UNIVERSIDADE DO SAGRADO CORAÇÃO

PIETRO DA SILVA PANZUTO

DESENVOLVIMENTO DE UMA ANTENA MODELO YAGI-UDA PARA ANÁLISES DE SINAIS *WIRELESS* E CÁLCULO DO ELIPSÓIDE DE FRESNEL.

BAURU
2008

UNIVERSIDADE DO SAGRADO CORAÇÃO

PIETRO DA SILVA PANZUTO

DESENVOLVIMENTO DE UMA ANTENA MODELO YAGI-UDA PARA ANÁLISES DE SINAIS *WIRELESS* E CÁLCULO DO ELIPSÓIDE DE FRESNEL.

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas como parte dos requisitos para a obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Ms. Kelton Augusto Pontara da Costa.

BAURU
2008

Panzuto, Pietro da Silva
P199d
Desenvolvimento de uma antena modelo YAGI-UDA para análises de sinais wirelles e cálculo do elipsóide de Fresnel / Pietro da Silva Panzuto – 2008.
63f.

Orientador: Prof. Ms. Kelton Augusto Pontara da Costa.
Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) - Universidade do Sagrado Coração - Bauru - SP.

1. Wireless 2. IEEE 3. Antenas 4. Elipsóide de Fresnel I. Pontara da Costa, Kelton Augusto II. Título

PIETRO DA SILVA PANZUTO

DESENVOLVIMENTO DE UMA ANTENA MODELO YAGI-UDA PARA ANÁLISES DE SINAIS *WIRELESS* E CÁLCULO DO ELIPSÓIDE DE FRESNEL.

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas como parte dos requisitos para a obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Ms. Kelton Augusto Pontara da Costa.

Banca examinadora:

Prof. Ms. Kelton Augusto Pontara da Costa _____

Prof. Esp. Henrique Pachioni Martins _____

Prof. Ms. Ronaldo Martins da Costa _____

10 DE DEZEMBRO DE 2008 – BAURU - SP

AGRADECIMENTOS

Aos meus pais, Nicola e Fátima que em nenhum momento de minha vida, deixaram de me apoiar e incentivar a busca de meus objetivos e lutaram com todas as forças possíveis para que eu tivesse a melhor educação social e moral possível.

A minha irmã Nicolle e aos meus amigos, Edvaldo dos Santos, Daniel Goes, Rodrigo Dener, André Pilastri que tiveram a disponibilidade em me ajudar no momento em que mais precisei, e a todos os meus amigos do curso que sempre me incentivaram no desenvolvimento deste projeto.

A minha querida namorada Paula por todos esses anos, de muito carinho, amizade, companheirismo, e sempre com palavras carinhosas e belas me confortava nos momentos mais difíceis.

Ao Professor Mestre Kelton Augusto Pontara da Costa, orientador, professor e amigo que acreditou em mim, incentivou e me cobrou resultados.

E por fim, agradeço a meu Deus, que me guia e fortalece na busca de meus objetivos.

E finalmente, agradeço a todos que me ajudaram direto ou indiretamente no desenvolvimento deste projeto. Muito obrigado a todos vocês!

“Pouca coisa é necessária para
transformar inteiramente uma vida:
amor no coração e sorriso nos lábios.”
Martin Luther King

RESUMO

O estudo sobre a tecnologia *wireless* desperta interesse em muitas pessoas e organizações, devido a sua mobilidade, facilidade de instalação e manutenção; faz com que essas redes sem fio (*wireless network*) tornem-se mais populares. O *Instituto de Engenharia Elétrica e Eletrônica* (IEEE) estabeleceu duas importantes topologias para a rede à Ad-Hoc, utilizado para efetuar a comunicação de ponto a ponto, e a infra-estrutura, que é utilizado para interligar vários hosts através de um AP (*Access Point*), também estabeleceu protocolos de segurança como a WEP, WPA, EAP, WPA2. As antenas, dispositivos com capacidade de irradiar e receber ondas eletromagnéticas tem grande importância no avanço da tecnologia *wireless*, pois, cada tipo de antena possui sua particularidade em relação ao seu uso e alcance no envio do sinal na utilização *outdoor*; é necessário saber as especificações corretas de cada antena e ter o conhecimento da aplicação do elipsóide de Fresnel, que é de grande valia em caso de obstáculos entre duas antenas. O presente estudo aborda o desenvolvimento de uma antena tipo Yagi-Uda, para ser utilizada como objeto de análise para o cálculo do elipsóide de Fresnel bem como o alcance e a freqüência gerada.

Palavras-chave: Wireless, IEEE, Antenas, Elipsóide de Fresnel.

ABSTRACT

Studying about wireless technology attracts many people and organization. Its mobility, easy setting up and maintenance have made these wireless networks become more popular. The Institute of Electrical and Electronics Engineers established two important topology to these networks: AD-HOC, used to establish a point-to-point link between two hosts; and the Infra-Structure, used to setup a link between various hosts trough a Access Point (AP); also established security protocols, like WEP, WPA, EAP, WPA2. The antennas, devices with the ability to irradiate and receive electromagnetic waves, has great importance in advancing wireless technology, therefore, each type of antenna has its particularity in relation to its scope and use in sending the signal in outdoor use; it's necessary to know the right specifications of each antenna and have the knowledge of the application of the Fresnel ellipsoid, which is of great value in the event of obstacles between two antennas. This study discusses the development of a Yagi-Uda antenna type to be used as objects of the analysis to calculate the ellipsoid of Fresnel and the reach and frequency generated.

Keywords: Wireless, IEEE, Antennas, Ellipsoid of Fresnel.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

AES	Advanced Encryption Standard
AP	Access Point
CRC-32	Cyclic Redundancy Check
dBi	Decibel Isotrópico
dBm	Decibel Milliwatt
EAP	Extensible Authentication Protocol
EAP-LEAP	Extensible Authentication Protocol - Lightweight Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
ESSID	Extended Service Set Identifier
GHz	Gigahertz
GPS	Global Positioning System
IAS	Internal Authentication Server
IEEE	Institute and Electrical and Electronics Engineers
IP	Internet Procotocol
IV	Vetor de Inicialização
LAN	Local Área Network)
MAC	Media Access Control
Mbps	Megabits per Second
PEAP	Protected Extensible Authentication Protocol
PSPF	Publicly Secure Packet Forwarding
RADIUS	Remote Authentication Dial-In User Server
RC4	Route Coloniale 4
SSID	Service Set Identifier
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TTAK	Temporal and Transmitter Address Key
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA-PSK	Wi-Fi Protected Access - Pre-Shared Key
WwiSE Word	Wide Spectrum Efficiency

SUMÁRIO

1. INTRODUÇÃO

Hoje muito se fala em novas tecnologias, mas uma das que despertou e ainda desperta interesse em qualquer pessoa ou organização, devido a sua mobilidade proporcionada e a facilidade de instalação e manutenção, é a tecnologia *Wireless*.

É fácil encontrar em qualquer aeroporto, centros de convenções, Universidades, acessos a rede sem fio. Essa tecnologia de fácil acesso é regulamentada pelo IEEE (*Institute and Eletrical and Eletronics Engineers*), que estabelece padrões técnicos nos campos da engenharia, elétrica, eletrônica e computação. Para o uso na transmissão sem fio foi estabelecidos os padrões 802.11a, 802.11b, 802.11g, 802.11i e 802.11n.

O padrão IEEE 802.11 também estabeleceu duas topologias para se utilizar redes sem fio, que foi a Ad-Hoc, utilizada para conexão entre duas maquinas dispensando a utilização de AP, e Infra-Estruturada, utilizada para ligar mais de duas maquinas tendo um AP controlado as conexões.

Este estudo mostra em seu primeiro capítulo uma breve introdução no mundo *wireless*, partindo de sua criação até as atuais utilizações, algumas vantagens e desvantagens, tipos de protocolos disponíveis e as formas de topologias que podem ser aplicadas na estruturação da rede, serão apresentadas também as formas de segurança que podem ser aplicadas, desde as mais simples até as mais complexas utilizando-se de combinações de seguranças existentes para essa rede como *firewall* e controle de acesso, criptografias e controle de MAC.

Ainda neste capítulo serão apresentadas as formas e ferramentas de segurança que podem ser aplicadas nas estruturas das redes wireless, mas também mostra algumas ferramentas que são utilizadas para localizar e varrer as redes sem fio, algumas com recursos que podem ser utilizados para invasão e outras que somente localizam e trazem informações sobre as redes e pontos de acesso.

No terceiro capítulo será descrito o conteúdo sobre antenas e a abordagem dos tipos de antenas usadas na comunicação *wireless*, suas características e utilização, dependendo do modelo da antena.

No quarto capítulo será apresentado o desenvolvimento da antena modelo Yagi-Uda, um circuito digital e o software utilizado para rotacionar a antena, que serviram de base para há análise da elipsóide de Fresnel apresentado no capítulo de resultados obtidos.

1.1 JUSTIFICATIVA

Analisando as vantagens e desvantagens das redes sem fio, será desenvolvido um *hardware* de baixo custo com capacidade de encontrar e analisar redes sem fios e também para aplicação do cálculo da elipsóide de Fresnel. Este estudo será realizado com o intuito de identificar e analisar redes sem fio, através do *hardware* desenvolvido, mas em momento algum este estudo foca em técnicas de invasão e exploração de possíveis falhas nessas redes.

1.2 OBJETIVOS

1.2.1 Objetivo geral

Montar um *hardware* usando um circuito digital controlado pela porta paralela para rotacionar uma antena de fabricação própria, com capacidade de analisar, enviar e receber sinais *wireless*.

1.2.2 Objetivos específicos

Desenvolver uma antena caseira modelo Yagi-Uda para analisar o ganho de sinal e para analisar o alcance do sinal, será aplicado o cálculo do elipsóide de Fresnel, e verificar também à possibilidade de transpor obstáculos.

2 - WIRELESS

2.1 - Historia sobre *wireless*

Rede sem fio (*wireless network*) a cada dia que passa se torna mais popular, principalmente pela sua praticidade e mobilidade oferecidas aos usuários. Nos últimos anos observou um aumento expressivo no número de dispositivos portáteis e suporte a essa tecnologia. Hoje encontramos salas de conferências, aeroportos e hotéis que oferecem como diferencial a seus clientes a possibilidade de acessar a internet a partir de seus dispositivos móveis (RUFINO, 2005 *apud* LACERDA, 2007).

O uso de redes sem fio não se restringe a ambientes públicos, pois seu uso em ambientes corporativos está cada vez mais utilizada como um auxiliar precioso para as LANs (*Local Área Networks*) convencionais, provendo vantagens econômicas e mobilidade aos usuários (DUARTE, 2003 *apud* LACERDA, 2007).

A primeira rede sem fio foi criada na Universidade do Havaí, em 1971 tinha objetivo de conectar computadores nas quatro ilhas que se localizavam os campos sem a utilização de cabos telefônicos. Somente nos anos 80 as redes sem fio ingressaram no ramo da computação pessoal e algumas das primeiras redes sem fio não utilizavam rádio, mas transceptores (uma combinação de transmissor e receptor) infravermelhos, mas tais redes nunca obtiveram sucesso, pois, a sua radiação emitida não tinha forças para atravessar a maioria dos objetos físicos (ENGST & FLSIESHMAN, 2005 *apud* LACERDA, 2007)

Somente no inicio dos anos 90 as redes sem fio utilizando ondas de rádio ganharam destaque, quando os processadores se tornaram capazes de gerenciar dados transmitidos por rádios, mas, somente em 1999 o IEEE (*Institute and Eletrical and Eletronics Engineers*) consolidou o padrão 802.11b, e em 2002 o padrão 802.11a foi ratificado, superando significativamente o 802.11b em velocidade, mas infelizmente, devido à utilização da banda de 5.8 GHz, o 802.11a não é compatível com os dispositivos 802.11b, o que contribui para sua pouca utilização. No final de 2002 surgiu o 802.11g, compatível com o 802.11b e com a mesma velocidade do 802.11a (ENGST & FLSIESHMAN, 2005 *apud* LACERDA, 2007).

As redes *wireless* possuem o mesmo princípio de todos os dispositivos sem fio, ou seja, um transceptor envia sinais através de ondas de radiação eletromagnética, que se propagam a partir de uma antena que recebe sinais propagados nas freqüências corretas e desejadas (ENGST & FLSIESHMAN, 2005 *apud* LACERDA, 2007).

2.2 Vantagens e desvantagens da tecnologia *wireless*

Algumas vantagens da tecnologia *wireless* destacam-se (MATHIAS, 2003);

- Flexibilidade: Estações de trabalho podem se mover sem problema, desde que não ultrapasse a área de cobertura;
- Velocidade e Facilidade: Redes sem fio podem ser instaladas e configuradas rapidamente;
- Redução do Custo Agregado: Redes sem fio, por serem de fácil instalação são também de fácil expansão, tendo também manutenção reduzida, sendo mais compensador que as redes cabeadas.
- Diversas Topologias: Essas redes podem ser configuradas em diversas topologias e podem ser alteradas a qualquer momento.

Algumas desvantagens da tecnologia *wireless* destacam-se (MATHIAS, 2003);

- Qualidade de serviço: a qualidade de transmissão ainda é inferior as redes cabeadas, pois algumas razões são as pequenas bandas, limitações de rádio transmissão e taxas de erros por interferência;
- Custo: Preço de equipamento para redes *wireless* tem um custo elevado comparados com as cabeadas;
- Segurança: É um dos principais fatores que atrapalha o crescimento dessa tecnologia, pois a mesma está mais suscetível a interceptação não desejada e interferências por alguns equipamentos de alta tecnologia, causando perda de dados e altas taxas de erros na transmissão;
- Baixa transferência de dados: Mesmo com o avanço das taxas de transmissão da rede sem fio, a mesma ainda é baixa comparada com a cabeada em uma situação que exija alto grau de processamento e transmissão.

2.3 Padrões IEEE 802.11

O IEEE é uma associação sem fins lucrativos de profissionais técnicos com o objetivo de estabelecer padrões técnicos nos campos das engenharias, elétricas, eletrônicas e computação. Um dos padrões mais conhecidos é o 802.11 que apresenta especificações que define o uso da comunicação entre dispositivos de uma rede sem fio (ENGST & FLSIESHMAN, 2005 *apud* LACERDA, 2007).

A seguir segue os principais padrões do IEEE 802.11 com suas semelhanças e diferenças.

2.3.1 Padrão IEEE 802.11b

Esse padrão surgiu entre 1999 a 2001, foi muito bem sucedido, pois ainda hoje temos estruturas em funcionamento com este dispositivo, pois o mesmo foi o mais popular e o que mais apresenta ferramentas para segurança e administração. Esse padrão oferece transmissão de 11 Mbps (*Megabits per Second*) com um *throughput* real de 5 Mbps, operando na freqüência de 2,4 GHz (*Gigahertz*).

2.3.2 Padrão IEEE 802.11a

Esse padrão surgiu em 2002 com sua principal característica o aumento da velocidade para no máximo 54 Mbps com um *throughput* real de 25 Mbps e uma diferença e que este padrão operar na faixa de 5,8 GHz, com menos concorrência (RUFINO, 2005 *apud* LACERDA, 2007).

Uma vantagem desse padrão é que o mesmo possui 12 canais não sobrepostos, permitindo assim que mais pontos de acesso atuem em um mesmo ambiente sem interferências entre eles (ENGST; FLSIESHMAN, 2005 *apud* LACERDA, 2007).

Uma desvantagem é que esse padrão não se comunica com o padrão 802.11b, por terem suas freqüências diferentes.

2.3.3 Padrão IEEE 802.11g

Esse padrão opera na velocidade de 54 Mbps, com um *throughput* real de 20 Mbps, utiliza freqüências do 802.11b e trabalha em ambientes com padrões (b e g).

2.3.4 Padrão IEEE 802.11i

Esse padrão foi criado em 2004, com a definição de mecanismos de autenticação e privacidade, podendo ser implementado nos padrões existentes, o mesmo inclui o WPA (W*i-fi Protected Access*) como objetivo de oferecer soluções seguras e eficientes.

2.3.5 Padrão IEEE 802.11n

Esse padrão é conhecido como WwiSE (*Word Wide Spectrum Efficiency*), e está em desenvolvimento, com o objetivo de oferecer um aumento de velocidade em torno de 100 a 500 Mbps.

Padrão	**Freqüência**	**Throughput Bruto/real**	**Compatível com o 802.11b**	**Ano em que se tornou real**	**Tendência à adoção**
802.11b	2,4 Ghz	11 Mbps/ 5 Mbps	Sim	1999	Diminuindo em computadores, avançando na eletrônica mais barata
802.11a	5 Ghz	54 Mbps/ 25 Mbps	Não	2002	Empresas adotando lentamente, sem consumidores
802.11g	2,4 Ghz	54 Mbps/ 20 Mbps	Sim	2003	Avançando em todos os lugares

Tabela 1 - Visão dos padrões IEEE 802.11
Fonte: ENGST & FLSIESHMAN (2005 *apud* LACERDA, 2007)

2.4 Topologia

Similares as de redes *Ethernet*, as redes *wireless* compartilham a comunicação entre todas as estações conectadas a um mesmo ponto de acesso ou concentrador. Sendo assim quanto maior a quantidade de usuários conectados a essa rede, menor será a banda disponível para cada um, com isso o tráfego fica visível para todos os usuários conectados, ou seja, similar a rede cabeada (RUFINO, 2005 *apud* LACERDA, 2007).

Com a organização do padrão IEEE 802.11 fomos estabelecidos dois modos distintos de operação: *Ad-Hoc* e infra-estrutura.

2.4.1 Ad-Hoc

A Figura 1 apresenta a topologia *Ad-Hoc*, em que todos os computadores trocam informações diretamente, sem necessidade de estações ou AP (*Access Point*) para se interligarem, esse modo é similar a uma rede ponto a ponto cabeada, mas no modo sem fio

essas informações são mais vulneráveis por serem facilmente interceptadas, pois, não existe um AP para uma segurança adequada.

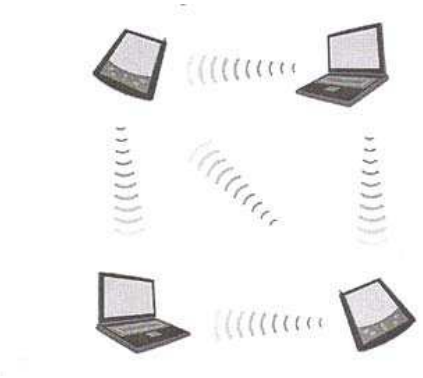

Figura 1 - Topologia modelo Ad-Hoc
Fonte: RUFINO (2005 *apud* LACERDA, 2007)

2.4.2 Infra-Estrutura

A Figura 2 apresenta a topologia Infra-estrutura, que é composta por um AP e todo tráfego da rede sem fio passe por ele, podendo efetuar controles como autorizações, autenticações, controle de banda, filtros de pacotes e criptografias.

Figura 2 - Topologia modelo infra-estrutura
Fonte: RUFINO (2005 *apud* LACERDA, 2007).

2.5 Criptografia

A criptografia é uma forma de proteção dos dados para serem trafegado na rede, pois os mesmo ficarão fora de uma ordem lógica e entendível (GIMENES, 2005 *apud* LACERDA, 2007). Caso alguma tentativa de interceptação desses dados seja praticada dificilmente será compreendida.

Segundo Aguiar (2005 *apud* LACERDA, 2007) criptografia é usada de forma a garantir:

- Sigilo: Só terão acesso às informações usuários autorizado;
- Integridade da informação: garantia da informação correta;
- Autenticidade do usuário: é a forma de verificar se a identidade do usuário, ou dispositivo que está efetuando a comunicação.

2.5.1 WEP (*Wired Equivalent Privacy*)

O protocolo WEP foi criado para fornecer uma segurança no início da criação das redes sem fio, hoje ele e o mais disseminado e está presente em todos os equipamentos de padrão *wireless*.

Segundo Rufino (2005 *apud* LACERDA, 2007) esse protocolo utiliza-se de algoritmos simétricos, ou seja, existe uma chave que deve ser compartilhada entre as estações de trabalho e o ponto de acesso, para cifrar e decifrar as mensagens transmitidas nessa rede *wireless*.

Esse protocolo trabalha na camada de enlace de dados e se baseia no método criptográfico RC4 (*Route Coloniale* 4) da RSA, que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (*secret shared key*) de 40 ou 104 bits. O IV é concatenado com a *secret shared key* para formar uma chave de 64 ou 128 bits que é usada para fazer a criptografia. O WEP utiliza o CRC-32 (*Cyclic Redundancy Check*) que serve para calcular o *checksum* da mensagem, que é incluso nos pacotes, visando à segurança dos dados. O receptor ao analisar o pacote recalcula o *checksum* para garantir que as mensagens não foram alteradas no seu percurso (GIMENES, 2005 *apud* LACERDA, 2007).

2.5.2 WPA (Wi-Fi Protected Access)

Devido alguns problemas de segurança do protocolo WEP, surgiu o WPA de uma aliança ente a *Wi-fi Alliance* e o IEEE, pois, possui melhores mecanismos de autenticação, privacidade, controle de integridade que fornecendo um tratamento melhor na segurança do que o WEP. O WPA não é compatível com os *hardwares* que utilizam o WEP, por isso em caso de migração é necessária à atualização do *firmware* dos dispositivos sem fio, sem ter à necessidade de efetuar alteração na estrutura física (AGUIAR, 2005 *apud* LACERDA, 2007).

O protocolo WPA, diferente do WEP não aceita a topologia de conexão *Ad-Hoc*, portanto sem a utilização de um ponto de acesso, nesse tipo de rede, ela não se beneficia de mecanismo de proteção que foram incluídas no WPA em sua primeira versão.

Esse protocolo trabalha de duas formas. A primeira é com o objetivo de substituir o WEP, criptografando os dados e garantindo sua privacidade. A segunda é a autenticação dos usuários, utilizando os padrões 802.1x e EAP (*Extensible Authentication Protocol*).

Rufino (2005 *apud* LACERDA, 2007) ressalta que o WPA, utiliza dois tipos de protocolos para criptografar as informações, uma esta voltada para pequenas redes que utilizam uma chave previamente compartilhada (Pré-shared Key) ou WPA-PSK, que é o responsável por fazer o reconhecimento do equipamento pelo ponto de acesso. O outro é conhecido como infra-estrutura, que necessita da utilização de um servidor de autenticação RADIUS (*Remoto Authentication Dial-In User Server*).

O método de chave compartilhada é feita manualmente, semelhante ao WEP, na qual tal atitude se restrinja as pequenas redes onde todos os participantes estão acessíveis na maior parte do tempo (GIMENES, 2005 *apud* LACERDA, 2007).

No WPA possui o protocolo TKIP (*Temporal Key Integrity Protocol*), que é responsável pela troca dinâmica das chaves, sendo que no WEP as chaves eram estáticas e possuía seu IV de apenas 24 bits e nesse protocolo trabalha com 48 bits (GIMENES, 2005 *apud* LACERDA, 2007).

Neste protocolo se utiliza uma chave base de 128 bits denominada TK (*Temporal Key*), que é combinada com o endereço MAC do transmissor, criando uma chave chamada TTAK (*Temporal and Tramsmitter Adres Key*), que é combinada com o IV do RC4 criando chaves diferentes para cada pacote transmitido (AGUIAR, 2005 *apud* LACERDA, 2007).

O TKIP fornece uma chave diferente para cada estação da rede para se comunicar com o ponto de acesso, quando a chave é gerada com o endereço MAC das estações. Esse protocolo TKIP pode também ser programado para alterar o IV para cada pacote, podendo ser definido por sessão ou por período, dificultando assim a obtenção que trafegam nessa rede (AGUIAR, 2005 *apud* LACERDA, 2007).

2.5.2.1 EAP (Extensible Authentication Protocol)

Esse protocolo EAP permite vários métodos de autenticação com a possibilidade de certificação digital, e o mesmo pode ser usado com outras tecnologias, com um servidor de autenticação RADIUS.

Segundo Aguiar (2005 *apud* LACERDA, 2007) o 802.11 utilizam-se do protocolo EAP de forma a controlar como as autenticações serão feitas na rede. Ele possibilita a escolha de um método de autenticação como senhas, certificações digitais ou *tokens* de autenticação. O autenticador não necessita entender o método de autenticação, simplesmente envia os pacotes e o EAP do usuário a ser autenticado para o servidor de autenticação e vice e versa.

Gimenes (2005 *apud* LACERDA, 2007) aborda que é possível configurar pontos de acesso como clientes RADIUS para que seja enviadas solicitações de acesso e mensagens de contas para os servidores de autenticação que executam IAS (*Internal Authentication Server*), que faz a autenticação dos usuários e dispositivos, controlando o acesso à rede por meio de diretivas de acesso remoto centralizado.

Grégio (2005 *apud* LACERDA, 2007) aborda que existem vários tipos de EAP que dão suporte a diversos métodos de autenticação:

- EAP-LEAP (*LightWeight EAP*): Desenvolvido pela CISCO, utiliza-se método de login e senha para enviar a identidade do usuário ao servidor de autenticação.
- EAP-TLS (*Transport Layer Security*): Especificado na RFC 2716, utiliza o certificado X.509 para autenticação.
- PEAP (*Protected EAP*): Utiliza-se de autenticação baseado em senha e o servidor de autenticação deve possuir um certificado digital, mas não exige certificados nos clientes, esse método de autenticação foi adotado pela Microsoft no Windows XP e Windows Server 2003.

2.5.3 WPA2 ou 802.11i

Esse protocolo foi ratificado pelo IEEE em 2004, tratando de um produto disponível por meio da *Wi-fi Alliance.* A diferença entre o WPA2 e o WPA e sua criptografia utilizada. O WPA utiliza o TKIP com o RC4, já o WPA2 utiliza o AES (*Advanced Encryption Standard*) em conjunto com o TKIP com chave de 256 bits, que é um método de criptografia muito mais poderoso. O AES permite a utilização de chaves de 128, 192 e 256 bits, que constituem assim uma ferramenta poderosa de criptografia. A chave de 256 bits no WPA2 é padrão. A utilização do AES necessita de um novo *hardware*, que seja capaz de realizar o processo criptográfico, pois em dispositivos mais recentes é necessário possuir um co-processador para realizar os cálculos da criptografia (AGUIAR, 2005 *apud* LACERDA, 2007).

2.6 Segurança

Com a flexibilidade e mobilidade oferecida aos usuários de rede sem fio, um fator fundamental é a implementação de uma segurança da informação. A utilização de estratégias de segurança eficaz e imprescindível, pois há a necessidade de diminuir os riscos de acessos por pessoas indevidas a essa rede. Para conseguir um nível de segurança é preciso implementar controles externos aos equipamentos, como configurações adequadas, criptografia, autenticação e monitoramento dos acessos à rede sem fio são indispensáveis. (JUNIOR et al, 2004 *apud* LACERDA, 2007).

2.6.1 Configuração do *Access Point*

Inicialmente para manter a rede mais segura, é necessário desabilitar o SSID (broadcast SSID), para assim esconder o nome da rede, fazendo que somente os clientes autorizados enxerguem o nome da rede, e sempre mudar o ESSID padrão dos equipamentos, e no caso de troca desse nome, sempre buscar não revelar o nome do equipamento e o nome da empresa, a fim de garantir uma segurança maior. Mais uma mudança importante a se fazer é que os pontos de acesso recusem solicitações com o SSID igual a “ANY”, pois é uma situação na qual o cliente busca conectar-se em qualquer ponto de acesso, mas como é impossível ter certeza de que seja um cliente autorizado, essa solicitação deve ser evitada (RUFINO, 2005 *apud* LACERDA, 2007).

Outra segurança é a alteração do endereço MAC do equipamento, fazendo com que um possível atacante não descubra o fabricante do equipamento, pois o mesmo está relacionado ao endereço MAC.

Segundo Rufino (2005 *apud* LACERDA, 2007) muitos *access point* permitem configuração via HTTP e TELNET, recomenda-se desabilitar essas opções do lado de acesso a rede sem fio, evitando que informações como usuário e senha sejam interceptadas por um possível atacante, sendo somente aceitas tais configurações, pela rede cabeada, na qual um atacante terá maior dificuldade de acesso.

Essas medidas de proteção apresentadas, usadas isoladamente não apresentam um bom nível de segurança, sendo necessário serem combinadas com outras medidas, para que assim, se tornem eficazes.

2.6.2 Defesas nos clientes

Um mecanismo de grande importância e o PSPF, que faz o papel de bloqueio entre dois usuários dentro de uma rede, ou seja, evita que um ataque o outro, mas esse método não impede que os pacotes sejam capturados. Sendo assim, este mecanismo de segurança deve ser aplicado de forma a combinar com outras medidas de segurança, visando à privacidade do usuário (RUFINO, 2005 *apud* LACERDA, 2007).

2.6.3 Métodos de Autenticação

O método de autenticação do padrão IEEE 802.11 são componentes importantes para aumentar o nível de segurança da rede sem fio. O servidor RADIUS é um componente muito utilizado para fazer autenticação.

Aguiar (2005 *apud* LACERDA, 2007) ressalta que em um processo de autenticação 802.11 existem 3 participantes:

- O Suplicante: usuário
- Servidor de autenticação: sistema de autenticação RADIUS, que realizará a autenticação do usuário cadastrado.
- Autenticador: mediador na transação entre o suplicante e o servidor de autenticação. Geralmente é o AP.

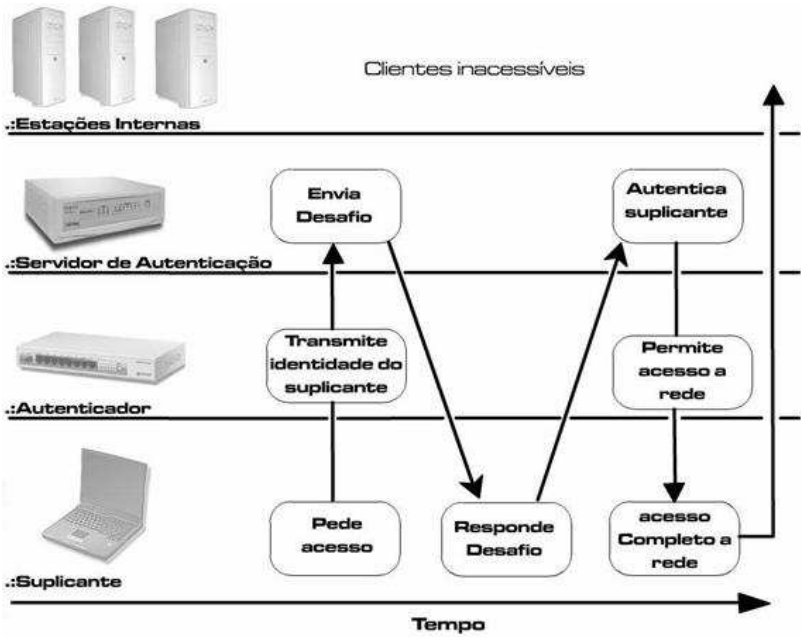

Figura 3 - Simulação de acesso a rede sem fio
Fonte: GIMENES (2005 *apud* LACERDA, 2007)

Na Figura 3 a maquina cliente (suplicante) pede o acesso para o autenticador o qual transmite uma identidade do cliente para o servidor de autenticação, que por sua vez inicia um desafio para o cliente. Ao responder o desafio o servidor autentica o usuário para que o autenticador libere o acesso à rede (GIMENES, 2005 *apud* LACERDA, 2007).

Segundo Aguiar (2005 *apud* LACERDA, 2007) o padrão 802.11x utiliza o protocolo EAP para gerenciamento da autenticação mútua que será feita na rede, possibilitando a escolha de um método específico de autenticação a ser utilizado, como senhas, certificados ou *tokens* de autenticação. O autenticador não precisa entender o método de autenticação, ele simplesmente repassa os pacotes EAP do suplicante para o servidor de autenticação e vice-versa.

2.6.4 *Firewalls*

Os *firewalls* são componentes fundamentais a qualquer rede, pois garantem a segurança e controle dos dados de entrada e saída baseado em configurações previamente estabelecidas (AGUIAR, 2005 *apud* LACERDA, 2007).

Segundo Junior (et al 2004 *apud* LACERDA, 2007) o *firewall* também pode assumir um papel de *gateway* entre redes, podendo um ser uma rede sem fio e o outro LAN, fazendo de tal forma que as redes fiquem isoladas, evitando que pessoas não autorizadas tenham acesso à outra rede, bloqueando o tráfego da LAN para a *wireless* e da *wireless* para a LAN.

Outra funcionalidade do *firewall* e a capacidade de analisar informações sobre as conexões, alterações suspeitas, analise do conteúdo dos pacotes que permite e garante uma segurança maior na rede (JUNIOR *et al*, 2004 *apud* LACERDA, 2007).

2.6.5 Senhas descartáveis

Um administrador de uma rede, após aplicar em seus equipamentos, tecnologias de *firewall*, antivírus, anti-spyware, é interessante que forneça mecanismos de autenticação baseados em senhas descartáveis, *tokens* e cartões processados (*smartcards*) ou fazer uso de dispositivos biométricos. Senhas descartáveis são as mais simples de implantação, pois permite que o usuário informe senhas diferentes a cada acesso, dificultando a captura da senha no caso de uma filtragem (RUFINO, 2005 *apud* LACERDA, 2007).

Esse processo de criação da senha descartável inicia quando o servidor envia uma informação como desafio, esse desafio é recebido pelo cliente, o qual irá concatenar com a

senha secreta, após essa concatenação o valor resultante será aplicado a uma função de criptografia, gerando a senha descartável a ser utilizada pelo cliente em cada seção.

2.6.6 Certificado digital

Aguiar (2005 *apud* LACERDA, 2007) afirma que os certificados é uma forma de associar a identidade digital de alguém a um par de chaves eletrônicas sendo elas privadas e públicas que usadas em conjunto servem para comprovar a identidade da pessoa.

Estes certificados são os métodos mais seguros, principalmente quando armazenados em dispositivos processados como *tokens* ou cartões, que segundo Aguiar (2005 *apud* LACERDA, 2007) um certificado digital contém três elementos:

- Informação de atributo: informação sobre o objeto que é certificado se for uma pessoa o seu nome, nacionalidade, etc.
- Chave de informação pública: essa é a chave pública na Autoridade Certificadora. O certificado atua para associar a chave pública à informação de atributo.
- Assinatura da Autoridade Certificadora: a autoridade validara os dois primeiros elementos.

2.6.7 Tokens e Smartcards

Tokens e *Smartcards* são dispositivos físicos utilizados para armazenar informações como chaves privadas e senhas, na tentativa de impedir uma possível captura dessas informações na rede. O *token* é um pequeno dispositivo, similar a um *pendrive*, como mostrado na Figura 4 é utilizado para armazenar identificação digital e dados para a autenticação. O *Smartcard* é um dispositivo portátil (cartão) que possui uma memória não volátil. Este dispositivo fornece um nível alto de segurança (AGUIAR, 2005 *apud* LACERDA, 2007).

Figura 4 - *Token*
Fonte: AGUIAR (2005 *apud* LACERDA, 2007)

2.6.8 Detecção de ataques e monitoramento

Rufino (2005 *apud* LACERDA, 2007) aborda que independente da rede cabeada e sem fio, elas estão expostas as possíveis ameaça e invasões, mas para que isso não ocorra alguns investimentos em segurança e monitoramento deve ter prioridade, pois, são eles que irão detectar pontos de falha e apresentar como determinado ataque ocorreu ou foi bloqueado.

Segue abaixo algumas ferramentas para análise e proteção das redes sem fio:

- IDS;
- Garuda;
- Kismet;
- Snort;
- Honey pots e Honey nets
- Air Magnet;
- Air Strike;

2.7 Vulnerabilidade

Vulnerabilidade entende-se por falhas ou falta de segurança das quais pessoas mal intencionadas possam se valer para invadir, subtrair, acessar ilegalmente, adulterar e destruir informações confidenciais, além de poder comprometer, corromper e inutilizar o sistema. Mesmo com o avanço da tecnologia nos dias de hoje, os riscos se apresentam de forma significativa, fazendo com que sejam analisados e minimizados na estruturação e implantação de uma rede sem fio.

2.7.1 Segurança física

Rufino (2005 *apud* LACERDA, 2007) ressalta que os posicionamentos das antenas devem ser cuidadosamente estudados, para não comprometer o bom funcionamento da rede e não facilitar o acesso indevido de pessoas ou outros tipos de ataques.

Um item que se deve verificar e o padrão utilizado e a potência dos equipamentos, pois o padrão 802.11a atinge uma distância menor que o 802.11b ou 802.11g e a maiorias dos pontos de acesos possibilitam selecionar valores intermediários de potência, no caso de o administrador da rede achar necessário poderá receber ou enviar sinal a distância não prevista pelo teste de propagação do sinal, isso dependendo da qualidade e da segurança que será

aplicada a estrutura, pois, em uma regra geral quanto mais estiver no centro da estrutura melhor será aproveitado no sinal pelas estações (GIMENES, 2005 *apud* LACERDA, 2007).

2.7.2 Mapeamento de ambiente

Fazer o mapeamento do ambiente é a primeira ação realizada pelo atacante, pois neste procedimento é possível obter o maior número de informações sobre a rede, adquirindo detalhes que lhe permitirão atacar de forma precisa e com menos riscos de ser identificado (RUFINO, 2005 *apud* LACERDA, 2007).

Aguiar (2005 *apud* LACERDA, 2007) diz que o mapeamento passivo é aquele onde o atacante obtém informações como IP, sistema operacional, SSID. Com posses destas informações o atacante pode selecionar o equipamento de seu interesse e que esteja vulnerável.

A utilização de GPS é uma possibilidade de localizar e identificar características de redes sem fio, podendo dessa forma gerar mapas com um grau de precisão do alvo a ser atacado (RUFINO, 2005 *apud* LACERDA, 2007).

A ferramenta Cheops-ng é utilizada para um mapeamento ativo pode ser tão completo quanto o atacante deseja, pois, não somente identifica em forma de gráfico os componentes, mas informa o sistema operacional, tipos e modelos de equipamentos e serviços em tempo real como apresentado na Figura 5 (CHEOPS-NG, 2008 *apud* LACERDA, 2007).

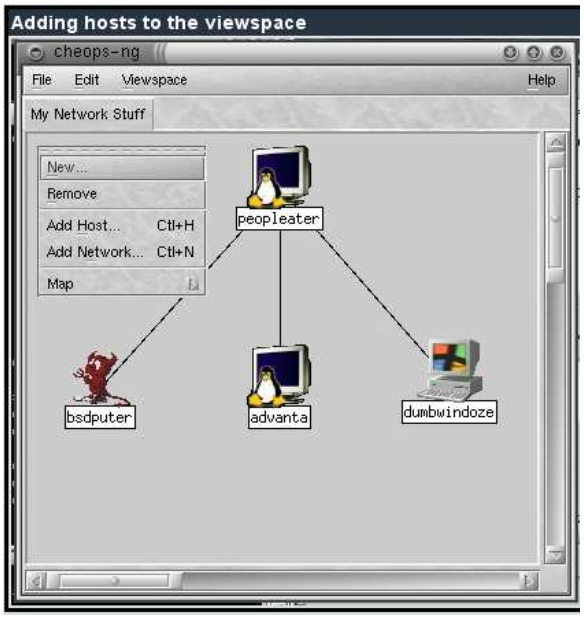

Figura 5 - Mapeamento
Fonte: CHEOPS-NG (2008 *apud* LACERDA, 2007).

2.7.3 Configurações

Rufino (2005 *apud* LACERDA, 2007) ressalta que existem muitos motivos para que um atacante busque o acesso a uma determinada rede como ter acesso a internet ou promover ataques a outros lugares, capturar algum tipo de informação como senhas de sites e bancos e dentre outros.

2.7.3.1 Configurações aberta

Esse tipo de configuração aberta se baseia em enviar através do ponto de acesso o SSID da rede, ou seja, aceita conexão de qualquer dispositivo, cujas compatibilidades de padrão sejam atendidas, muito comuns encontrar locais onde o ponto de acesso foi mal configurado ou configurado de forma a permitir o fácil acesso por parte de qualquer usuário (GIMENES, 2005 *apud* LACERDA, 2007).

2.7.3.2 Configurações fechadas

Esse tipo de configuração o ponto de acesso não envia o SSID, sendo somente aceito conexão de usuários que saibam o SSID da rede, com essa atitude os atacantes são forçados a varrer o sinal para localizar o SSID correto para enfim conectar-se a rede (GIMENES, 2005 *apud* LACERDA, 2007).

2.8 Vulnerabilidades WEP e WPA

Os protocolos WEP e WPA oferecem segurança as redes sem fio, mas como as ondas de radiofreqüência se propagam pelo ar, se tornam passíveis de captura, caso não estejam devidamente criptografadas, seu tráfego pode ser facilmente copiado.

Segundo Duarte (2003 *apud* LACERDA, 2007) o protocolo WEP utiliza-se de uma chave única e estática conhecida por ambos os lados da comunicação, em caso de troca da chave, o processo se torna inviável, pois dependendo do tamanho da rede todas as máquinas que fazem parte desta precisarão ser trocadas e quanto mais pessoas tiverem conhecimento dela a mesma se torna insegura.

Outro problema que o protocolo WEP apresenta é o pequeno IV, que não é suficiente para evitar a repetição das chaves e geralmente como é aplicado em uma rede com grande

volume de tráfego e o IV é transmitido em texto puro, sem criptografia facilita algum tipo de ataque ou invasão (WARCHALKING, 2006).

Tews (*et al* 2007 *apud* LACERDA, 2007) afirma que é possível a quebra de uma chave WEP de 104 bits em menos de sessenta segundos.

O protocolo WAP tem características de segurança superiores ao WEP, mas o mesmo está sujeito a ataques como de força bruta (*brutal force*) ou dicionário, e quando o atacante testa senhas em seqüências ou palavras comuns, e outro problema é o armazenamento das chaves nos clientes e nos concentradores (RUFINO, 2005 *apud* LACERDA, 2007).

2.9 Ferramentas e técnicas de ataque

Gimenes (2005 *apud* LACERDA, 2007) ressalta que os ataques às redes sem fio não são diferentes dos aplicados às redes cabeadas, outros ataques tiveram que sofrer algumas modificações para conseguirem melhores resultados. Segue algumas ferramentas e técnicas de ataque utilizadas.

2.9.1 *Access Point Spoofing* (Associação Maliciosa)

Essa associação maliciosa é quando o atacante se passa por um *Access Point*, iludindo outro sistema de maneira que acreditem que estão conectados a uma WLAN real (DUARTE, 2003 *apud* LACERDA, 2007).

2.9.2 ARP *Poisoning*

Este é um ataque de camada de enlace de dados que somente pode ser disparado quando o atacante já está conectado na mesma rede local da vítima. Este ataque pode ser disparado de uma estação da WLAN a uma estação guiada, sendo assim, o ataque não fica restrito apenas às estações sem fio (DUARTE, 2003 *apud* LACERDA, 2007).

2.9.3 MAC *Spoofing*

É quando o atacante se apodera de um endereço MAC de um cliente da rede, e utiliza-se disto para poder participar da mesma rede, sabendo que esses equipamentos sem fio têm a possibilidade da troca do endereço físico.

2.9.4 *Wardriving*

Esse tipo de ataque conta com a ajuda de um GPS para mapear o *Access Point.*

Aguiar (2005 *apud* LACERDA, 2007) afirma que neste tipo de ataque, equipamentos são configurados para encontrar tanto as redes sem fio como as redes que estiverem na abrangência do equipamento.

2.9.5 *Warchalking*

Esse tipo de ataque utiliza-se de equipamentos da *Warchalking* para fazer a localização e marcação das redes através de pichações de muros e calçadas com símbolos específicos. Estes símbolos são usados para guiar outros atacantes, informando também as características da rede (DUARTE, 2003 *apud* LACERDA, 2007).

Segundo Duarte (2003 *apud* LACERDA, 2007) existe grupos organizados para *warchalking* que utilizam os próprios símbolos para marcar as redes na tentativa de mantê-las em segredo.

Alguns símbolos utilizados pelo atacante podem ser observados na Figura. 6.

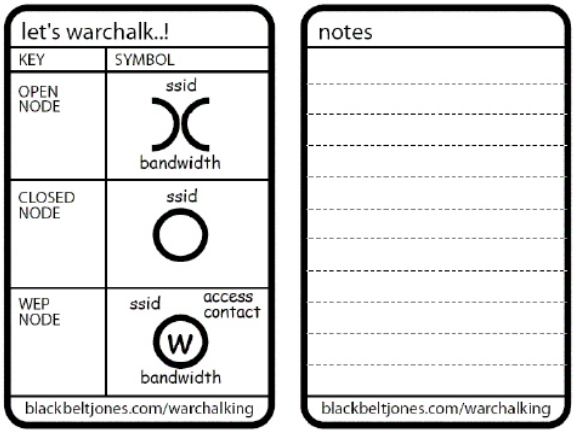

Figura 6 - Exemplo de *Warchalking*
Fonte: DUARTE (2003 *apud* LACERDA, 2007)

O primeiro símbolo identifica uma rede sem fio aberta, descrevendo o seu SSID e sua largura da banda.

O segundo símbolo identifica uma rede fechada, descrevendo apenas o SSID.

O terceiro símbolo identifica uma rede protegida pelo protocolo WEP junto com o SSID, o *Access contact* (chave WEP utilizada) e a largura da banda (velocidade da rede).

2.9.6 Ferramentas de ataque

Rufino (2005 *apud* LACERDA, 2007) ressalta que ao contrário das redes cabeadas, onde os fabricantes e modelos dos equipamentos não influenciam o comportamento de uma ferramenta de ataque, em redes *wireless* a maior parte das ferramentas depende diretamente dos equipamentos específicos e/ou modelos de placa de rede ou até do protocolo utilizado.

A seguir algumas ferramentas gratuitas de ataques.

2.9.6.1 Airtraf

Esta ferramenta conforme apresentada na Figura 7 coleta grandes informações como clientes conectados e serviços atualizados em tempo real, ela também possibilita a quebra da chave WEP no padrão 802.11b e seu monitoramento é de forma passiva (RUFINO, 2005 *apud* LACERDA, 2007).

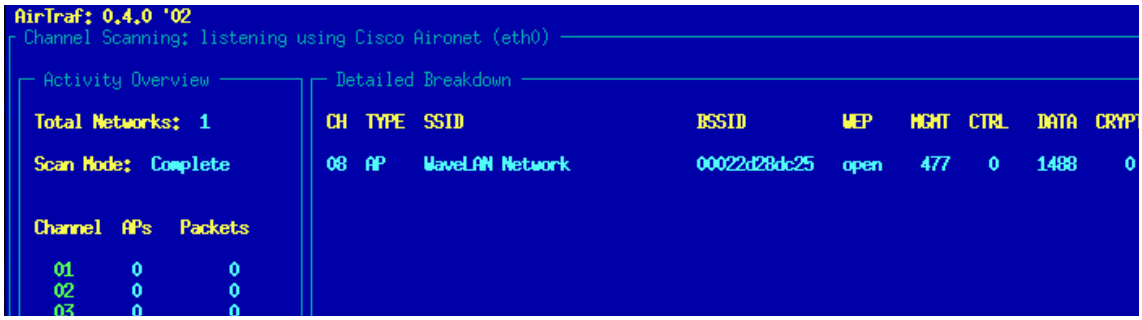

Figura 7 - Ferramenta Airtraf
Fonte: AIRTRAF (2002 *apud* LACERDA, 2007).

2.9.6.2 Netstumbler

Essa ferramenta foi uma das primeiras disponíveis para verificar e identificar rede sem fio para ambiente Windows. Ela permite integração com GPS, possibilitando a criação de mapas precisos e também permite verificar redes em todos os padrões comerciais (RUFINO, 2005 *apud* LACERDA, 2007).

O Netstumbler apresentado na Figura8, não captura o tráfego da rede e não efetua quebra da chave WEP.

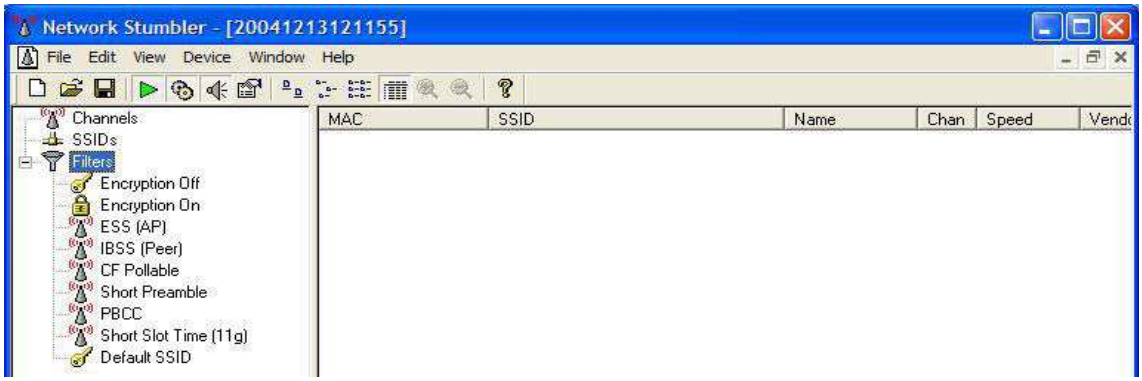

Figura 8 - Ferramenta Netstumbler
Fonte: NETSTUMBLER (2008 *apud* LACERDA, 2007)

2.9.6.3 Kismet

Esta ferramenta possui uma atualização constante em suas funcionalidades. O Kismet pode ser utilizado para o mapeamento de redes, captura de tráfego e localização por GPS. Toda análise do Kismet pode ser armazenada em arquivo ou visto em tempo real (KISMET, 2007 *apud* LACERDA, 2007).

Essa ferramenta como apresentado na Figura 9 não apresenta quebra de chave WEP.

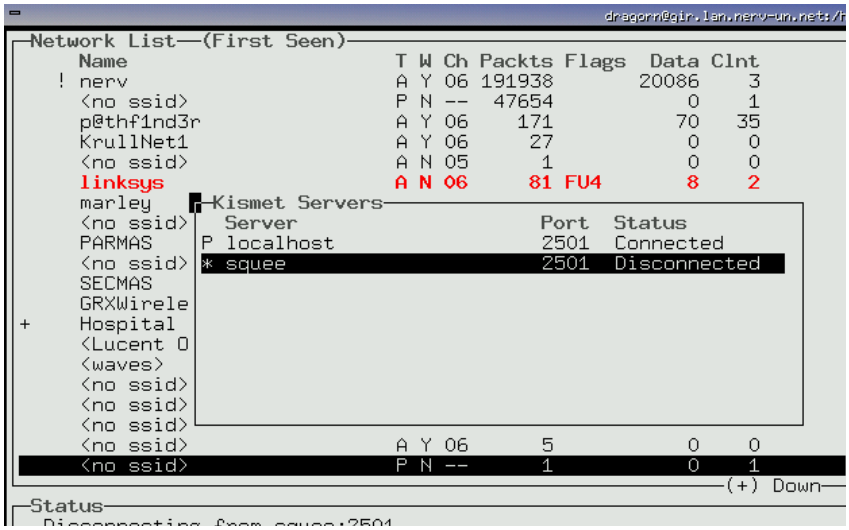

Figura 9 – Ferramenta Kismet
Fonte: KISMET (2007 *apud* LACERDA, 2007)

2.9.6.4 AirJack

Essa ferramenta apresenta um ataque o qual simula ser um ponto de acesso interposto aos oficiais, sendo assim passa a receber todo o tráfego da rede.

2.9.6.5 Ferramentas para quebra de chaves WEP

Algumas ferramentas oferecem grandes recursos para quebra dessa chave, utilizando-se também de combinação de força bruta e ataques de dicionário, mas algumas podem ser destacadas como a *Airsnort, WepCrack, WepAttack, AirCrack.*

3. ANTENAS

Antenas podem ser definidas como um dispositivo com a capacidade de radiar e receber ondas eletromagnéticas. Essa característica de radiação difere-se a cada tipo de antena, pois dependem da forma física e dos materiais utilizados em sua construção, fatores fundamentais na distribuição dos campos elétricos e magnéticos (SILVA, 2006).

3.1 Conceituando antenas

Segundo Gomes (1985) antenas consistem de um dispositivo equipado de condutores, geralmente dispostos em pares, sendo alimentados por uma linha de transmissão, denominada de dipolos, que é a capacidade de produzir ondas eletromagnéticas no espaço livre a partir de uma corrente elétrica variável no tempo, onde por sua vez gera um campo magnético variável no tempo induzindo assim a formação de um campo elétrico variável no tempo, podendo ser observado na Figura 10.

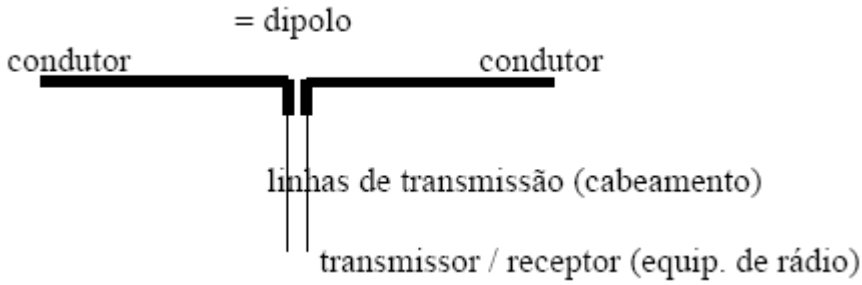

Figura 10 - Esboço de uma antena comum
Fonte: MAIA (2000)

As antenas possuem um sentido de “mão-dupla” onde é possível transmitir e receber ondas e a unidade de grandeza física (MAIA, 2000).

3.2 Características básicas das antenas

Segundo Maia (2000) algumas características que compreendem a construção e a aplicação das antenas buscando um melhor desempenho e seu comportamento satisfatório tanto para ambientes internos como externos, alguns parâmetros são dispostos:

- Diagramação de Irradiação
- Ângulo de Abertura

- Eficiência
- Diretividade
- Ganho
- Relação Frente-Costa
- Resistência a Irradiação
- Largura de Faixa
- Potencia Recebida
- Polarização
- Área Física x Área Utilizada
- Ruídos Incidentes nos Sistemas de Antenas RF

3.3 Antena Yagi-Uda

A antena Yagi foi apresentada no Japão pelo engenheiro S.Uda, sendo introduzida no mundo ocidental pelo engenheiro H. Yagi, logo conhecida como Yagi-Uda. Este tipo de antena utiliza-se dos mesmos princípios do dipolo de meia-onda, e vários dipolos curtos, colocados em seqüência afim de dar direção e radiação desejada (MAIA, 2000).

Esta antena foi chamada de antena radiante, pois seu conjunto de elementos paralelos em ordem, feito usualmente de alumínio, tubo ou aço inoxidável em forma de varetas, sendo um ou mais destes elementos é condutor, e outros são parasitados. Estes elementos estão alinhados em algum plano podendo ser orientado horizontalmente, verticalmente ou inclinado (GOMES, 1985).

3.4 Tipos de antenas

Antenas na tecnologia *wireless* são de extrema importância, pois a mesma é a responsável pela velocidade e qualidade de transmissão dos dados. As antenas que por padrão são utilizadas nos pontos de acesso apresentam uma área de cobertura de 30 metros em espaços fechados onde existem paredes e outros obstáculos e em torno de 150 metros em áreas abertas, mas como o avanço tecnológico é possível utilizar-se de antenas mais sofisticadas para melhorar seu desempenho de transmissão de dados (MORIMOTO, 2008).

As antenas padrões dos pontos de acessos são chamadas de dipolo ou ominidirecionais, pois sua irradiação segue em todas as direções como apresentado na Figura

11, permitindo a conexão em qualquer ponto em volta do ponto de acesso, ou seja, cobre uma área de 360º (MORIMOTO, 2008).

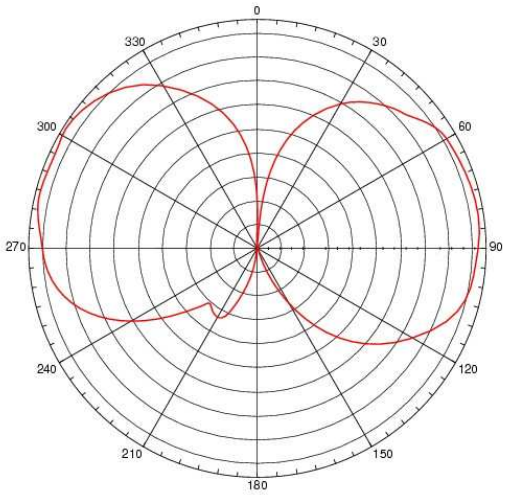

Figura 11 - Irradiação da antena Ominidirecional
Fonte: MORIMOTO (2008).

Segundo Morimoto (2008) a potência de uma antena é medida em dBi (*decibel isotrópico*), sendo que uma antena que apresenta um ganho de 10 dBi é o que equivale a um aumento de 10 vezes a potência de um equipamento podendo exceder a área de cobertura padrão do ponto de acesso.

Antenas geralmente concentram sinais em determinadas direções, sendo assim quanto mais o sinal é concentrado maior é o ganho, de forma que quanto maior a antena maior é o ganho (MORIMOTO, 2008).

O ganho da antena é medido em dBi, já a potência de transmissão é medida em dBm (*decibel milliwatt*). O padrão de comparação de potência de transmissão é de 1 *milliwatt* e corresponde a 0 dBm, que partindo disso cada vez é dobrada a potência do sinal, são somados aproximadamente 3 decibéis, já que dentro dessa escala apresenta um aumento de sinal duas vezes mais forte (MORIMOTO, 2008).

0 dBm = 1 milliwatts
3 dBm = 2 milliwatts
6 dBm = 4 milliwatts
9 dBm = 7.9 milliwatts
12 dBm = 15.8 milliwatts
15 dBm = 31.6 milliwatts

18 dBm = 61.1 milliwatts
21 dBm = 125.9 milliwatts
24 dBm = 251.2 milliwatts
27 dBm = 501.2 milliwatts
30 dBm = 1000 milliwatts
60 dBm = 1000000 milliwatts

3.4.1 Antena Ominidirecional

Antenas ominidirecionais cobrem 360º no plano horizontal como mostrado na Figura 12, indicada para melhor desempenho em áreas bem amplas, ou aplicações multipontos, onde essa antena é utilizada de estação de base, com estações remotas ao seu redor. Uma desvantagem dessa antena é a exposição de ruídos na transmissão do sinal, pois uma vez que seu sinal cobre um grau de 360º dependendo da potência do equipamento pode colidir com sinais de outras bases transmissoras podendo afetar a desempenho do seu sinal como do sinal invadido (MORIMOTO, 2008).

Figura 12 - Antena omnidirecional
Fonte: HYPERLINK (2008)

3.4.2 Antenas Direcionais

Antena direcional tem a concentração do seu sinal em uma única direção. Esse sinal pode ter alcance curto e amplo ou longo e estreito. Quanto mais o sinal for estreito maior a distância alcançada (MORIMOTO, 2008).

3.4.3 Antena Parabólica

Segundo Morimoto (2008) essa antena emite o sinal em forma de cone, é indicada para aplicações de longa distância. Seu modelo em *grid* (grelha) mostrado na Figura 13 são

menos suscetíveis a ação dos ventos em razão dos mesmos passarem pela sua estrutura, pois dessa forma evita que seu posicionamento seja alterado, tendo a necessidade de um novo ajuste. Seu sinal chega em torno de 40 a 50 km em condições visuais perfeitas.

Figura 13 - Antena parabólica
Fonte: HYPERLINK (2008).

3.4.4 Antena Setorial

Antenas setoriais como mostrado na Figura 14 têm seu formato amplo e plano cobrindo um ângulo de 90º, são normalmente montadas em paredes podendo seu uso ser interno e externo. Esse tipo de antena é usado para interligação de prédios ou uma área de cobertura de no máximo 8km de distância dependendo do equipamento (MORIMOTO, 2008).

Figura 14 - Antena setorial
Fonte: HYPERLINK (2008).

3.4.5 Antena Yagi

As antenas yagi possuem um melhor ganho de sinal, mas sua capacidade de cobertura é pequena, normalmente num raio de 24 x 30 graus, podendo ser mais estreito. Ela apresenta um ganho de 14 a 19 dBi bem superior as setoriais. Essas antenas são utilizadas para cobrir

algumas áreas especificas que estejam muito distantes do ponto de acesso ou utilizadas para conectar redes distantes, tendo à necessidade de ambas as antenas estarem apontadas exatamente uma para a outra, podendo fechar links de até 25 km e que representa 150 vezes seu alcance inicial (MORIMOTO, 2008).

Figura 15 - Antena Yagi
Fonte: HYPERLINK (2008)

Segundo Morimoto (2008) as antenas Yagi como mostrado na Figura 15 são as melhores quando se tem a necessidade de que o sinal “fure” um obstáculo que está entre as redes, mas neste caso a distância atingida será mais curta, do que o comum.

3.5 Elipsóide Fresnel

A Elipsóide de Fresnel é o ponto geométrico entre duas antenas, na qual possui comprimento igual à soma de suas distâncias e o meio comprimento de onda. Essa região é denominada primeira zona de Fresnel como apresentado na Figura 16 (WARCHALKING, 2003).

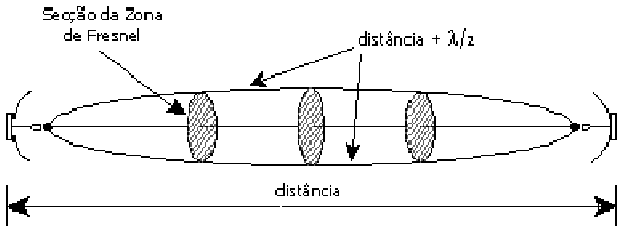

Figura 16 - Zona de Fresnel
Fonte: WARCHALKING (2003)

O objetivo do Elipsóide de Fresnel como mostra a Figura 17 é calcular o raio desta zona, em um determinado ponto entre as duas antenas, para verificar a possibilidade de visada mesmo atrás de um obstáculo (WARCHALKING, 2003).

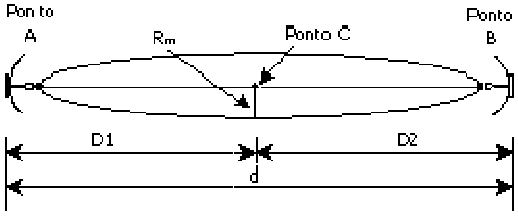

Figura 17 - Ponto central do encontro do sinal
Fonte: WARCHALKING (2003)

Segue cálculo segundo Warchalking (2003) como mostra a Figura 18.

Rm = raio de Fresnel (m)

D1 = Distancia AC (km)

D2 = Distancia BC (km)

d = Distancia de Enlace (km)

F = Frequencia em Mhz

$$r_m = 547\sqrt{\frac{D_1.D_2}{f.d}}$$

Figura 18 - Cálculo de Fresnel
Fonte: WARCHALKING (2003)

4. DESENVOLVIMENTO

4.1 Desenvolvimento da antena

O desenvolvimento da antena se baseia no modelo Yagi-Uda que segundo Morimoto (2008) essas antenas apresenta um ganho de 14 a 19 dBi bem superior as setoriais que são utilizadas para cobrir áreas que estejam muito distantes do ponto de acesso ou utilizadas para conectar pontos distantes de até 25 km, muito utilizada para transpor obstáculo que esteja entre as antenas, mas neste caso a distância atingida será mais curta, do que o esperado.

Para a criação da antena foi utilizada uma lata de solvente, podendo também ser utilizada lata de óleo de mesma dimensão ou até mesmo a lata da batata Pringles, mas sempre mantendo as medidas necessárias para fixação do conector.

O material utilizado para o desenvolvimento da parte física da antena foi uma lata de solvente, um conector N fêmea, fio de quatro milímetros, alicate, solda, ferro de solda, rebite e uma furadeira.

Para facilitar a compreensão da construção da antena a que se refere o presente trabalho o desenvolvimento desta foi dividido em quatro passos, que serão descritos a seguir.

Primeiro passo:

Segundo Moreira (2008) após limpeza da lata realizar uma abertura em uma das extremidades, como mostrado na Figura 19.

Figura 19 - Abertura da Lata

Segundo Moreira (2008) após a abertura, realizar um furo à ¼ da base da lata, como é exibido na Figura 20.

Figura 20 - Furo na lata

Segundo passo:

Segundo Warchalking (2006) para a fixação do conector à lata é preciso fazer algumas modificações, pois o conector deve ter uma altura de ¼ λ° (comprimento de onda), e para achar o comprimento λº foi utilizada a equação fundamental da ondulatória, sendo a velocidade "v" igual à velocidade da luz no vácuo (3.10^8 m/s).

Equação: v = λº * f; que no caso usado para a freqüência de 2,45 GHz. Cálculos:

3.10^8m/s = λº * 2,45. 10^9 Hz

λº = 3.10^8 m/s / (2,45 .10^9 Hz)

λº ~ 12,25 cm.

Como o comprimento deve ser de λº/4, então o comprimento do pino foi de pouco mais de 3 cm. Esse valor é fixo, pois o comprimento de onda λº depende apenas da freqüência e velocidade de propagação, sendo independente das medidas da sua lata (WARCHALKING, 2006).

Após os cálculos foi feita a solda de um pedaço de fio rígido de aproximadamente 3 cm no conector N externo como mostrado na Figura 21.

Figura 21 – Conector N

Terceiro passo:

Após soldagem do fio rígido no conector, o mesmo foi preso no furo feito na lata com um rebite como mostrado na Figura 22 e 23.

Figura 22 - Fixação do conector.

Figura 23 – Visão interna da lata

Quarto passo:

Após a criação da antena, é confeccionado o cabo de comunicação entre a antena e a placa wireless.

Os materiais utilizados foram quatro metros de cabo coaxial RG58 de 50 ohms, um conector N macho, que foi usado para ligar ao conector fêmea da antena, um conector RP-SMA macho, que foi utilizado para conectar a placa *wireless.*

4.2 Criação da estrutura

Para o suporte e fixação da antena foi construída uma estrutura que possui uma base de 22,5 x 22,5 cm em ferro como e apresentado na Figura 24.

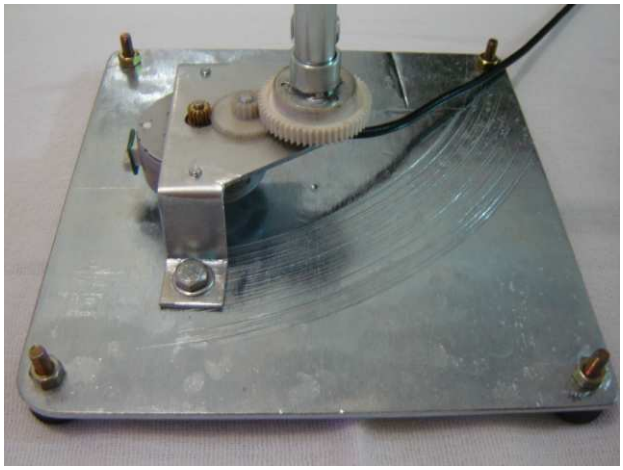

Figura 24 – Base da estrutura da antena e suporte do motor de passo

A Figura 25 apresenta uma pequena base que acomoda o motor de passo responsável pelo movimento da antena e uma engrenagem de plástico retirada de uma unidade CD-ROM serve de ligação entre o motor de passo a uma outra engrenagem que foi aproveitada de uma peça de impressora.

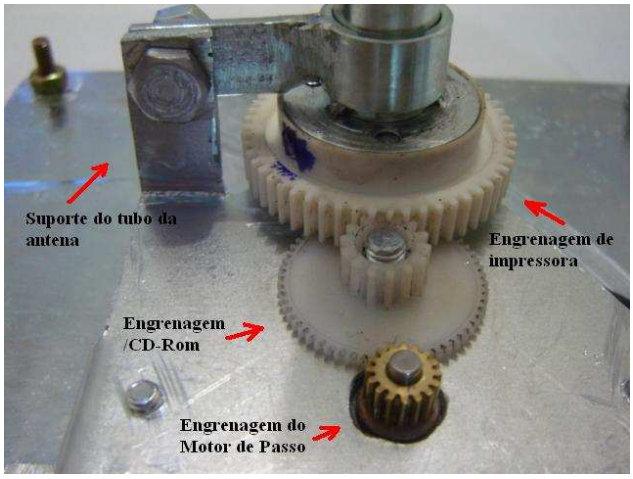

Figura 25 – Engrenagens e suporte da antena

Na engrenagem que fornece a base da antena, foi fixado um tubo de 55 cm de altura 1,5cm de diâmetro e na outra extremidade foi criada uma cinta de chapa de ferro que serve para fixar a antena permitindo a movimentação em diversos ângulos na horizontal como mostrado na Figura 26.

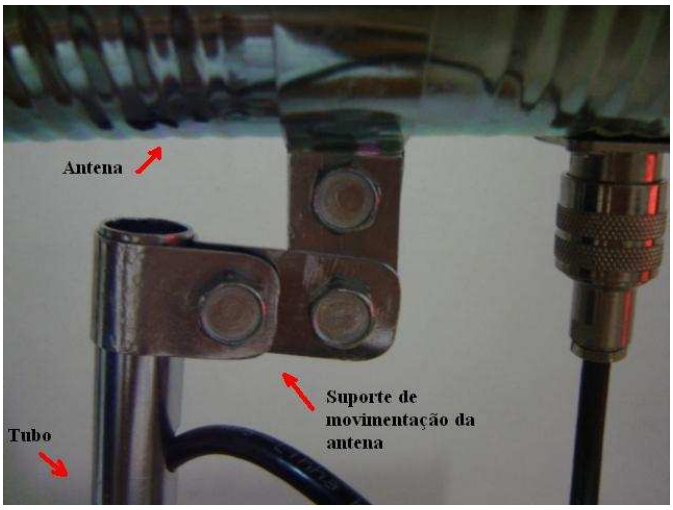

Figura 26 – Tubo e Suporte da antena

4.3 Criação da placa e motor de passo

Para a criação do circuito responsável pela movimentação da antena, foram utilizados os seguintes componentes:

- Um cabo paralelo com conector DB25 macho;
- Acido;
- Placa lisa de circuito;
- 1 motor de passo;
- 4 resistores de 10 ohms;
- 4 fotoacoplador 4n25h;
- 4 resistores de 100 ohms;
- 4 Tips 122;
- 4 resistores 1k;
- 4 leds;
- 1 resistor de 5 watts;
- 1 conector de fonte;
- 1 fonte de energia de 9 volts.

Para a criação do circuito foi utilizada a porta paralela mostrada na Figura 27, e os pinos responsáveis pelo envio dos sinais foram:

- Pino 2 D0 cabo marrom, envio de dados;
- Pino 3 D1 cabo rosa, envio de dados;
- Pino 4 D2 cabo laranja, envio de dados;
- Pino 5 D3 cabo amarelo, envio de dados;
- Pino 20 GND cabo preto, terra;

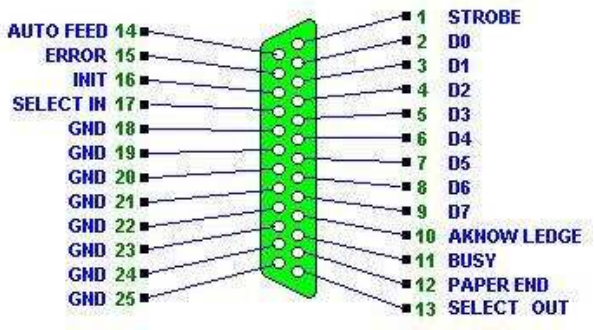

Figura 27 – Conector DB25

4.4 Circuito

O circuito mostrado na Figura 28 é o responsável pela movimentação da antena, para seu desenvolvimento foi dividido em 4 etapas.

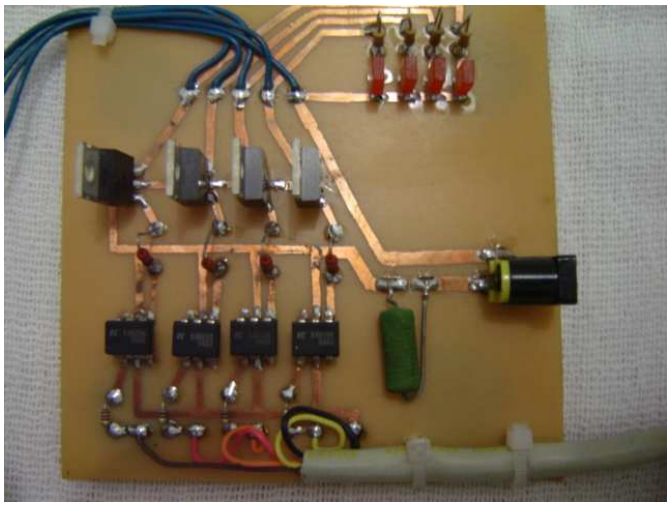

Figura 28 – O Circuito

1º etapa:

Nesta etapa os componentes mostrados na Figura 29 são responsáveis pela entrada dos sinais ao circuito através dos cabos da porta paralela, como os mesmos enviam sinais com corrente elétrica, estes precisam ser tratados antes de chegarem ao motor e a qualquer componente. Logo que soldados a placa em seu trajeto de envio de sinais eles passam por resistores de 10 ohms responsáveis por controlar a corrente que logo é enviada para os fotoacopladores (4n25h) que filtraram novamente a voltagem enviada.

Esse primeiro grupo tem em seu conjunto a importância de separar os circuitos de forma que se algo acontecer como o envio de alguma voltagem fora dos padrões por parte das portas paralelas, não danifique o restante do circuito ou o próprio motor, ou ao contrario caso aconteça de alguma voltagem retornar do motor ou de alguma parte do circuito.

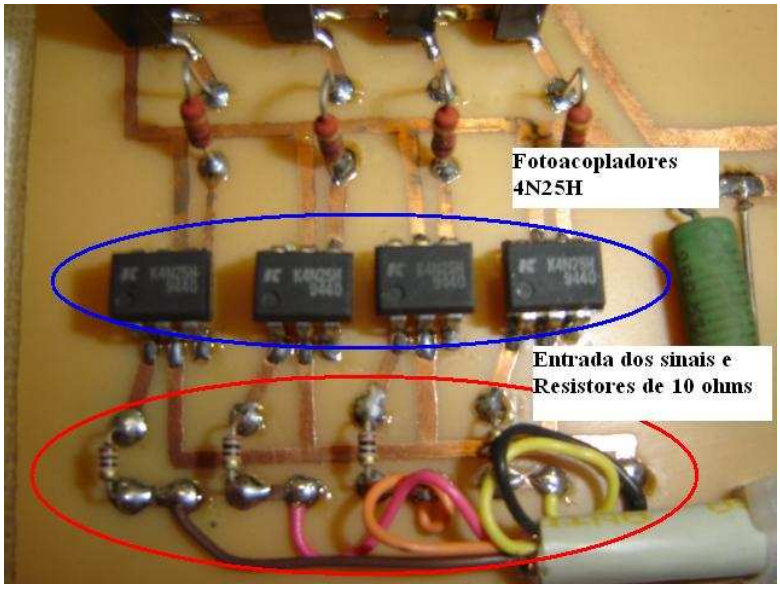

Figura 29 – Entrada dos sinais e fotoacopladores

2º etapa:

Nessa etapa do circuito após os sinais terem sido filtrados pelos fotoacopladores eles passam por mais um resistor de 100 ohms, que já é enviado para os TIP122 que é o responsável por normalizar a corrente do sinal que será enviada ao motor de passo como mostrado na Figura 30.

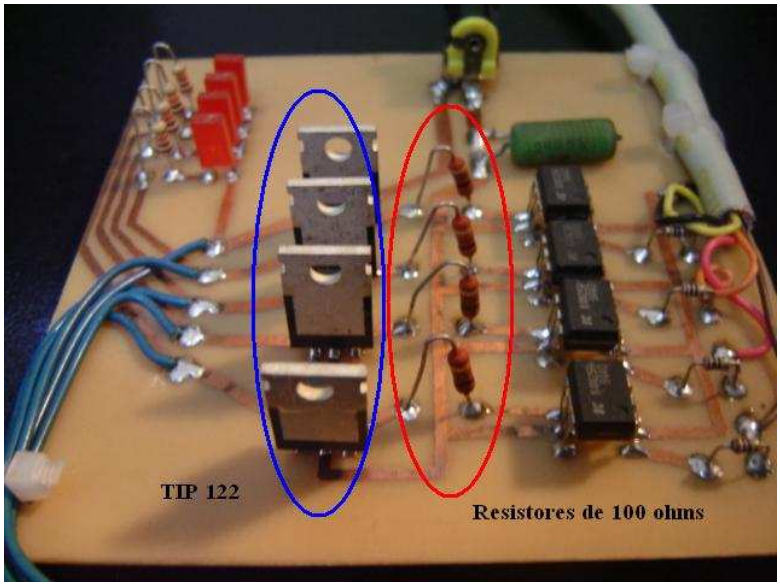

Figura 30 – Resistores e Tips

3º etapa:

Essa etapa do é a responsável por receber a energia externa que é alimentada por uma fonte de 9 volts e que percorre o circuito, mas antes é filtrada por um resistor de 5 watts que

controla a corrente da fonte de energia antes de chegar aos componentes como pode ser mostrado na Figura 31.

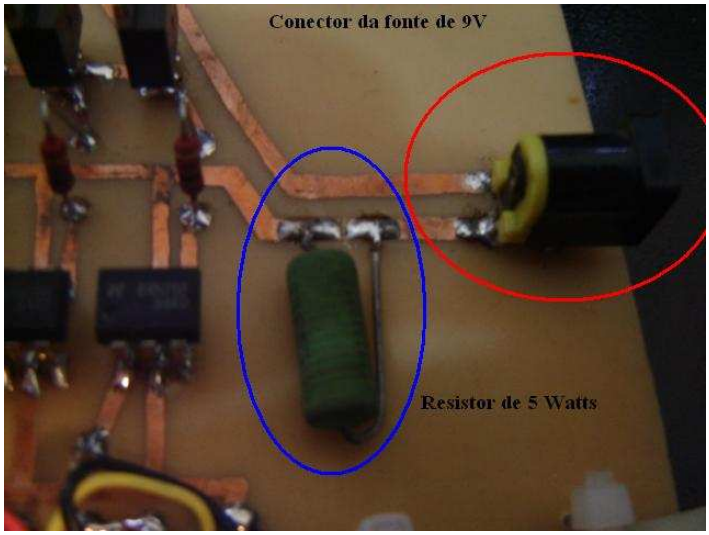

Figura 31 – Fonte de energia e resistor

4º etapa:

Essa etapa do circuito é a responsável pelo envio do sinal ao motor de passo e aos leds que indicaram qual bobina do motor que estará energizada, mas antes de receberem o sinal são filtrados por resistores de 1k limitando a corrente para não danificá-los como mostrado na Figura 32.

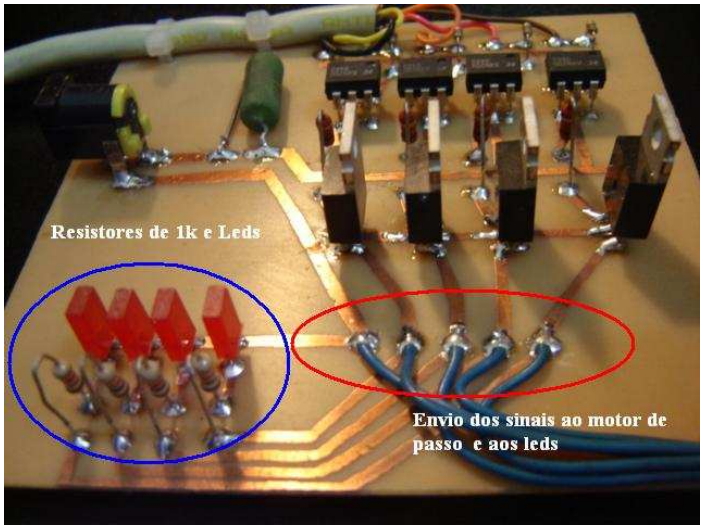

Figura 32 – Leds e envio de sinais

O motor de passo utilizado para rotacionar a antena foi um da Minebea-Matsushita modelo PM55L-048, utilizado em impressoras laser da marca HP mostrado na Figura 33.

Figura 33 – Motor de Passo

4.6 Programa e envio dos sinais

Para o envio de sinal ao circuito e ao motor de passo foi utilizado o programa DSPCOM como mostrado na Figura 34.

Figura 34 – Programa DSPCOM

A Figura 35 mostra a tela inicial do programa é encontrado varias opção de envio de sinal pela porta paralela.

Figura 35 – Tela inicial do Programa

Para o envio do sinal ao circuito foi selecionada a aba “Enviar”, e para que o motor movimente-se de acordo com o desenvolvimento proposto, criamos um “*Loop*” com valores binários, que foi carregado o arquivo em através da opção “Abrir” mostrado na Figura 36.

Figura 36 – Abrindo arquivo

A Figura 37 mostra o arquivo utilizado que foi o “14 voltas hi ant volta.DSP”.

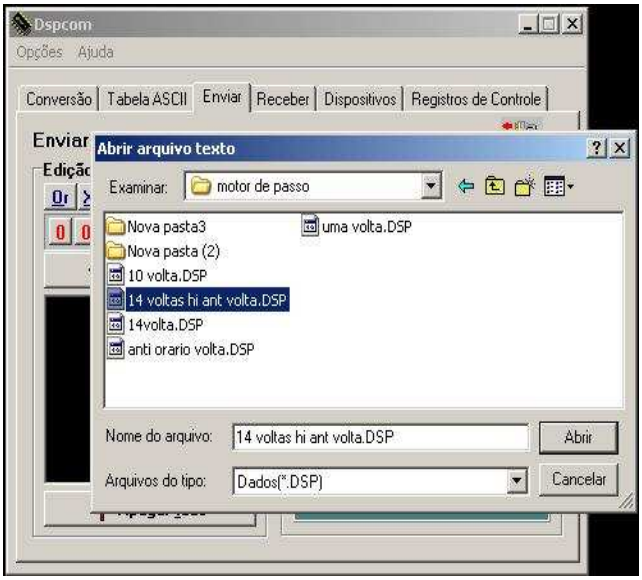

Figura 37 – Localizando arquivo

Após carregar o arquivo, ao lado esquerdo do programa apresenta o conteúdo do arquivo, o mesmo mostra os números binários referente ao envio de sinal as pinagens da porta paralela, para que o motor gire a antena em uma volta completa o mesmo precisa dar um *Loop* de 14 voltas horárias e anti-horárias como mostrado na Figura 38.

Figura 38 – Código do arquivo

Após o arquivo inserido a Figura 39, mostra as opções marcadas “Enviar para a porta” e em “Repetir” a opção “Infinito”, logo após foi escolhida uma velocidade em que o código será enviado a porta paralela, podendo ser alta, media e baixa, para concluir o envio é pressionado o botão “*play*”.

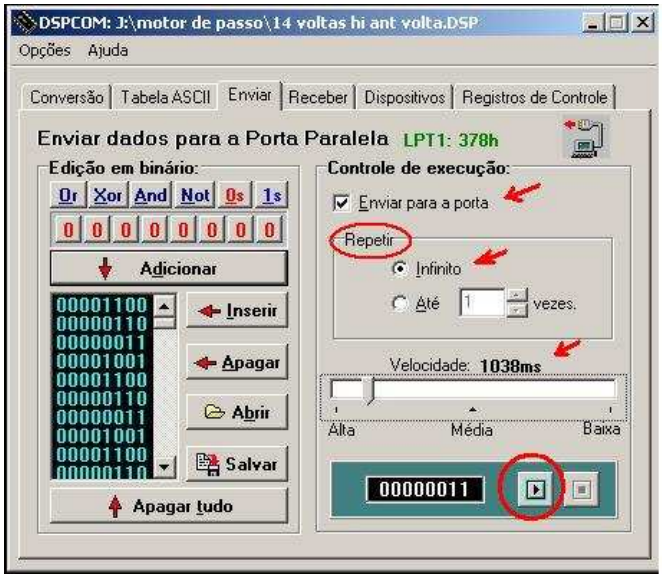

Figura 39 – Enviando o sinal

4.7 Antena e sinal

Para realizar a análise do raio de Fresnel, foi utilizada a seguinte equação:

$$r_m = 547\sqrt{\frac{D_1 . D_2}{f . d}}$$

rm = raio de Fresnel (metros),

D1 = Distancia do primeiro ponto (Km),

D2 = Distancia do segundo ponto (Km),

d = Distancia do enlace (Km),

f = Freqüência em Mhz.

Na Figura 40 é possível ver a aplicação do cálculo de raio de Fresnel, pois na distância do ponto A até o obstáculo tem-se 8 km (D1), do ponto B até o obstáculo temos 2 km (D2), temos 10 km (d) que é a distância total do enlace e a freqüência 2.4 Ghz que foi convertida para 2400Mhz.

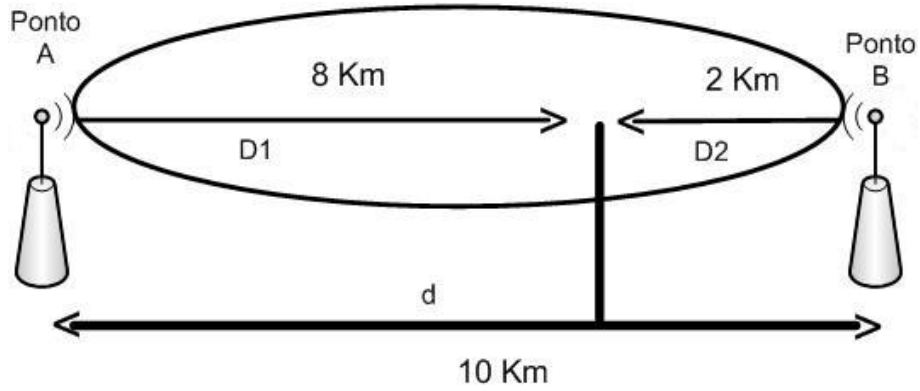

Figura 40 – Elipsóide de Fresnel

É possível verificar a seguir uma aplicação/exemplo da fórmula:

Rm = 547 √8*2 / 2400*10
Rm = 547 √6.666
Rm = 547 * 2.58
Rm = 1411,26

Com este exemplo temos um raio de 1411,26 metros, o mesmo podendo estar sob um obstáculo com o máximo de 25% desse total para não ter problemas com o envio e recebimento do sinal.

5. RESULTADOS OBTIDOS

Com a antena desenvolvida descrita pelo capítulo anterior, foi possível realizar alguns testes para averiguar o alcance medido em metros e aplicar na fórmula de Fresnel.

Para realizar os testes foram definidos aleatoriamente dois pontos em regiões afastadas, mais precisamente na região leste (Distrito Industrial II e Vale do Igapó) que se localizam na cidade de Bauru, estado de São Paulo.

Nos testes para análise foi utilizado à antena Yagi-Uda desenvolvida neste trabalho e como resultado foi identificado uma melhora nos sinais wireless baseada na ferramenta denominada NetStumbler, esta ferramenta é gratuita e possui uma interface de fácil manipulação, sendo possível analisar os níveis de sinais presentes ao seu alcance dependendo da antena utilizada.

A melhora do sinal conforme citado no parágrafo anterior, baseando-se nos testes realizados e não descartando os objetos que possam barrar os sinais (árvores, fios elétricos, entre outros), o ganho de sinal foi de aproximadamente 1.000 metros, podendo facilmente ser utilizado para trafegar informações e utilização para navegação na internet.

O primeiro teste foi realizado em uma rua localizada no Distrito Industrial II em Bauru, e conforme Figura 41, representada através da ferramenta de análise NetStumbler, mostra o momento em que a antena Yagi-Uda estava próxima da base (no caso era um roteador wireless D-Link modelo DI-524 com uma antena omni de baixo alcance), a partir deste momento iniciou-se o deslocamento em aproximadamente 600 metros e foi observado que a qualidade do nível de sinal diminuía, mas que se manteve constante em determinado momento, mas em outros momentos teve falta de sinal devido ao teste estar sendo efetuado em uma rua que em alguns momentos havia a presença de carros e ônibus atravessando o sinal e também a movimentação humana em relação ao manuseio dos equipamentos, pois ambos, antena Yagi-Uda e roteador D-Link, estavam sendo manuseados não em bases fixas sendo que qualquer movimentação provocava alterações no nível do sinal.

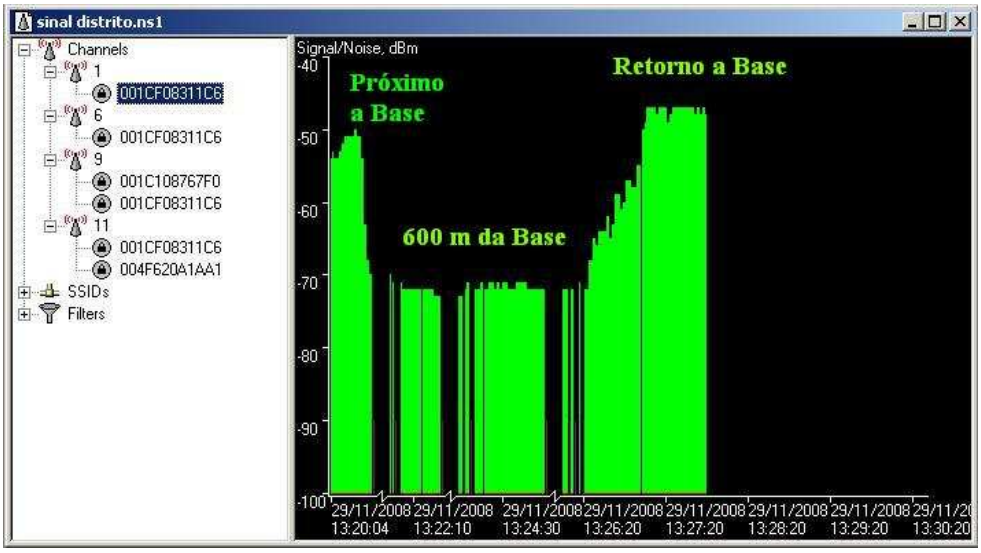

Figura 41 - Primeiro teste Distrito Industrial II

O segundo teste foi realizado no Vale do Igapó em Bauru, e conforme apresentado na Figura 42, a ferramenta de análise NetStumbler mostra inicialmente o momento em que a antena está próxima ao roteador e se desloca 1300 metros, e analisando o nível de sinal, o mesmo se manteve constante em determinado momento, mas com algumas oscilações devido a essa área escolhida conter fatores que possam barrar ou causar oscilações como as árvores e fios de eletricidades na trajetória do sinal. Vale também ressaltar que no primeiro teste em uma distância de 600 metros o sinal chegou ao mesmo nível comparado com o segundo teste que chegou a 1300 metros, sendo possível observar que no caso de conseguir uma visada de maior distância e manter ambos os pontos fixos em uma base, poderíamos ter melhores resultados em maiores distâncias.

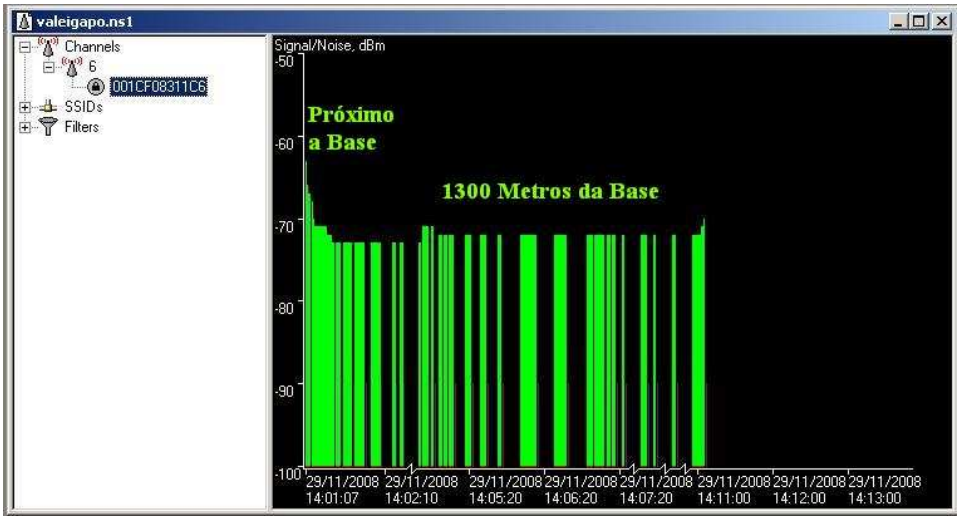

Figura 42 - Segundo teste Vale do Igapó

Após os testes, os resultados obtidos pela antena desenvolvida, foram aplicados ao cálculo da elipsóide de Fresnel para verificar em relação a distâncias o raio que poderia ser gerado e chegou-se aos seguintes resultados:

Na aplicação da Elipsóide de Fresnel no teste feito no Distrito Industrial II:

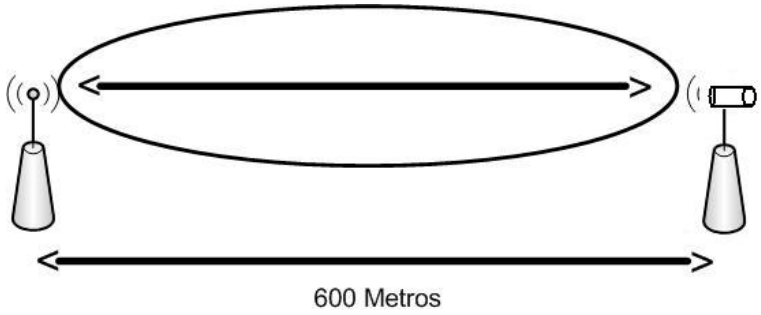

Figura 43 - Elipsóide de Fresnel aplicado ao primeiro teste prático

Aplicação da fórmula representada pela Figura 43:

Rm = 547 √0,6 / 2400*0,6

Rm = 547 √0, 000416

Rm = 547 * 0, 0203

Rm = 10, 982

O resultado do primeiro teste apresenta um raio de 10, 982 metros, o mesmo livre de interferência podendo se usar todo o raio sem problema de interferência.

No segundo local, o Vale do Igapó, com o teste já realizado através da antena e aplicando o cálculo da Elipsóide de Fresnel tem-se o seguinte resultado:

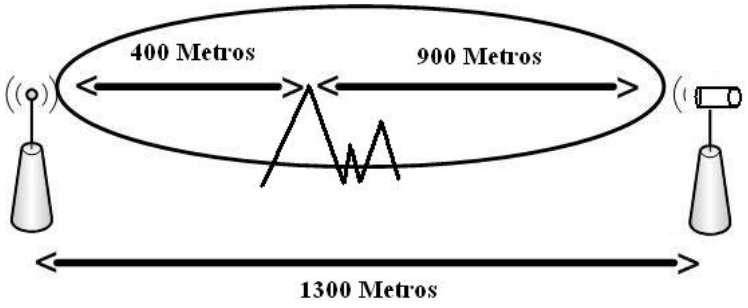

Figura 44 - Elipsóide de Fresnel aplicado ao segundo teste prático

Aplicação da fórmula representada pela Figura 44:

Rm = 547 √0,4*0,9 / 2400*1,3
Rm = 547 √0,000115
Rm = 547 * 0,0107
Rm = 5,852

O resultado deste teste apresenta um raio de 5, 582 metros, no momento que encontra o obstáculo, podendo o mesmo ter no máximo 25% de obstrução que não causará interferência no sinal.

Com isso todos os resultados foram satisfatórios observados que através de uma antena caseira de baixo custo, e lugares não muito apropriados para o uso, foi possível ter um sinal de qualidade satisfatória e que em melhores condições poderia ser usado com maior qualidade para enviar e receber informações.

6. CONSIDERAÇÕES FINAIS

O constante crescimento da rede sem fio se deve ao grande avanço tecnológico e a mobilidade oferecida por essa tecnologia. Uma vez em que essas redes podem ser implementadas em um ambiente coorporativo ou residencial, pois, hoje equipamentos são facilmente encontrados a um preço bem acessivo.

Com o avanço da utilização de redes sem fio, muitos problemas são apresentados, devido a fácil configuração muitos usuários não se preocupam com a segurança, tornando-se alvo de algum tipo de ataque ou utilização indevida, com isso o IEEE apresenta formas de segurança como padrões de autenticações, trocas de chaves, cartões e *tokens*, sempre com o objetivo de manter as informações trafegadas o mais seguro possível.

Sabemos que na área da informática nunca iremos ter um ambiente totalmente seguro, no uso de redes sem fio a utilização dos padrões e protocolos criados pelo IEEE já servem de segurança, mas podemos ter um ambiente ainda mais seguro quando aplicado em conjunto com Firewalls e uma monitoração constante dos acessos. Essas redes bem estruturadas, com todas as políticas possíveis aplicadas ao determinado ambiente, trazem uma segurança necessária.

A utilização de antenas para uso indoor como outdoor, tem um papel fundamental no tipo de aplicação a redes sem fio, pois em um ambiente em que se deseja conectar poucas máquinas em uma estrutura indoor, tende-se a levar em consideração a estrutura física aplicada, pois uma antena que irradie uma freqüência muito longa pode apresentar risco caso o sinal ultrapasse a estrutura, já no caso de uma utilização outdoor, como na interligação de prédios, é necessário observar as distâncias que serão utilizadas as antenas e levando em consideração a qualidade da antena na irradiação do sinal e possíveis interferências e obstáculos.

A criação de uma antena caseira, mostra que é possível de uma forma simples, interligar prédios ou emitir sinal a um determinado lugar. A criação da antena modelo Yagi-Uda serviu de base para implementar o estudo da elipsóide de Fresnel que tem por objetivo mostrar que dependendo do ambiente aplicado, pode-se possuir objetos que atrapalhem a visão total ou parcial entre pontos de acesso e mostra que mesmo assim é possível enviar e receber sinal, baseado em seus cálculos.

7. REFERÊNCIAS BIBLIOGRÁFICAS

LACERDA, P. S. **Análise de Segurança em Redes Wireless 802.11x.** 2007. 49f. Trabalho de Conclusão de Curso (Ciência da Conputação) - Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora.

RUFINO, N.M.O. **Segurança em Redes sem Fio:** Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**.** São Paulo: Novatec, 2005. 224p.

DUARTE, L.O. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x.** São José do Rio Preto, SP. UNESP / IBILCE , 2003, 55p. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação.

ENGST, A.; FLEISHMAN, G. **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.

MATHIAS, A.P.; **IEEE 802.11 – Redes Sem Fio.** Disponível na Internet. www.gta.ufrj.br/grad/00_2/ieee/ . 01/04/2008.

AGUIAR, P.A. F. **Segurança em Redes WI-FI.** Montes Claros, MG. Universidade Estadual de Montes Claros, 2005, 79p. Monografia defendida para obtenção do grau de Bacharel em Sistemas de Informação.

GIMENES, E.C. **Segurança de Redes Wireless.** Mauá, SP. FATEC, 2005, 58p. Trabalho de Conclusão do Curso de Tecnólogo em Informática com ênfase em Gestão de Negócios.

AIRTRAF. **Documentation.** 2002. Disponível em: http://airtraf.sourceforge.net. Acessado em: 20/03/2008.

CHEOPS-NG. **Description**. 2008. Disponível em: http://cheops-ng.sourceforge.net/index.php. Acessado em: 29/03/2008.

KISMET. **Documentation.** 2007. Disponível em: http://www.kismetwireless.net/ . Acessado em: 30/03/2008.

NETSTUMBLER. **Documentation.** 2008. Disponível em: http://www.netstumbler.org/. Acessado em : 30/04/2008.

TEWS, E.; WEINMANN, R.; PYSHKIN, A. **Breaking 104 bit WEP in less than 60 seconds.** 2007. 12p.

WARCHALLING. **Entendendo e vencendo WEP.** 19 de Julho de 2006. Disponível em https://capivara.warchalking.com.br/index.php?option=com_content&task=view&id=39& . Acessado em 28/03/2008.

HYPERLINK. **Antenas.** 2008. Disponível em: http://www.hyperlinktech.com/category.aspx?id=73. Acessado em 21/04/2008.

WARCHALKING. **Cálculo do raio de Fresnel**. 04 de Setembro de 2003. Disponível em: http://www.warchalking.com.br/cgi-bin/base/tutoriais2.444?27. Acessado em 22/05/2008.

WARCHALKING. **Como fazer uma Cantenna (Antena de lata).** 02 de Setembro de 2006. Disponível em: https://capivara.warchalking.com.br/index.php?option=com_content&task=view&id=43&Itemid=2. Acessado em 20/04/2008.

MOREIRA, A. **Sinhantena - antena 2.5Ghz wireless.** Disponível em: http://www.geocities.com/sinhantena/. Acessado em 18/04/2008.

MORIMOTO, C.E. **Redes Wireless.** 06 de fevereiro de 2008. Disponível em: http://www.guiadohardware.net/tutoriais/alcance-antenas-conectores-potencia/. Acessado em: 17/04/2008.

MAIA, W.L.G. **Um estudo de Viabilidade de Links de Rádio Freqüência para Integração de Redes de Computadores na UFACNet e Região do Acre.** Florianópolis, SC. Universidade Federal de Santa Catarina, 2000, 191p. Dissertação de Mestrado para a obtenção do grau de Mestre em Ciência da Computação.

SILVA, L.W.T. **Otimização do Controle Eletrônico do Diagrama de Radiação de Arranjos de Antenas Usando Algoritmos Genéticos com Codificação Real.** Natal, RN. Universidade Federal do Rio Grande do Norte, 2006, 165p. Dissertação de Mestrado defendido para a obtenção do grau de Mestre em Ciência.

GOMES, A.T. **Telecomunicações: transmissão e recepção AM - FM: Sistemas pulsados**. Ed. Érica, 2ª ed. São Paulo, 1985.

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.

8. GLOSSÁRIO

Anti-spyware - (anti = contra, spy = espião, ware = programa) são programas utilizados para combater programas espiões.

Antivírus - são softwares projetados para detectar e eliminar vírus de computador.

Criptografia - é um conjunto de métodos e técnicas destinadas a proteger o conteúdo de uma informação, tanto em relação a modificações não autorizadas quanto à alteração de sua origem.

Ethernet - rede de computadores interligada por cabos.

Firewall - pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre um computador e a Internet Wireless.

Gateway - é um dispositivo utilizado para unir duas redes de computadores.

Hardware - é a parte física do computador, ou seja, é o conjunto de componentes eletrônicos, circuitos integrados e placas, que se comunicam através de barramentos.

HTTP - é o protocolo usado para a transmissão de dados no sistema World-Wide Web.

Smartcards - é um cartão contendo um chip responsável pela geração e o armazenamento de certificados digitais.

Spoofing - é uma técnica de ataque que consiste em esconder a verdadeira identidade do atacante na rede, fazendo que todos os hosts da rede se comuniquem com ele sem saber que é falso.

TELNET - é um protocolo de login remoto utilizado na comunicação entre cliente-servidor.

Throughput - (ou taxa de transferência) é a quantidade de dados transferidos de um lugar a outro, ou a quantidade de dados processados em um determinado espaço de tempo, pode-se usar o termo throughput para referir-se a quantidade de dados transferidos em uma rede.

Tokens - é um dispositivo (hardware) com conexão via USB, que permite armazenar e transportar de forma segura seu certificado digital. Dessa forma, o usuário poderá fazer assinaturas digitais de qualquer computador com uma porta USB, não ficando limitado a assinar digitalmente somente através de seu computador.

Warchalking - é uma forma de encontrar redes sem fio e fazer marcações com o tipo da rede encontrada, segurança aplicada e vulnerabilidades.

Wardriving - é uma técnica de ataque em redes sem fio que consistem em o atacante estar em movimento (dentro de um carro) procurando redes vulneráveis.

Wi-fi Alliance - é uma organização sem fins lucrativos criada para difundir o uso das conexões sem fio.