urbana faz parte dos números que serão apresentados no decorrer do projeto. Para determinar os pontos de coleta nao foi usada nenhuma técnica de subdivisão da área. Foram percorridos os principais pontos de acesso a cidade, as ruas mais movimentadas e alguns pontos onde eventos e hotéis importantes estão localizados.

3.2 Dados coletados

Como citado anteriormente, com a utilização do software NetStumbler foi possível fazer a captura dos dados. Os dados que o netstumbler consegue capturar vão além da tela principal. O software possui um recurso de exportação de dados o qual foi explorado neste trabalho. Todos os 21 pontos de coleta tiveram seu "Sumary" exportado em formato texto, e em seguida, importados para uma planilha eletrônica. Os dados foram dispostos na seguinte sequência. SSID, BSSID, SNR Sig Noise, Flags, Channelbits, Bclntvl, Data Rate, LastChannel. Podemos ver abaixo uma tabela da planilha eletrônica e seus dados.

Tabela 3.1: Exposição dos dados em planilha eletrônica.

(SSID)	(BSSID)	[SNR Sig Noise]	Flags	Channelbits	BcnIntvl	DataRate	LastChannel
( )	(00:0e:2e:85:2d:f7)	[14 63 49]	1	20	100	110	5
(NewSupri)	(00:19:5b:4f:ec:c5)	[24 73 49]	431	2	100	540	1
(_Wget_wan_SAMT)	(00:12:0e:8c:6f:ad)	[36 85 49]	11	80	100	540	7
(Proacao)	(00:1d:0f:fa:5b:78)	[7 56 49]	431	40	100	540	6
( )	(00:4f:62:18:19:e7)	[11 60 49]	401	2	100	540	1
(ITALFAST4)	(00:02:6f:4c:1c:55)	[14 63 49]	421	8	100	110	3

Fonte: Própria.

Abaixo serão relacionadas as principais e mais importantes colunas, são elas:

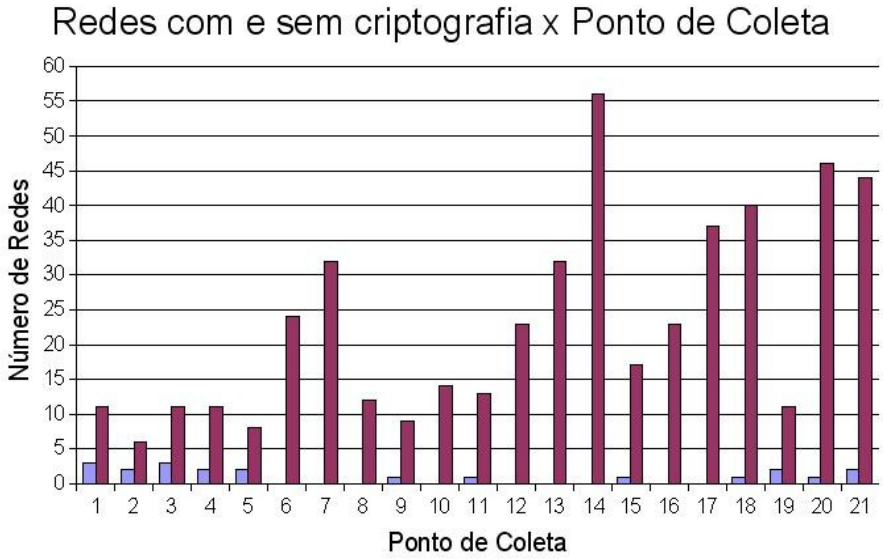
- SSID; Identificação da rede, ou seja, nome dado a rede no momento de sua configuração. Importante ressaltar que as redes sem nome,ou seja, as que são apresentadas apenas com dois parenteses "()", tratam-se de redes sem segurança.
- BSSID; Identificação do endereco MAC do equipamento transmissor.
- SNR Sig Noise; Sao três valores distintos, onde o primeiro (SNR), refere-se a confiabilidade do sinal, quanto maior melhor. O Sig refere-se a intensidade do sinal e o Noise, o ruido. Relacionando os dois ultimos, temos o SNR.

Os dados das 21 capturas foram postos em uma unica planilha eletronica no formato acima. Estas capturas totalizaram 501, sendo que algumas se repetiram em função de sua potência. Incialmente foi feita uma ordenação desta planilha pela coluna SSID, de forma a identificar quantas redes nao possuem SSID, ou seja, estão sem criptografia. O resultado será apresentado no próximo capítulo.

3.3 Analise dos Dados

Algumas análises puderam ser feitas em relação as dados coletados. Inicialmente, procurou-se identificar as redes abertas, ou seja, as redes que não apresentavam nenhuma

criptografia. Pode-se identificar que 21 das 501 totais não apresentavam nenhum tipo de criptografia, ou seja, 4,2% estavam totalmente abertas. Inversamente à esta análise, faz-se uma análise gráfica também das rede com criptografia relacionando por ponto de coleta de dados. Como temos 4,2% de redes abertas, obviamente, teremos 95,8% de redes fechadas: O gráfico abaixo apresenta uma visão organizada das redes abertas e fechadas com seus respectivos pontos de coleta.

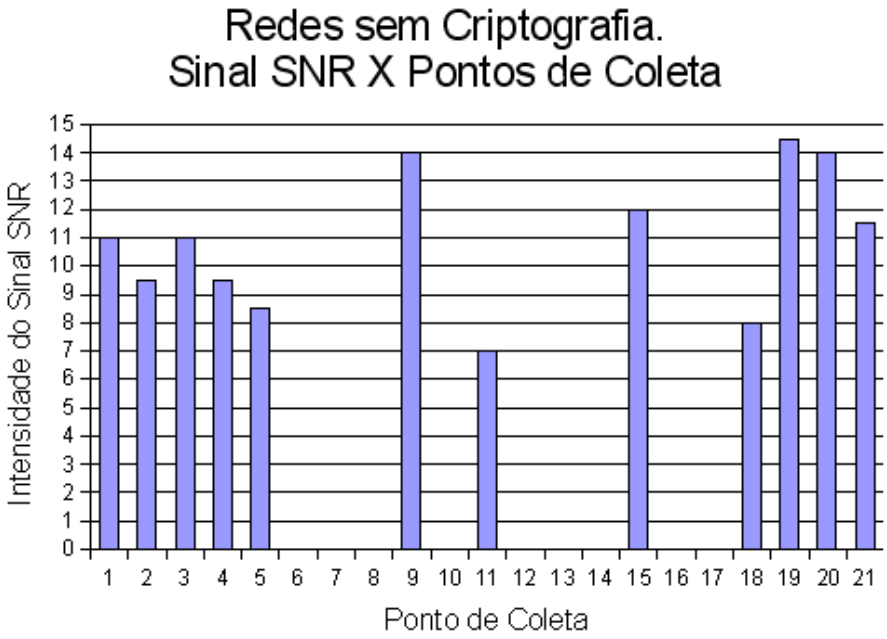


Fonte: Própria

Figura 3.3 – Redes com e sem criptografia e seus pontos de coleta.

Pode-se ver que em alguns pontos, como por exemplo, 6, 7, 8, 12, nenhuma rede aberta pode ser detectada. Observa-se que grande parte das redes possui criptografia, em especial os pontos 14, 20 e 21, com mais de 40 redes cifradas.

Por conta das redes abertas, nao se pode afirmar que estas estão acessíveis. Deve-se levar em conta também o fator SNR+, ou seja, a relação entre o sinal e o ruído. A figura abaixo apresenta os pontos e a intensidade dos sinais.

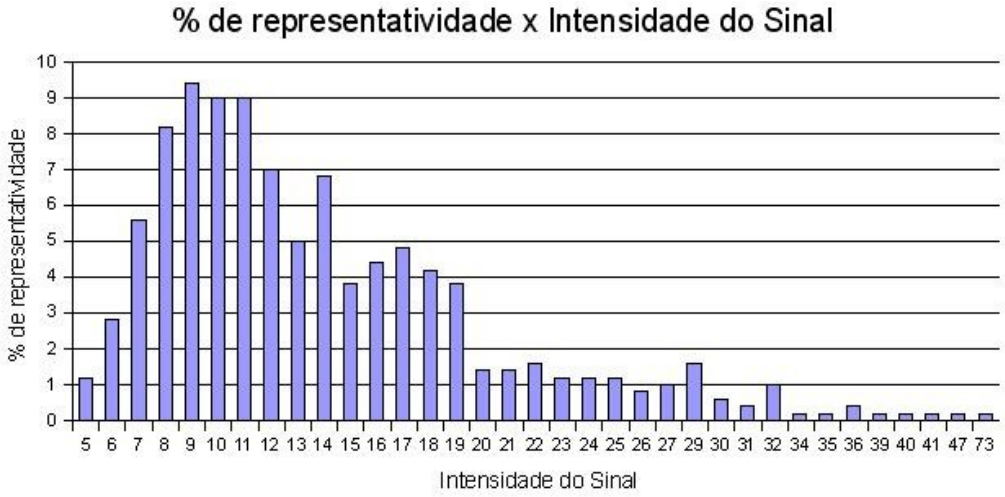


Fonte: Própria
Figura 3.4 – Intensidade do sinal das redes sem criptografia.

O SNR+ apresentado na figura acima trata-se da intensidade do sinal em relação ao ruído. Vale ressaltar que quanto maior o SNR+, mais intenso é o sinal e mais coonfiável o link.O gráfico acima apresenta sinal que chega a 15 dB (deciBel) o que segundo testes realizados neste experimento, os quais serão apresentados ainda neste capítulo, tem-se dificuldades de conexão para troca de pacotes.

Sabe-se que as redes abertas são 4,2%, porém, não se pode fazer o levantamento de quantas são as redes que apresentas criptpografia do tipo WEP e WPA. De qualque forma, consideraremos neste pesquisa apenas redes totalmente abertas e redes fechadas, façam elas uso de WEP ou WPA.

Uma análise importante também feita, refere-se a intensidade do sinal dos pontos de captura e uma média geral. Anteriormente foi feita uma análise da intensidade do sinal apenas das redes abertas. A seguir, será apresentado um gráfico contendo todas as redes e o sinal, seja sinal de rede fechada ou aberta.

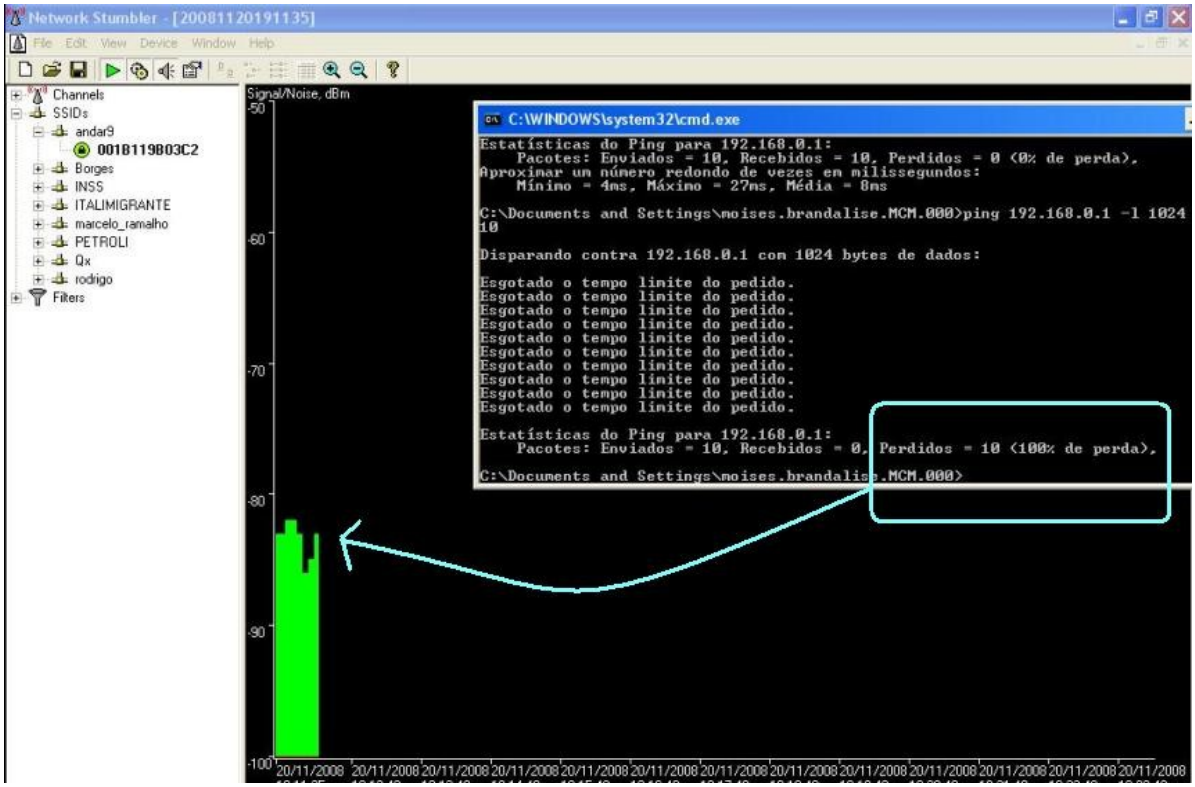


Fonte: Própria
Figura 3.5 – Percentual de representatividade pela intensidade do sinal (SNR+) em todas as redes.

Pode-se observar na figura acima que a intensidade de sinal com maior número de representatividade são os sinal de 7 dB a 19dB. A sinal que mais se fez presente foi o de intensidade 9dB representando 9,38% das redes capturadas seguido do sinal 10 e 11, ambos presentes em 8,98% das redes.

Outro experimento foi feito acerca de avaliar a possibilidade de trocar pacotes entre o link e o notebook no que se refere a intensidade do sinal. Inicialmente tentou-se estabelecer uma conexão de um local com alguns obstáculos como paredes e móveis entre o AP e o notebook. Enquanto conectado foram disparados 10 pings de 1024 bytes. Ao mesmo tempo, o netstumbler ficou rodando na máquina monitorando a intensidade do sinal. Constatou-se que que com o sinal em torno de 16 a 19dB os pacotes não ecoavam, ou seja, o link era perdido.

Podemos ver na figura abaixo a monitoração feita e a intensidade do sinal. Vale ressaltar que o netStumbler apresenta seus dados em SNR, ou seja, negativo. Para chegar nos 16 e 19 apresentados acima, faz-se "-(-100 – (- sinal capturado))" o que matematicamente o torna positivo (SNR+).



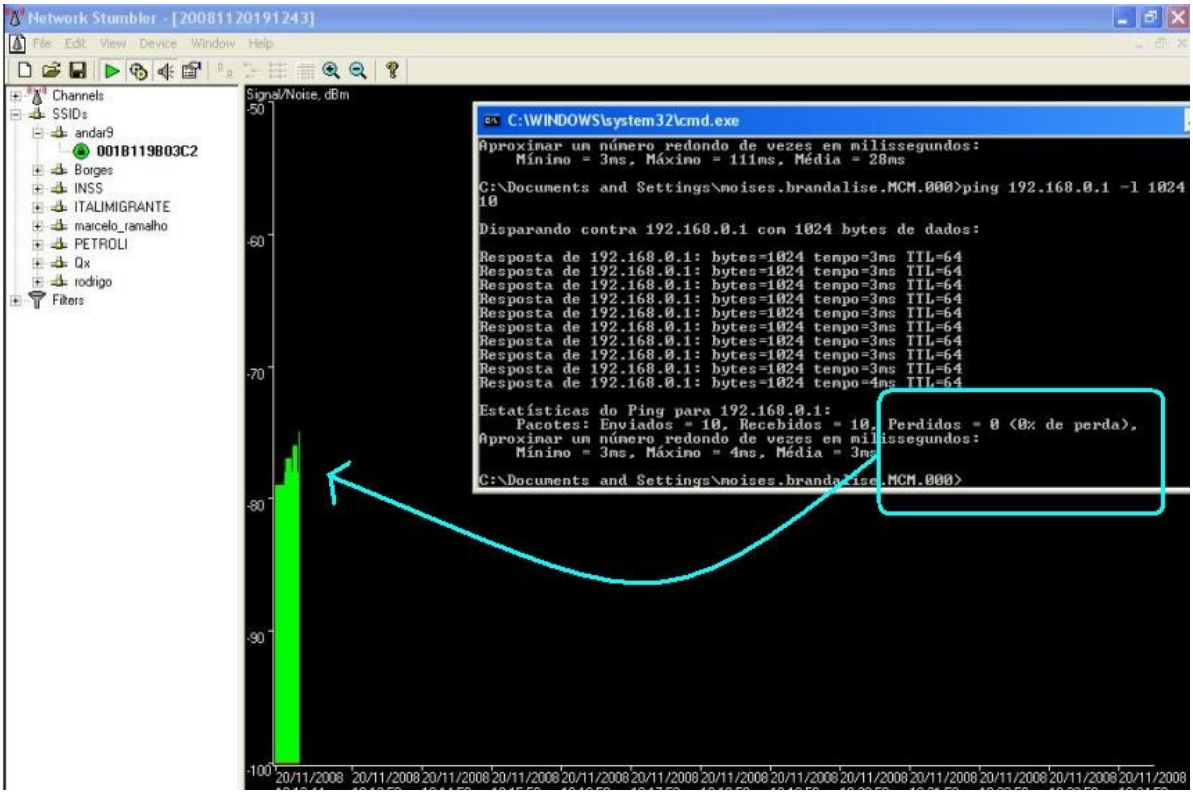
Fonte: Própria

Figura 3.6 – Troca de pacotes entre o notebook e a base com 100% de perda.

Como pode-se observar, o sinal SNR oscila entre 84 e 81 aproximadamente. Se convertido para SNR+, teremos 16 e 19 dB. Diante deste teste, constata-se que com este sinal não é possivel efetuar a troca de pacotes, pois 100% dos pacotes não foram ecoados.

Outro teste foi realizado de forma a conseguir fazer um levantamento a que intensidade de sinal seria possível efetuar a troca de pacotes. O mesmo teste foi realizado, porém, com menos obstáculos entre a base e o notebook. Observou-se que a troca de pacotes foi realizada com sucesso enquanto o sinal oscilava na faixa de 22dB.

Segue abaixo figura ilustrando o teste realizado e o resultado obtido através de um mesmo ping de 1024 bytes.



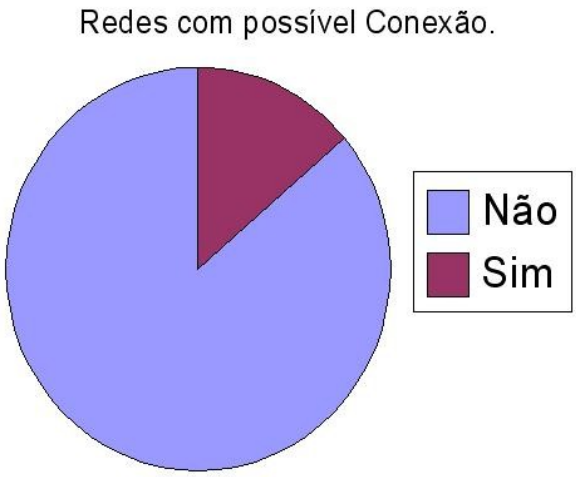
Fonte: Própria

Figura 3.7 – Troca de pacotes entre o notebook e a base com 0 % de perda.

Da mesma forma que a conversão anterior, se convertido o sinal SNR para SNR+, teremos uma intensidade de sinal na faixa de 22 a 24dB. Com estes números, pode-se efetuar a troca de pacotes com 0% de perda.

Com estes números em mãos, pode-se fazer uma média simples e dizer que a faixa de transição entre uma link conectado e um não conectado está em aproximadamente 20dB. Tomando como base este número, será feito a seguir uma análise do número de redes capturadas nos pontos de coleta e em quantas delas é possível conectar e trocar pacotes com o transmissor.

Fazendo-se uma análise detalhada das redes de possível conexão, podemos obter números que caracterizam uma conexão estável entre o transmissore e o receptor nos pontos de coleta de dados. Abaixo, segue gráfico representando o número de redes com possibilidade de troca de dados.



Fonte: Própria
Figura 3.8 – Representatividade das redes com possibilidade de troca de pacotes.

Pode-se observar que são poucas as redes que possibilitam que pacotes sejam trocados. Em números, estas redes representam cerca de 13,7% das redes totais. Dentre todas, apenas uma delas é aberta, ou seja, sem criptografia.

Dentre todas as redes capturadas, algumas se repetiram devido a intensidade e pontência do transmissor. De todas as redes capturadas (501 total), cerca de 19% das redes apareceram no mínimo duas vezes em pontos diferentes de coleta.

4 CONCLUSÃO

De acordo com o estudo realizado, notou-se que grande parte das redes apresentam alguma segurança implícita. Poucas das redes capturadas apresentaram possibilidade de conexão devido ao sinal ser fraco, ou seja, com baixo SNR+. Obviamente o sinal poderia ser intensificado deslocando-se dos pontos de acesso e monitorando a intensidade do mesmo, porém, não era objetivo desta pesquisa realizar a coleta desta forma.

Da forma como o experimento foi feito, ou seja, parando de carro até os pontos de coleta e durante cerca de 60 segundos capturando as redes que se apresentavam no espectro, pode-se dizer que grande parte das redes na área mapeada fez parte desta avaliação. Pode-se dizer também que algumas delas poderiam estar desligadas ou inoperantes durante o tempo de captura, mas isso também não foi levando em consideração, em outras palavras, a captura dos dados foi feita em um único dia sem repetição.

Em relação a segurança das redes, pode-se afirmar que um número muito pequeno de redes estão abertas, ou seja, apenas 4,2% delas. Em conversa com duas das principais empresas prestadoras de serviços de instalação de pontos de acesso wireless, pode-se averiguar que em todas as instalações feitas ao menos um tipo de segurança é adotada, seja WEP ou WPA. Desta forma, os 4,2% de redes abertas podem estar associadas a usuários despreparados que instalaram o equipamento por conta própria, mas isto é apenas uma consideração, não necessariamente um fato.

Em relação ao sinal capturado na redes abertas, em nenhuma delas se pode estabelecer uma conexão confiável. Isto se deve ao fato do sinal monitorado estar abaixo dos 20 dB, onde segundos os testes feitos, impossibilita a transmissão de pacotes de 1024 bytes. Sendo assim, o uso do sinal dentre todas as redes abertas está abaixo do mínimo necessário para uso. Já em relação as redes cifradas, temo algumas redes com possibilidade de transmissão de dados. Segundo análise, 13,7% das redes apresentam sinal SNR+ capaz de possibilitar uma conexão e uma possível troca de dados. Destas, todas possuem algum tipo de criptografia o que impede a conexão. Para o projeto, mesmo redes com baixa segurança (WEP) foi considerada rede fechada. Sabe-se de softwares capazes de burlar o esquema de segurança, principalmente com

o uso do WEP, mas não entraremos em detalhes. Para fins de pesquisa, mesmo as vulneráveis redes WEP foram consideradas seguras.

Diante destes testes e experiências, pode-se dizer que Bento Gonçalves possui uma estrutura wireless confiável, em outras palavras, as empresas prestadoras de serviços e os usuários possuem algum tipo de conhecimento, ou seja, buscaram conhecimento para cifrar suas redes aumentando a segurança e sigilo dos dados que trafegam no raio de seu espectro.

REFERÊNCIAS

BERKELEY, UNIVERSITY. **Secure Protocols.** Disponível em: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.htm. Acessado em: 11 nov 2008.

BORISOV, N., GOLDBERG, I., and WAGNER, D. 2001. "**Intercepting Mobile Communications: The Insecurity of 802.11"** (p 10), São Paulo, Novatec Editora, 2001.

BULHMAN, HAROLSO JOSÉ. **Redes LAN / MAN Wireless III: Aplicação do Padrão 802.11.** Disponível em: http://www.teleco.com.br/tutoriais/tutorialrwlanman3/default.asp, Acessado em: 10 nov, 2008.

G. BIANCHI, Performance Analysis of the IEEE 802.11 Distributed Coordination Function. **IEEE Journal on Selected Areas in Communications**, Vol 18, No. 3, Mar 2000.

GOLDBERG, D. E. **Genetic algorithms in search, optimization, and machine learning,** Person Editora, 1989.

IEEE 802.11i. **Wireless LAN Medium Access Control and Physical Layer specifications.** Disponível em: www.ieee.com. Acessado em: 15 nov, 2008.

INFOWESTER. **Redes sem fio**. Disponível em: http://www.infowester.com/wifi.php. Acessado em: 13 nov, 2008.

RUFFINO, NELSON MURILO DE, "**Segurança em Redes sem Fio**", Novatec Editora, 2005, p 33 a p186.

RNP. **Redes Wireless.** Disponível em: http://www.rnp.br/newsgen/9805/wireless.html. Acessado em: 2 nov, 2008

TANENBAUM, A. S.: "**Redes de Computadores**", 4.ed, Rio de Janeiro, Ed. Campus, 2003.

TECHNET. **Tendencias Tecnológicas** Disponível em: http://technet2.microsoft.com/windowsserver/pt-pt/library/f2552467-f693-4c14-b421-9cb2491bb362070.mspx?mfr=true. Acessado em: 2 de nov, 2008.

TKOTZ, V. "**Criptografia: Segredos embalados para Viagem**", São Paulo: Novatec Editora, 2005, p 27.

TURATTO. **Características do Protocolo TKIP.** Disponível em: http://www.networkexperts.com.br. Acessado em: 12 nov, 2008.

USR. **Tecnologia Wireless Maxg.** Disponível em: http://www.usr.com/download/whitepapers/port/maxg-port-wp.pdf. Acessado em 12 nov, 2008.

WI-FI ALLIANCE. **Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks.** Disponível em: http://www.trentu.ca/admin/it/airtrent/WPA.pdf. Acessado em: 29 nov, 2008.