UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

VINÍCIUS SALOMÃO DE OLIVEIRA RAMOS

ANALISE DA SEGURANÇA E VULNERABILIDADES DO PADRÃO 802.15

MONOGRAFIA

CURITIBA
2011

VINÍCIUS SALOMÃO DE OLIVEIRA RAMOS

ANALISE DA SEGURANÇA E VULNERABILIDADES DO PADRÃO 802.15

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Fabiano Scriptore de Carvalho

CURITIBA

2011

AGRADECIMENTOS

Agradeço a Deus pela oportunidade do aprendizado recebido neste curso.

Aos meus pais, Ana Nunes de Oliveira de Ramos e Euclides Salomão Ramos pela compreensão de sempre e incentivo.

Ao meu orientador Prof. Fabiano Scriptore Carvalho pelo empréstimo de equipamentos e os auxílios necessários para o desenvolvimento do presente.

Aos meus colegas de trabalho.

A empresa que trabalho por disponibilizar equipamentos para meus estudos.

Aos meus amigos e amigas mais próximos.

Aos meus colegas de sala.

A Universidade Tecnológica Federal do Paraná.

RESUMO

RAMOS, Vinícius S. de O. **Analise da segurança e vulnerabilidades do padrão 802.15**. 2011. 57 folhas. Monografia (Especialista em configuração e gerenciamento de servidores e equipamentos de redes) - Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

Esta pesquisa apresenta um estudo sobre as vulnerabilidades das redes sem fio que utilizam o padrão IEEE 802.15 (*Bluetooth).* Complementado por uma pesquisa de campo, o estudo identificou diversas vulnerabilidades na utilização deste padrão, bem como o desconhecimento destas vulnerabilidades por parte dos seus usuários. Discute um levantamento teórico sobre a tecnologia *Bluetooth,* padronizado pelo *Institute of Electrical and Electronic Engineers* (IEEE) 802.15 e como esta tecnologia está presente no cotidiano das pessoas, que está sendo cada vez mais utilizado nos dias atuais. Conceitua a pilha de protocolos TCP/IP, redes sem fio e faz uma análise do espectro eletromagnético utilizado por estas redes. Em relação a faixa de frequência *Industrial, Scientific and Medical* (ISM), apresenta os possíveis problemas de interferências com outros dispositivos. Traz como resultado do estudo uma identificação das vulnerabilidades da utilização do IEEE 802.15 e apresenta formas de corrigir as falhas de segurança apresentadas na utilização deste.

Palavras-chave: *Bluetooth.* Vulnerabilidades. padrão 802.15.

ABSTRACT

RAMOS, Vinícius S. O. Bluetooth tecnology – Security and vulnerability analysis of the 802.15 standard. 2011. 57 pages. Monograph (Specialist in configuring and managing serves and network equipament), Federal Technological University od Paraná. Curitiba, 2011.

This research presents a study on the vulnerabilities of wireless networks using IEEE 802.15 (Bluetooth). Complemented by a field survey, the study identified several vulnerabilities in using this standard, as well as the ignorance of these vulnerabilities by their users. Discusses a theoretical survey on the Bluetooth technology, standardized by the Institute of Electrical and Electronic Engineers (IEEE) 802.15 and how this technology is present in daily life, which is being increasingly used today. Conceptualizes the TCP / IP, wireless networks and provides an analysis of the electromagnetic spectrum used by these networks. Regarding the frequency band Industrial, Scientific and Medical (ISM), shows the possible interference problems with other devices. Brings as a result of a study identifying the vulnerabilities of using IEEE 802.15 and presents ways to fix security flaws in the use made of this.

Keywords: Bluetooth. vulnerabilities. 802.15 standard.

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

ACK	Acknowledgement
ARPANET	Advanced Research Projects Agency Network
IEEE	Institute of Electrical and Electronic Engineers
L2CAP	Logical Link Control and Adaptation Protocol
LAN	Local Area Network
MAC	Media Access Control
OSI	Open Systems Interconnection
PIN	Personal Identification Number
RFCOMM	Radio Frequency Communications
SIG	Special Interest Group
TCS BIN	Telephony Control Protocol-Binary

LISTA DE SIGLAS

ACL	ASYNCHRONOUS CONNECTION-LESS
ADSL	ASYMMETRIC DIGITAL SUBSCRIBER LINE
AP	ACCESS POINT
BBS	BASIC SERVICE SET
BDADDR	BLUETOOTH DEVICE ADDRESS
CSMA/CA	CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE
CSMA/CD	CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION
CTS	CLEAR TO SEND
DSSS	DIRECT SEQUENCE SPREAD SPECTRUM
EIA-232	ELECTRONIC INDUSTRIES ASSOCIATION
ESS	EXTENDED SERVICE SET
FHSS	FREQUENCY HOPPING SPREAD SPECTRUM
FTP	FILE TRANSFER PROTOCOL
IBSS	INDEPENDENT BASIC SERVICE SET
IP	INTERNET PROTOCOL
ISM	INDUSTRIAL, SCIENTIFIC AND MEDICAL
OFDM	ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING
PCS	PERSONAL COMPUTERS
PDA	PERSONAL DIGITAL ASSISTANT
PPP	POINT-TO-POINT PROTOCOL
TCP	TRANSMISSION CONTROL PROTOCOL
RS-232	RECOMMENDED STANDARD
RTS	REQUEST TO SET
SCO	SYNCHRONOUS CONNECTION ORIENTED
SMS	SHORT MESSAGE SERVICE
SMTP	SIMPLE MAIL TRANSFER PROTOCOL
UDP	USER DATAGRAM PROTOCOL
WAE	WIRELESS APPLICATION ENVIRONMENT
WAP	WIRELESS APPLICATION PROTOCOL

SUMÁRIO

1 INTRODUÇÃO

Neste primeiro capítulo abordará a introdução da pesquisa, apresentando seu tema, delimitação da pesquisa, problemas e premissas, objetivos, justificativa, procedimentos metodológicos, embasamento teórico e estrutura completa da pesquisa.

1.1 TEMA

As redes sem fio estão se tornando cada vez mais presentes no cotidiano das pessoas. Cada vez mais os usuários necessitam estar conectados para compartilhar documentos, enviar ou receber e-mails, ou simplesmente conversar com outras pessoas por meio de um chat de bate-papo. Ao contrário do que se imagina, a transmissão de informações sem fio não é uma tecnologia nova. Em 1899 o físico italiano Guglielmo Marconi demonstrou por meio de um telégrafo sem fio a transmissão de informações de um navio para o litoral por meio de código Morse (TANEMBAUM, 1994). Os sistemas digitais modernos tem um desempenho superior ao utilizado em 1899, mais a ideia central é a mesma (TANEMBAUM, 1994).

As redes sem fio demoraram à se tornarem populares, devido a uma série de fatores, mas o mais importante é o custo dos equipamentos, que era elevado. Em 1987 foi formado um grupo de trabalho denominado *Institute of Electrical and Eletronics Engineers* (IEEE), com o objetivo de definir padrões para o uso das redes sem fio. Esses padrões seriam basicamente definir a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos clientes (RAPPAPORT, 2009). As redes sem fio se tornaram mais populares no final dos anos 90 com a popularidade da *Internet* e a queda nos custos dos equipamentos de redes. Com o decorrer do tempo os grupos do IEEE responsáveis pela padronização das redes sem fio trabalharam em vários padrões, como o 802.11, o 802.15 e o 802.16. (RAPPAPORT, 2009) (RUFINO, 2007).

O padrão IEEE 802.15, também chamado de *Bluetooth* é o foco principal deste trabalho, tem como meio de transmissão o ar, utilizando rádio frequência. Com

isto é passível de ataques de usuários que podem ter acesso à rede interna, alterar ou roubar dados dos usuários que estão utilizando esta rede. A tecnologia *Bluetooth* está presente em vários equipamentos como notebooks, impressoras, mouses, teclados, carros, equipamentos de som e principalmente em celulares. Estes são os alvos preferidos dos atacantes, pois é possível extrair varias informações como contatos, fotos e mensagens.

Segundo RUFINO (2007) as redes *Bluetooth* tem os mesmos riscos que as outras redes sem fio, podendo receber ataques de negação de serviço, captura e escuta entre outros tipos de ataques. Ainda segundo RUFINO (2007) em alguns *softwares* é possível fazer uma ligação utilizando um telefone atacado, copiar agendas, redirecionar chamadas, copiar mensagens entre outros exemplos.

O tema principal deste trabalho é mostrar as vulnerabilidades da tecnologia IEEE 802.15 e as formas que podem ser utilizadas para evitar que os usuários fiquem expostos a estes riscos.

1.2 DELIMITAÇÃO DA PESQUISA

A delimitação da pesquisa será relacionada à tecnologia *Bluetooth* e vai abranger um breve histórico sobre a tecnologia, as características técnicas do padrão, que incluem o controle de acesso ao meio, o espectro eletromagnético, formato de quadros e funcionamento nas camadas física e de enlace do modelo de referência *Open Systems Interconnection* (OSI). Será abordado também os aspectos de segurança da tecnologia e da sua utilização. O padrão IEEE 802.15 é o assunto principal do trabalho.

1.3 PROBLEMA E PREMISSAS

Existem vulnerabilidades de segurança na tecnologia *Bluetooth* ? É possível invadir um dispositivo que contenha a tecnologia *Bluetooth* ? *O* que pode ocorrer se uma pessoa de má índole conseguir invadir um dispositivo através da rede

Bluetooth? Se as respostas a estas perguntas forem positivas, o que podemos fazer para evitarmos estes ataques?

Conforme citação de (RUFINO, 2007) a tecnologia *Bluetooth* permite recursos iguais as redes convencionais, como comunicação em grupo, comunicação com redes que utilizam o endereçamento IP entre outros recursos, com isso podemos dizer que como as redes convencionais tem vulnerabilidades e estão propicias a sofrerem ataques as redes Bluetooth também estão vulneráveis.

Um dos problemas relacionados a esta tecnologia é que por padrão equipamentos de alguns fabricantes vem com a opção do Bluetooth ativada de fabrica e os usuários acabam não desativando esta opção ou quando vem desativada de fabrica os usuários a ativam e esquecem de desativar, sendo uma brecha de segurança (RUFINO, 2011).

1.4 OBJETIVOS

Neste tópico será abordado qual o objetivo geral e objetivos específicos desta monografia.

1.4.1 OBJETIVO GERAL

Identificar as vulnerabilidades de segurança e propor formas para se proteger de ataques.

1.4.2 OBJETIVOS ESPECÍFICOS

- Fazer um levantamento da parte teórica da tecnologia *Bluetooth*;
- Identificar as vulnerabilidades de segurança nas redes sem fio – *Bluetooth*;

- Analisar os *softwares* necessários para a pesquisa de campo;
- Analisar as ferramentas disponíveis para que se consiga identificar as vulnerabilidades de segurança nas redes sem fio do padrão IEEE 802.15;
- Identificar e apresentar formas de corrigir as falhas de segurança do *Bluetooth*;
- Descrever como esta sendo utilizada a tecnologia Bluetooth atualmente e como ela esta presente no cotidiano das pessoas.

1.5 JUSTIFICATIVA

Atualmente as tecnologias de redes sem fio estão cada vez mais sendo utilizadas no cotidiano das pessoas, pelo fato de ser uma tecnologia que proporciona mobilidade, praticidade, conexões mais rápidas e estáveis e preços mais acessíveis.

A tecnologia *Bluetooth,* que é uma das tecnologias de redes sem fio, está cada vez mais presente em equipamentos eletrônicos sendo utilizada de várias formas, muitas vezes nestes equipamentos eletrônicos elas já vem ativadas por padrão sendo uma brecha para ataques a estes dispositivos. Muitas pessoas acreditam que pelo *Bluetooth* ser uma tecnologia de pequeno alcance e utilizar protocolos simples não estão sujeitas a ataques de pessoas que desejem roubar seus dados pessoais. Este trabalho esta sendo elaborado com o intuito de alertar e mostrar a estas pessoas que ataques a estes dispositivos, que utilizam a tecnologia *Bluetooth*, são possíveis e podem ocorrer em uma distancia maior do que imagina e com certa facilidade.

1.6 PROCEDIMENTOS METODOLÓGICOS

Esta pesquisa será de natureza aplicada e estudo de campo. Segundo Gil (2007), estudo de campo é um aprofundamento maior das questões propostas apresentando fatos e relatos ocorridos em uma comunidade ou local de estudo, será analisado as vulnerabilidades da rede *Bluetooth* utilizando alguns *softwares* livres e

seus resultados serão apresentados no decorrer do trabalho e em cima destes dados será analisado formas de se proteger a esses possíveis ataques.

1.7 EMBASAMENTO TEÓRICO

Como auxilio para o desenvolvimento bibliográfico deste trabalho em relação a segurança das redes *Bluetooth* será utilizado livro o autor Rufino (2007 e 2011), para outros assuntos relacionados a *Bluetooth* e redes sem fio se destacam Rufino (2007), Tanenbaum (2003), Rappaport (2009), Stallings (2003), Kurose e Ross (2006), Morimoto (2008) e Comer (2007).

1.8 ESTRUTURA

A estrutura desta monografia é composta por quatro etapas ou capítulos. O capitulo de número um trata-se da introdução, serão apresentados o tema, suas delimitações e problemas, os objetivos gerais e específicos, a justificativa, os procedimentos metodológicos e a estrutura da monografia.

No capitulo de número dois será abordado à parte bibliográfica ou teórica da monografia abrangendo neste capitulo os itens mencionados a seguir. Sobre o padrão IEEE 802.15 será escrito sobre seu histórico, topologia, características, pilha de protocolos, estrutura de quadro, como esta sendo utilizado atualmente e sua segurança, ainda neste capitulo será abordado sobre o modelo TCP/IP e suas camadas, camada física, acesso a rede, inter rede, aplicação e transporte. Ainda dando continuidade ao capitulo será abordado a topologia e o controle de acesso ao meio das redes sem fio e finalizando este capitulo será abordado o espectro eletromagnético *frequency hopping spread spectrum* (FHSS), *direct sequence spread spectrum* (DHSS) e *orthogonal frequency division multiplexing* (OFDM).

No capitulo de número três será apresentado a analise dos softwares utilizados para a pesquisa de campo, problemas que puderem ocorrer durante os testes, como utilizar os softwares, o que eles podem fazer, quais são as

vulnerabilidades que eles conseguem demonstrar em relação ao Bluetooth e as possíveis formas de se corrigir as vulnerabilidades demonstradas na utilização dos softwares.

No último capitulo de número 4 será abordado as considerações finais, conclusão e outros aspectos pré-textuais da pesquisa realizada.

2 REFERENCIAIS TEÓRICOS

Este capítulo de número 2 abordará a parte teórica da pesquisa, a história do padrão IEEE 802.15, topologia, características, pilha de protocolo, estrutura dos quadros, como é utilizada na atualidade, o modelo de referencia tcp/ip e suas camadas, redes sem fio e espectro eletromagnético.

2.1 PADRÃO IEEE 802.15

O padrão IEEE 802.15 é nomeado de *Bluetooth*, nome derivado do rei viking do século X da Dinamarca chamado Harald Blatand vulgo *Bluetooth*, ganhou este apelido devido aos seus dentes azuis (RAPPAPORT, 2009) (RUFINO, 2007). O rei Harald conseguiu unir a Dinamarca e a Noruega usando o diálogo como estratégia, este padrão veio para unificar as tarefas de conectividade dos aparelhos, ser uma tecnologia de baixo custo, baixa complexidade e pouca potência (cerca de 10 metros por padrão e em outros equipamentos podendo chegar a quilômetros de distância), possivelmente a indicação do nome *Bluetooth* foi feita pela empresa Ericsson que em 1994 tinha interesse em conectar seus aparelhos de telefone móveis a outros dispositivos, junto com outras quatro empresas criaram um grupo chamado *Special Interest Group* (SIG), com objetivo de desenvolver um padrão para conectar dispositivos usando redes sem fio de baixo alcance, atualmente este grupo conta com mais de duas mil empresas (RAPPAPORT, 2009) (RUFINO, 2007) (TANENBAUM, 2003).

2.1.1 CARACTERISTICAS

O *Bluetooth* opera na camada ISM 2.4 GHz, mesma camada da rede sem fio wireless, foi desenvolvido para transportar dados e voz por dispositivos móveis, mais hoje são utilizados por outros equipamentos que não são móveis como impressoras.

Seus canais de banda tem largura de 1MHz e taxa de saltos de até 1600 saltos(RAPPAPORT, 2009) (RUFINO, 2007). A varredura em procura de outros dispositivos que possuem a tecnologia é feito de 2 formas, *page* e *inquiry*, a primeira envia mensagens aguardando uma resposta para fazer conexão e a segunda envia mensagem para o ISM tentando reconhecer equipamentos que estão dentro da mesma área de cobertura com características iguais, a cobertura de varredura pode variar dependendo da potência, a seguir a tabela 1 mostra as potências e área de cobertura (RUFINO, 2007).

TABELA 1 - POTÊNCIAS X ÁREA DE COBERTURA

Classe	Potência (mV)	Potência (Dbm)	Área de cobertura
Classe 1	100	20	100 metros
Classe 2	2,5	4	10 metros
Classe 3	1	0	10 centímetros

Fonte: Rufino 2007

2.1.2 TOPOLOGIA

A unidade básica de uma rede *Bluetooth* é a rede *piconet*, nela podem conter no máximo 8 dispositivos, sendo um o concentrador e os demais clientes em uma distância de 10 metros por padrão, como mostra a figura 1 (RUFINO, 2007) (TANENBAUM, 2003). A *piconet* pode ter até 255 nós inativos em sua rede, estes foram comutados para um estado de baixa energia para poupar suas baterias, neste estado os dispositivos apenas respondem a um sinal enviado pelo concentrador, toda comunicação em uma rede *piconet* é feita entre o concentrador e o cliente não é possível comunicação direta entre clientes (TANENBAUM, 2003).

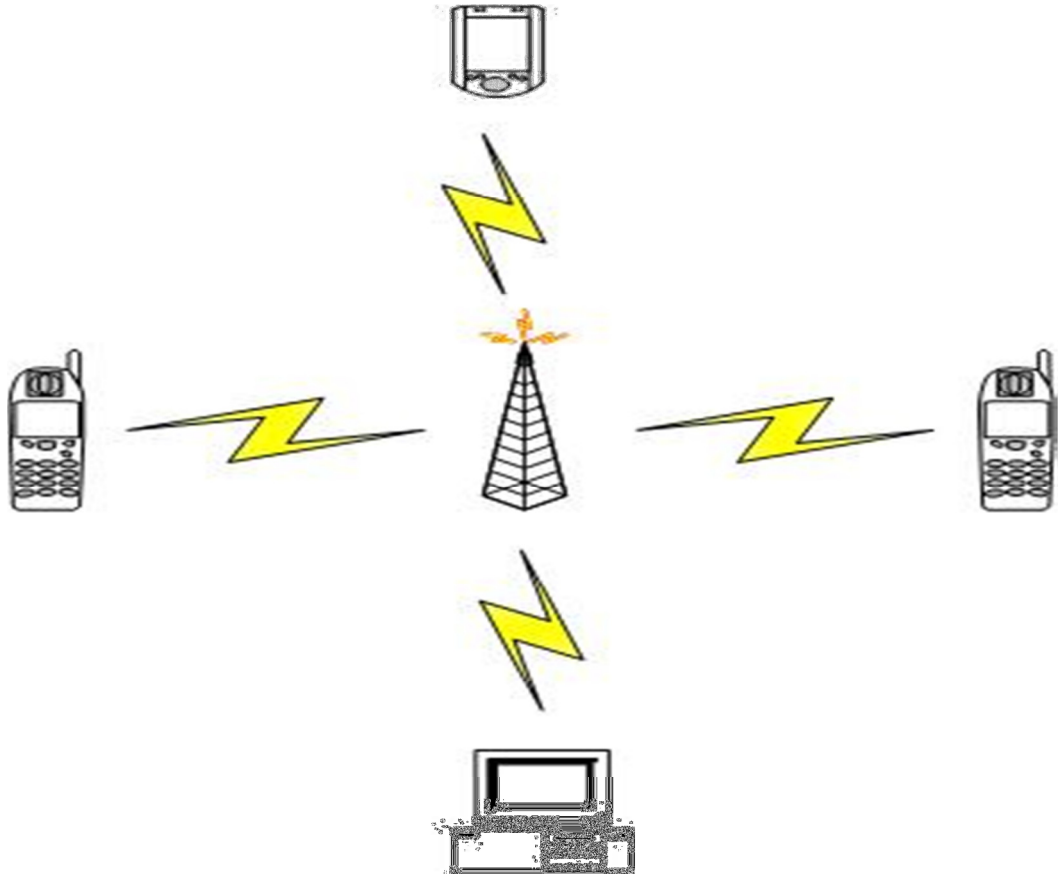

Figura 1 - Rede Piconet
Fonte: do autor

Redes *piconets* podem se interconectar em no máximo 10 redes compondo uma rede maior, assim um dispositivo pode estar conectado em mais de um concentrador, como se vê na figura 2, este conjunto de *piconets* é chamado de *scatternet* (RUFINO, 2007).

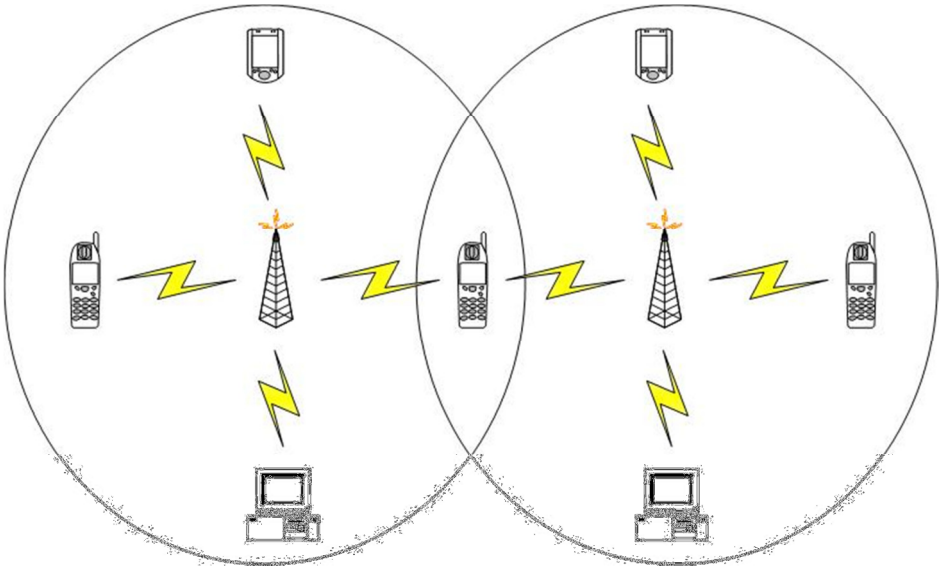

Figura 2 - Rede sacatternet

Fonte: do autor

2.1.3 PILHA DE PROTOCOLOS

A pilha de protocolos do *Bluetooth* são agrupados em quatro camadas básicas, são elas:

- Camada física de rádio;
- Camada de enlace de dados ou banda base;
- Camada de *middleware*;
- Camada de aplicação.

A estrutura das camadas citadas acima segue o padrão do modelo TCP/IP e não o modelo OSI (TANEMBAUM, 2003).

A camada mais inferior é a camada física de radio, ela correspondente a camada física do modelo OSI. Esta camada é responsável pela transmissão e modulação de rádio tendo um sistema de baixa potência com alcance de 10 metros e usando a banda de 2,4GHz dividida em 79 canais de 1MHz, esses por sua vez utilizam o espectro de dispersão de saltos de freqüência de 1600 hops/s e um tempo de parada de pequeno valor. Por o *Bluetooth* estar na mesma faixa de ISM do padrão 802.11 e sendo mais rápido em seus saltos, é provável que ele arruíne as transmissões do 802.11, o IEEE esta procurando uma forma de contornar este

problema, mais como os dois padrões usam a banda ISM pelo mesmo motivo, não é exigido nenhum licenciamento nesta banda, fica difícil de contornar este problema (TANENBAUM, 2003).

A camada de banda base inclui elementos da camada física e controla os slots de tempo e como eles são agrupados em quadros esses por sua vez são transmitidos sobre um canal lógico chamado enlace. Existem 2 tipos de enlace o *asynchronous connection-less* (ACL) usado por dados comutados com intervalos irregulares, são enviados pela camada *Logical Link Control and Adaptation Protocol* (L2CAP) no lado de transmissão e são entregues na camada L2CAP de recepção essa transmissão não utiliza nenhum tipo de garantia, sendo assim os dados podem ser perdidos havendo a necessidade de transmiti-los novamente. O outro enlace é S*ynchronous Connection Oriented* (SCO) utilizados em serviços que necessitam dados em tempo real, utiliza correção de erros antecipada proporcionando confiabilidade na entrega dos dados, não sendo necessária a retransmissão dos dados (TANENBAUM, 2003).

A camada L2CAP aceita pacotes de ate 64 KB e os divide em quadros para a transmissão, determina a qual protocolo da camada superior vai ser entregue, trabalha com a qualidade dos serviços desde quando os enlaces são estabelecidos e até durante a operação normal e negocia o tamanho máximo de carga útil permitido, estas são as principais funções da camada L2CAP (TANEMBAUM, 2003).

A camada de aplicação ou programa de descoberta de serviço é possível realizar consultas das informações de dispositivos, serviços e suas características sendo possibilitando o estabelecimento de uma conexão entre dispositivos (STALLINGS, 2005).

Além dos protocolos da camada básica outros protocolos são utilizados pelo *Bluetooth* como protocolo de substituição de cabo, protocolo de controle de telefonia e os protocolos adotados.

O *Radio Frequency Communications* (RFCOMM) é o protocolo de substituição do cabo, ele apresenta uma porta serial virtual possibilitando a substituição dos cabos seriais. Este protocolo fornece transporte de dados binários emulando sinais de controle *Electronic Industries Association*-232 (EIA-232) ou *Recommended Standard*-232(RS-232) sobre a camada de banda base (STALLINGS, 2005).

O protocolo de controle de telefonia é o *Telephony Control Protocol-Binary* (TCS BIN), ele é baseado em bits e faz o controle da chamada para o estabelecimento de chamadas de fala e dados entre os dispositivos (STALLINGS, 2005).

Os protocolos adotados são protocolos de terceiros incorporados na arquitetura do *Bluetooth,* os protocolos adotados são:

- *point-to-point protocol* (PPP), protocolo padrão de *Internet*;
- TCP/UDP/IP, protocolos básicos da família TCP/IP;
- OBEX, protocolo usado para a troca de objetos;
- *Wireless Application Environment* (WAE)/ *Wireless Application Protocol* (WAP), protocolos de aplicação sem fio (STALLINGS, 2005).

2.1.4 ESTRUTURA DE QUADRO

Inicia com o código de acesso que é o identificador do concentrador para que os clientes possam conhecer o destino de cada trafego, o tamanho deste campo é de 72 bits. O próximo campo é o de cabeçalho com o tamanho de 54 bits contendo campos da subcamada *Media Access Control* (MAC), dentro do cabeçalho encontramos os seguintes campos:

- Endereço: indica qual é o destino do quadro, tamanho 3 bits;
- Tipo: identifica o tipo de quadro (ACL, SCO, nulo), tamanho 4 bits;
- Bit fluxo: identifica se o *buffer* está cheio ou não, tamanho 1 bit;
- Bit confirmação: transporta uma mensagem *Acknowledgement* (ACK) em um quadro, tamanho 1 bit;
- Bit sequencia: numera os quadros para detectar retransmissões, tamanho 1 bit.
- Total de verificação: tamanho 8 bits.

No total este cabeçalho tem um total de 18 bits, para chegar aos 54 bits mencionados anteriormente é necessário que este cabeçalho seja repetido três vezes. O receptor examina as três cópias do cabeçalho, caso as três sejam iguais o bit será aceito caso contrario vence a opinião da maioria (TANEMBAUM, 2003).

O campo de dados tem vários formatos tendo como mais simples os quadros SCO com tamanho de 240 bits. O tamanho dos quadros pode ser representado de três formas distintas 80, 160 ou 240 bits de carga útil real e os restantes dos bits são usados para a correção de erro.

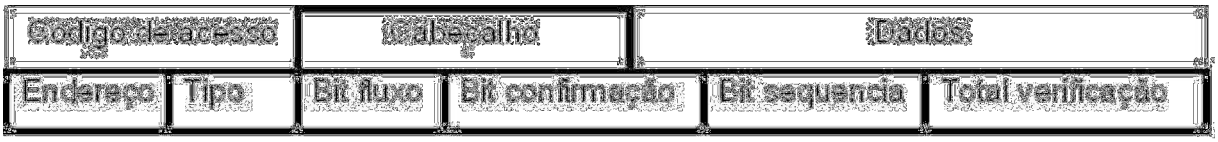

Figura 3 - Representação de um quadro de dados.

Fonte: Tanembaum, 2003.

2.1.5 UTILIZAÇÃO

A tecnologia *Bluetooth* atualmente está presente em diversos equipamentos moveis, entre eles se destacam *Personal Computers* (PCs), *Personal Digital Assistant* (PDA), Celulares, relógios de pulso, televisores, câmeras de vídeos e outros dispositivos eletrônicos.

Um dos locais que mais será utilizado esta tecnologia será em escritórios de negócios, carros, shoppings, hotéis e etc. Hoje em dia já é possível em algumas lojas, por exemplo, usuários sincronizar suas listas de compras com um mapa atual da loja, obtendo as direções corretas do local onde estão cada item de sua lista. Hospedes de hotéis tem maior facilidade de utilizar equipamentos como impressoras e outros dispositivos, ajuda também a descobrir com maior facilidade qual é seu quarto entre outras facilidades. Os fabricantes de automóveis vêm adicionando em seus carros dispositivos *Bluetooth* para manter conectado o usuários sem a necessidade de utilizar as mãos para atender telefones celulares. Existem estudos para que o *Bluetooth* seja utilizado também na medicina, os monitores cardíacos enviariam o sinal para os telefones moveis dos pacientes auxiliando hospitais e médicos no tratamento (ERASALA, YEN, 2002).

2.1.6 SEGURANÇA

Os sinais de rádio podem ser facilmente interceptados, a tecnologia *Bluetooth* utiliza técnicas de segurança de autenticação e criptografia para tentar evitar a espionagem ou a falsificação de mensagens de *spoofing* (ERASALA, YEN, 2002).

As redes *Bluetooth* estão expostas aos mesmos ataques que todas as redes sem fio da atualidade, é possível identificar quais equipamentos estão na rede, poder receber ataques de negação de serviço, captura e escuta de trafego e outras tipos de ataques conhecidos.

2.1.6.1 FERRAMENTAS DE ATAQUE

Atualmente existem várias ferramentas capazes de interferir em um trafego existente ou que consiga se passar por outro dispositivo. Muitas destas ferramentas estão disponíveis na *Internet* e geralmente funcionam em sistemas operacionais livres, a seguir serão abordadas algumas ferramentas com as características citadas acima.

Com a ferramenta *blooover* (Junção de *Bluetooth + hoover*) é possível identificar dispositivos e fazer invasões aos mesmos como: redirecionar chamadas, copiar agenda telefônica, copiar e enviar mensagens *Short Message Service* (SMS) entre outras funcionalidades, a figura 4 ilustra a tela do programa onde é possível configurar os ataques disponíveis (RUFINO, 2007).

Figura 4 - Tela de configuração de vulnerabilidades

Fonte: Rufino, 2007.

Uma ferramenta que pode ser utilizada na identificação de componentes de uma rede *Bluetooth* é a ferramenta BlueZ, é uma ferramenta feita para sistemas operacionais Linux e é muito utilizada para preparação de um ataque a uma rede ou dispositivo. Com o comando hciconfig é possível verificar as configurações da interface a ser utilizada no Linux. O comando hcitool usando a opção *scan* permite descobrir dispositivos na mesma área de cobertura, emitindo sinais característicos de uma rede *Bluetooth*. Outra ferramenta muito utilizada por quem usa o sistema operacional Mac OSX é a ferramenta chamada iStumbler, ela é bem simples e mais voltada para analise de redes sem fio, nela é possível observar varias informações sobre o dispositivo encontrado, como demonstra a figura 5 a seguir (RUFINO, 2011).

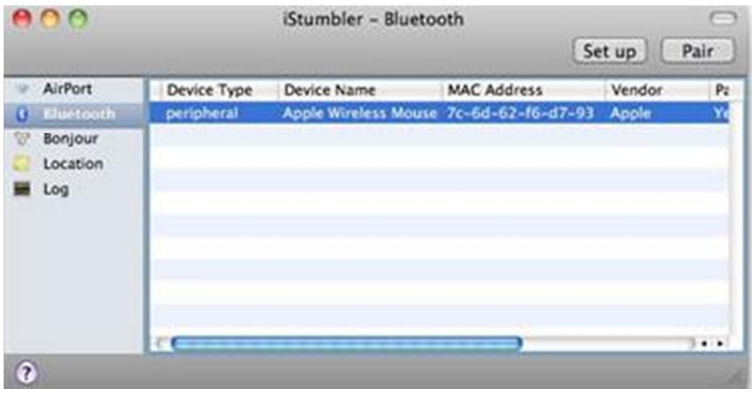

Figura 5 - iStumbler identificou um dispositivo nas proximidades

Fonte: Rufino, 2011

Para evitar que ferramentas, como as apresentadas anteriormente, consigam obter informações sobre um determinado dispositivo *Bluetooth* é possível configurar no dispositivo uma opção para bloquear a propagação de sinais na presença de equipamento, assim para acessar ou descobrir informações do dispositivo só é possível por equipamentos que já conheça o endereço deste dispositivo. A figura 6 ilustra um aparelho com a opção de visualização para todos (RUFINO, 2011).

Figura 6 - Equipamento com opção de visualização para todos

Fonte: http://www.nokiatividade.com/aplicativo-quickbt-Bluetooth-onoff-com-um-toque/

O desligamento da opção de visualização do telefone trás certa segurança à proteção dos dispositivos que necessitem estar disponíveis para conexão e ao mesmo tempo estão protegidos contra ataques. Mas esta segurança é irrisória, pois se o equipamento estiver se comunicando com outro pode ser descoberto por ferramentas que testam endereços sequenciais, é o caso da ferramenta chamada

RedFang, é uma ferramenta simples que pode realizar ataques caso seja de conhecimento do atacante o endereço do dispositivo ou ela realiza uma varredura numa sequência de possíveis endereços, fazendo o teste de um em um. Ele consegue varrer até 256 endereços em aproximadamente 10 minutos dependendo do equipamento que esta sendo utilizado para realizar a varredura (RUFINO, 2011).

2.1.6.2 AUTENTICAÇÃO

Uma das formas mais comuns de autenticação e estabelecimento de conexão dos equipamentos de redes sem fio é a utilização de uma senha, mais com a evolução das ferramentas atuais isso pode ser subvertido de varias formas.

Uma das formas é presumir o *personal identification number* (PIN) dos equipamentos, alguns equipamentos vêm de fábrica com um PIN padrão e ao detectar um dispositivo na varredura é possível um atacante utilizar esse PIN previamente conhecido para roubar informações.

Outra forma é utilizar o método de força bruta, em geral os PINs vem de fábrica com 4 bytes de tamanho, com isso mesmo que o atacante não conheça o PIN padrão é possível que por este ataque de força bruta ele consiga obter esta informação. Mesmo que o usuário troque o PIN dificilmente ele irá colocar um tamanho maior de 4 bytes, com isso o ataque ainda é eficiente ou pelo menos possível (RUFINO, 2011).

2.1.6.3 TIPOS DE ATAQUES

Um dos ataques mais conhecidos nas redes é o ataque de negação de serviço, onde com um comando é possível enviar vários pacotes sem esperar resposta, ele é usado para testes de desempenho de rede mais também pode comprometer um equipamento ou uma rede toda, não se trata de invadir a rede mais sim de fazer com que seus serviços parem ou o equipamento seja reinicializado.

Outro ataque baseado em dificultar a comunicação dentro de uma rede ou não permitir a comunicação é o ataque de geração de ruído. Para ter êxito neste tipo de ataque, o atacante deve equipamentos com potência suficiente para preencher totalmente ou pelo menos grande parte do espectro utilizado. Outra forma de conduzir este ataque é baseando-se na repetição de saltos, uma vez que o receptor e o transmissor combinam seus saltos numa mesma frequência e sequencia, seria necessário apenas identificar a sequencia correta e sincronizar o envio do ruído com o trafego legitimo. Ferramentas que podem ser utilizadas para realizar escuta de trafego são: Hcidump, tcpdump, wireshark entre outras (RUFINO, 2011).

Outra forma que os atacantes podem invadir equipamentos ou redes é pela identificação do nome, usuários podem incluir equipamentos ou redes como confiáveis em suas listas em geral a associação de dispositivos é feita pelo nome + seu endereço BD, mas algumas implementações utilizam apenas o nome para identificar um equipamento, este nome pode ser modificado a qualquer momento tornando este tipo de associação mais frágil em sua segurança (RUFINO, 2011).

Outra situação de ataque possível é o atacante simular mensagens de texto ou multimídia levando o usuário a crer que esta confirmando o recebimento de uma mensagem, mas na verdade esta aceitando a conexão de outro dispositivo remoto.

O padrão *Bluetooth* renomeou o endereço MAC para o nome *Bluetooth Device Address* (BDADDR), mais a teoria é a mesma do endereço MAC, identificar individualmente cada dispositivo. Atacantes conseguem alertar este endereço facilmente usando *softwares* livres como o Spooftooph, podendo forjar completamente outro dispositivo (RUFINO, 2011).

2.2 MODELO DE REFERÊNCIA TCP/IP

O modelo de referência TCP/IP nasceu de estudos, pesquisas e desenvolvimentos de protocolos em uma rede experimental chamada *Advanced Research Projects Agency Network* (ARPANET) que foi patrocinada pelo departamento de defesa dos estados unidos, em pouco tempo esta rede já estava conectada a centenas de universidades e repartições públicas, com isso começaram

a aparecer problemas com os protocolos utilizados sendo necessária a criação de uma nova arquitetura de referencia (STALLINGS, 2005) (TANEMBAUM, 2003).

Diferentemente do modelo OSI, não existe um modelo de protocolo oficial para a arquitetura TCP/IP ela é dividida em cinco camadas:

- Camada de aplicação;
- Camada de transporte;
- Camada de inter-rede;
- Camada de acesso a rede;
- Camada física (STALLINGS, 2005).

2.2.1 CAMADA FÍSICA

A camada física é a camada mais baixa, nela são tratados os meios de comunicação que serão utilizados para trafegar os dados e suas especificações de características do meio, taxa de dados, natureza dos sinais e outras especificações relacionadas (STALLINGS, 2005).

2.2.2 CAMADA DE ACESSO A REDE

Segundo Stallings (2005, p. 84), “A camada de acesso a rede trata da troca de dados entre um sistema final (servidor, estação de trabalho, etc.) e a rede à qual está conectado.” O dispositivo que esta enviando os dados deve fornecer o endereço do dispositivo que irá receber os dados, assim a rede pode rotear os dados até o dispositivo de destino correto. Pode ser utilizado um *software* especifico para esta camada caso seja necessário enviar dados com algum tipo de prioridade, mais a utilização deste *software* depende da rede utilizada para o trafego pois existem diferentes padrões de comutação de serviços, comutação de pacotes, *Local Area Network* (LAN) e outros. Ainda segundo Stallings (2005, p. 84) “faz sentido separar essas funções que tem acesso a rede em uma camada separada”.

2.2.3 CAMADA DE INTER-REDE

A Camada de inter-rede é responsável pelo roteamento dos dados entre redes distintas atravessando varias redes interconectadas, seu trabalho é fazer com que os dados cheguem a seus destinos independentemente da ordem de chegada, caso cheguem em ordem diferente do que foi enviado os protocolos da camada superior é responsável pela reorganização. O protocolo usado para navegar entre redes distintas é o protocolo *Internet protocol* (IP). Ele é implementado em vários dispositivos inclusive nos roteadores, que tem a função de conectar duas redes e repassar os dados de uma para outra (TANEMBAUM, 2003) (STALLINGS, 2005).

Um exemplo simples de como funciona a camada de inter-rede é uma pessoa deixando várias cartas empilhadas e numeradas em uma determinada sequência para que sejam enviadas à um endereço em outro país. Provavelmente estas cartas passaram por outros países, receberão outros selos e chegaram até o destino na mesma ordem que foi enviada ou não, de qualquer forma essas etapas do envio da carta se tornam transparente para o usuário assim como na rede o pacote passa por vários roteadores e recebe vários “selos” e também é transparente para o usuário (TANEMBAUM, 2003).

2.2.4 CAMADA DE TRANSPORTE

Na camada de transporte são encontrados os protocolos que garantem que a mensagem enviada pelo remetente seja entregue ao destinatário e chegue na mesma ordem que foi enviada o protocolo mais utilizado nesta camada para esta função é o *Transmission Control Protocol* (TCP) (STALLINGS, 2005).

O protocolo TCP é orientado a conexão confiável permitindo entrega dos dados sem erros. Ele fragmenta o fluxo de bytes de entrada e passa cada uma delas para a camada de inter-redes e no destinatário o TCP monta a mensagem novamente. O TCP também atua no controle de fluxo impedindo que um transmissor

sobrecarregue um receptor com um volume de dados maior do que ele pode manipular (TANEMBAUM, 2003).

Outro protocolo utilizado nesta camada é o *User Datagram Protocol* (UDP) ele não garante entrega, nem que a sequência dos dados enviados seja a mesma ou que o arquivo seja duplicado. Ele permite apenas que um processo envie mensagens a outros processos.

2.2.5 CAMADA DE APLICAÇÃO

A camada de aplicação é a camada que da suporte a maioria das aplicações dos usuários. É nela também que se encontram os protocolos de níveis mais altos como TELNET, *File Transfer Protocol* (FTP), *Simple Mail Transfer Protocol* (SMTP) entre outros (TANEMBAUM, 2003).

TELNET é o protocolo de acesso remoto a outro computador possibilitando trabalhar neste equipamento. FTP é o protocolo de transferência de arquivos. SMTP protocolo responsável pelo envido de mensagens (TANEMBAUM, 2003).

2.3 REDES SEM FIO

As redes sem fio até pouco tempo, eram pouco utilizadas devido ao valor alto de seus dispositivos, baixas velocidade de dados e preocupações com a segurança, à medida que esses problemas foram resolvidos, as redes sem fio cresceram rapidamente (STALLINGS, 2005). Os primeiros dispositivos de redes sem fio surgiram na década de 80 com o intuito de substituírem as redes cabeadas, devido a redução de custos com cabeamento e facilidade para realocação e outras modificações na estrutura de rede. A rede sem fio tem a topologia de rede semelhante com as redes com fio. O switch central é substituído pelo ponto de acesso, a diferença é que são utilizadas transmissões e antenas ao invés de cabos (MORIMOTO, 2008). Existem poucas vantagens em utilizar uma rede sem fio para desktops, pois estes equipamentos não precisão sair do lugar com tanta freqüência,

as redes sem fio se adaptam melhor com equipamentos como notebook, palmtops, e outros equipamentos que precisão de mobilidade (MORIMOTO, 2008). As redes sem fio servem como alternativa mais eficaz e atraente em alguns ambientes como, construções com grandes áreas livres, construções históricas onde não é possível abrir novos furos para passagem de cabeamento, pequenos escritórios onde a instalação com fios teria um custo muito elevado, outro uso das redes sem fio é a conexão entre dois prédios próximos (STALLINGS, 2005)

As redes em geral precisam atender a alguns requisitos como: capacidade de cobrir distâncias curtas, total de conectividade entre os dispositivos conectados na rede e capacidade de broadcast, além disso, as redes sem fio têm outros requisitos importantes conforme elenca Stallings (2005) os itens abaixo:

Vazão: maximizar a capacidade do meio sem fio de forma mais eficaz possível utilizando o protocolo de controle de acesso.

Número de nós: capacidade de aceitar vários nós.

Conexão com a rede de *backbone*: é facilmente obtido com o uso de módulos de controle que se conectam as 2 redes, com fio e sem fio.

Área de serviço: área de cobertura da rede em diâmetros.

Consumo de bateria: os trabalhadores usam maquinas de trabalho que são reabastecidas por baterias que possuem necessidade de longa duração quando são usadas em dispositivos sem fio. Isto demonstra que não é apropriado a utilização de um protocolo MAC nessas ocasiões.

Robustez e segurança da transmissão: uma rede sem fio é capaz de sofrer interferências e com facilidade de espionagem. Para projetar uma rede segura é preciso de um ambiente estável que proporcione segurança contra espionagem.

Operação de redes em local comum: nos locais que existem redes sem fio, há probabilidade de sofrerem interferências de outras redes. Devido a esta interferência é possível uma rede especifica não operar no local.

Operação livre de licença: os usuários optam em usar uma rede sem fio a usar uma licença assinada para obter uma freqüência usada pela rede.

Handoff/*roaming*: permite que dispositivos móveis se movam de uma célula para outra.

Configuração dinâmica: a rede deve permitir adição, exclusão e relocação dinâmica e automatizada sendo transparente para os usuários.

Ainda segundo Stallings (2005), as redes sem fio são categorizadas devido a técnica de transmissão utilizada, as categorias são:

Redes Infravermelhas: é limitada a um determinado local, pois não penetra em paredes.

Redes de amplo espectro: são redes que operam dentro das bandas ISM de modo de não precisar de nenhum licenciamento para seu uso.

Microondas de banda estreita: operam em freqüência de microondas, sem usar amplo espectro. Algumas operam em bandas que necessitam de licenciamento e outras operam em bandas ISM não-licenciadas.

2.3.1 TOPOLOGIA

As redes sem fio têm dois tipos de topologia, uma topologia de ponto a ponto chamada rede AD HOC onde os dispositivos se comunicam diretamente e a rede infra estruturada onde a comunicação entre os dispositivos são feitas indiretamente, sendo necessário um concentrador para permitir a integração dos dispositivos (STALLINGS, 2005) (MORIMOTO, 2008) (KUROSE; ROSS, 2006).

2.3.1.1 REDE AD HOC

A rede AD HOC é uma rede que não tem um concentrador centralizado, é uma rede não hierárquica montada geralmente para atender necessidades imediatas, onde não precisem acessar a *Internet* ou outros grupos de trabalho. Sua rede de cobertura é menor existindo uma limitação ao controle de acesso, os próprios dispositivos conectados a esta rede devem prover serviços de roteamento, endereços, tradução de endereços e outros serviços. Um exemplo de utilização desta rede é uma reunião de negócios onde todos os integrantes da reunião possuem um notebook ou qualquer dispositivo móvel e os integrantes conectam seus computadores em uma rede ad hoc pelo período que durar a reunião (STALLINGS, 2005) (MORIMOTO, 2008) (KUROSE; ROSS, 2006).

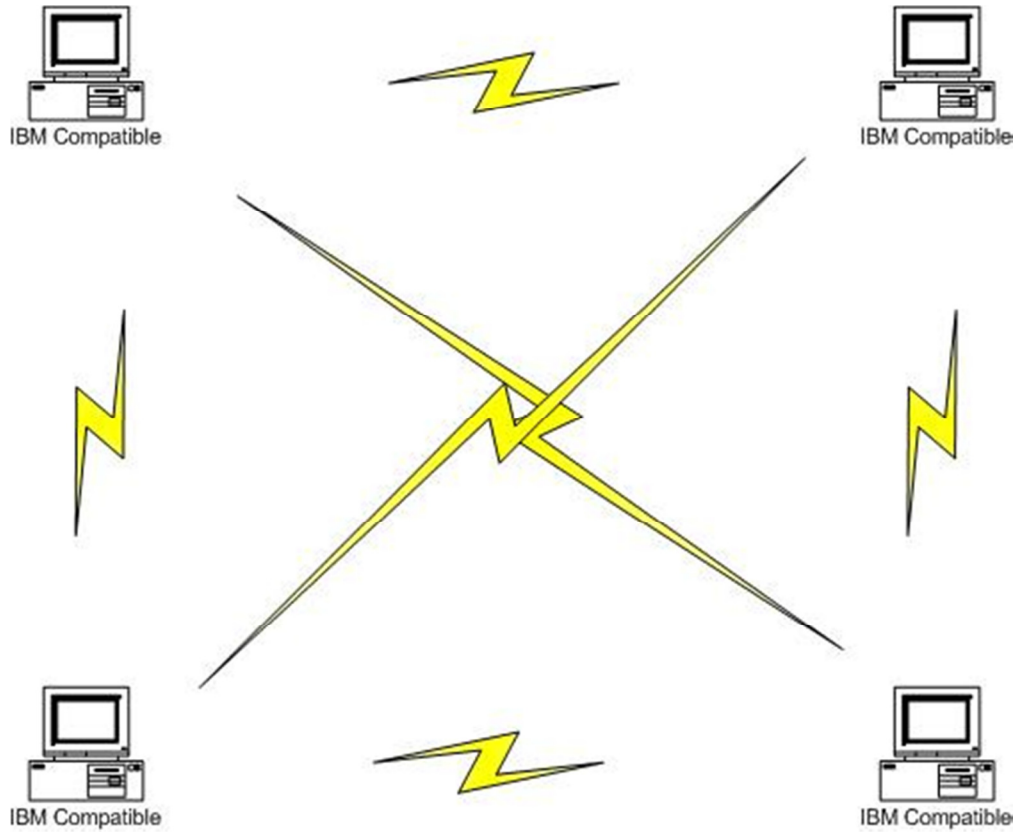

Figura 7 - Exemplo de uma rede AD HOC

Fonte: Stallings, 2005.

A figura 7, a cima, exemplifica uma rede AD HOC, que não depende de um concentrador para trocar informações, pois as informações são trocadas diretamente entre os dispositivos. Esse conjunto forma uma célula denominada *Independent Basic Service Set* (IBSS) (STALLINGS, 2005).

2.3.1.2 REDE DE INFRAESTRUTURA

A rede de infraestrutura é a rede que possui um concentrador centralizado e todos os serviços de rede são fornecidos pela rede a qual estiverem conectados, permite a integração de diversos dispositivos e diferentes grupos de trabalho. A

figura 8, a seguir, exemplifica a topologia de rede de infraestrutura (KUROSE; ROSS, 2006).

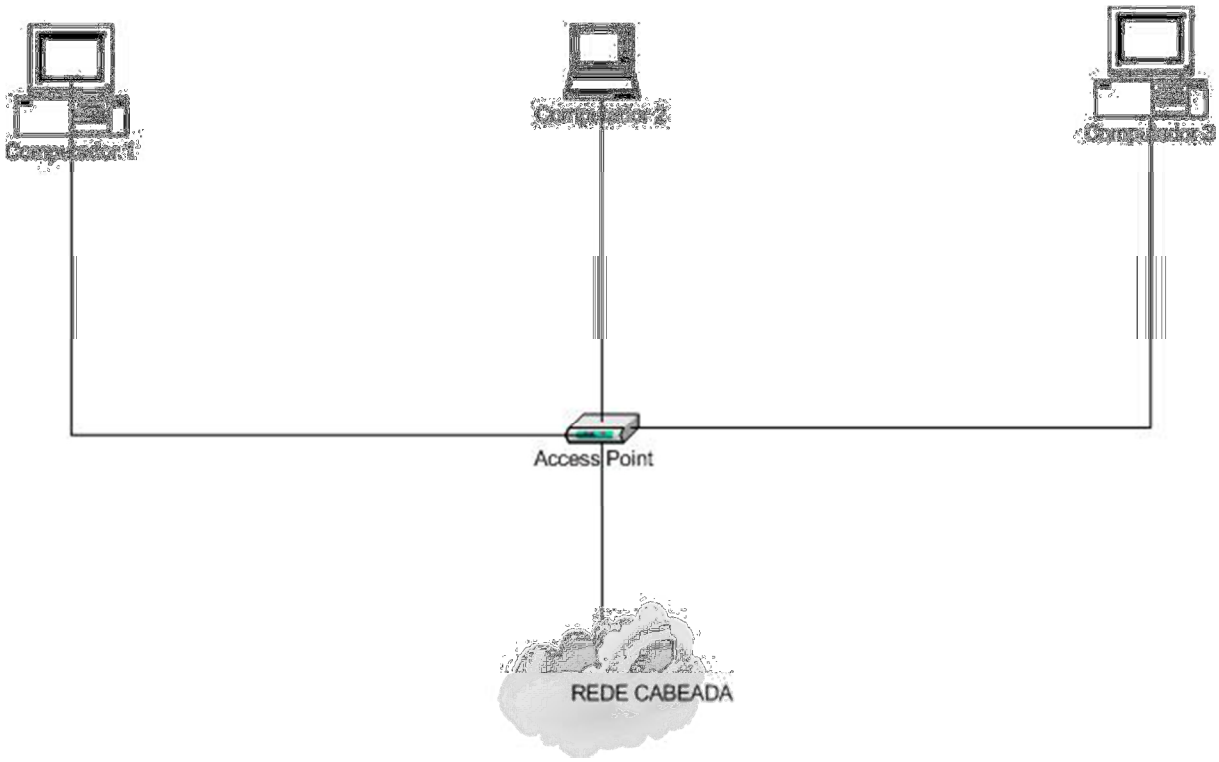

Figura 8 - Exemplo de uma rede de infraestrutura

Fonte: Stallings, 2005.

A figura 8, a cima, ilustra uma rede de infraestrutura onde o *access point* (AP) é interligado a uma rede cabeada. O conjunto da rede, computadores ou outros dispositivos móveis e o AP, constituem em uma célula denominada de *basic service set* (BBS) e o conjunto da rede cabeada é denominado de *Extended Service Set* (ESS) (KUROSE; ROSS, 2006).

2.3.2 CONTROLE DE ACESSO AO MEIO (CSMA/CA)

As redes cabeadas e as redes sem fio tem um objetivo em comum que é o controle de acesso ao meio, nas redes cabeadas é utilizado o protocolo *Carrier*

Sense Multiple Access with Collision Detection (CSMA/CD) e as redes sem fio utilizam o protocolo *Carrier sense multiple access with collision avoidance* (CSMA/CA), que será abordado no decorrer deste trabalho (KUROSE; ROSS, 2006).

O protocolo CSMA/CA significa acesso múltiplo por detecção de portadora, este protocolo escuta o meio antes de transmitir, caso o meio esteja ocioso ele transmite os dados, mas não escuta enquanto faz a transmissão, neste caso a transmissão pode ser destruída devido a uma interferência. Se o meio estiver ocupado ele aguarda até que o meio fique inativo. Caso ocorra uma colisão as estações terão de aguardar um tempo aleatório para poder tentar novamente enviar os dados. Este protocolo utiliza técnicas de prevenção de colisão diferente do protocolo CSMA/CD que utiliza detecção de colisão e utiliza um esquema de reconhecimento/retransmissão devido às altas taxas de erros de bits em canais sem fio (KUROSE; ROSS, 2006). Um exemplo de como funciona o protocolo CSMA/CA pode ser visto na figura 9, logo na sequencia.

Imagine um cenário com dois computadores cada um na distância máxima permitida para transmitir dados, digamos que o computador 1 precise transmitir dados para o computador 2, o computador 1 escuta o meio para verificar se esta disponível e caso esteja envia uma mensagem de controle para o computador 2, se não estiver disponível a transmissão é suspensa e um contador de tempo é ativado, iniciando uma contagem decrescente quando o meio ficar livre se o meio estiver ocupado o contador para ate o meio estiver livre novamente, assim que o contador de tempo chegar a zero poderá iniciar a transmissão. O computador 2 após receber a mensagem de controle do computador 1 envia outra mensagem de controle ao computador 1 dizendo que está apto a receber os dados, caso o computador 1 não receba esta mensagem do computador 2 ele terá que fazer todo o processo novamente, caso o computador 1 receba a mensagem ele poderá iniciar a transmissão dos dados para o computador 2 (COMER, 2007).

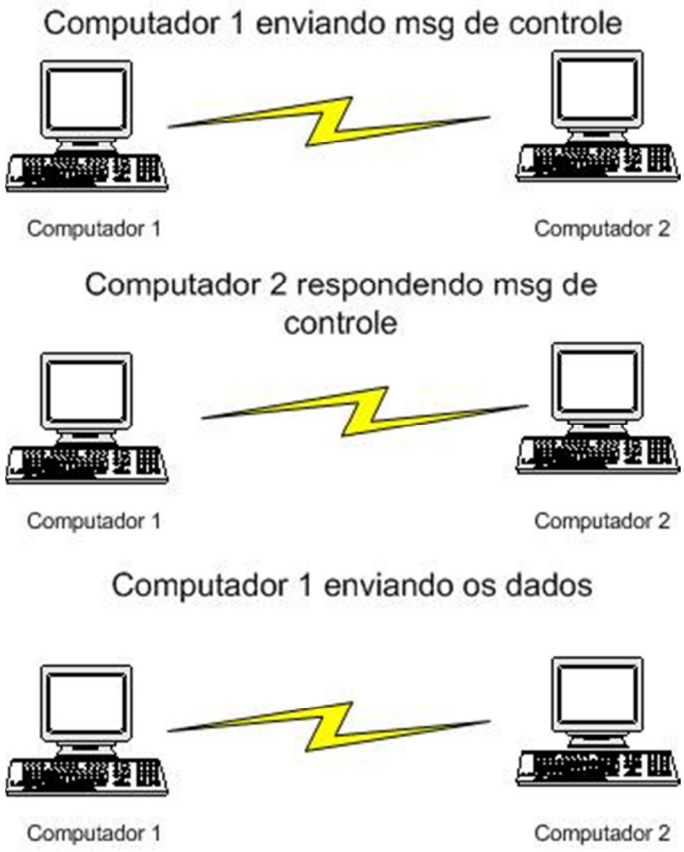

Figura 9 - Mensagem de controle CSMA/CA

Fonte: do autor

Muitos dispositivos não conseguem alcançar os sinais uns dos outros dentro de uma mesma célula, isto pode ocorrer devido a dois problemas: estação oculta ou estação exposta (TANEMBAUM, 2003).

Referente ao problema de estação oculta, ele ocorre devido a sua área de cobertura ser menor que a área da célula. O alcance dos sinais de rádio de determinado dispositivo é limitado a uma determinada área de cobertura, sendo assim os outros dispositivos que pertencem a mesma célula não tem como detectar se esta ocorrendo comunicação. A figura 10 relata este problema (TANEMBAUM, 2003).

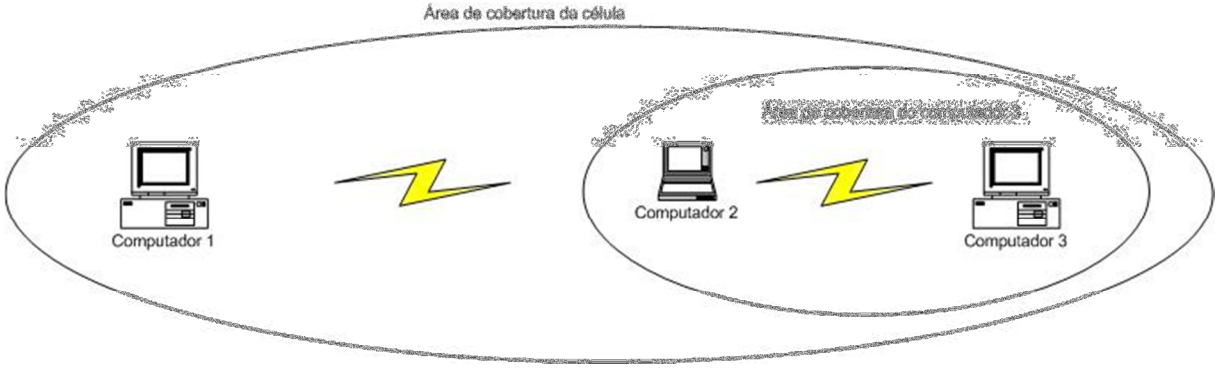

Figura 10 - Problema de estação oculta

Fonte: Tanembaum, 2003

A figura acima ilustra o computador 3 enviando dados ao computador 2 e o computador 1 esta fora da área de cobertura, com isso o computador 1 não consegue saber que o computador 2 está ocupado (TANEMBAUM, 2003).

O problema da estação exposta é que ela tenta fazer uma transmissão e não a faz, pois entende que esta recebendo a transmissão de outro dispositivo, mais na verdade ela não esta recebendo nenhuma transmissão. A figura 11 mostra este problema (TANEMBAUM, 2003).

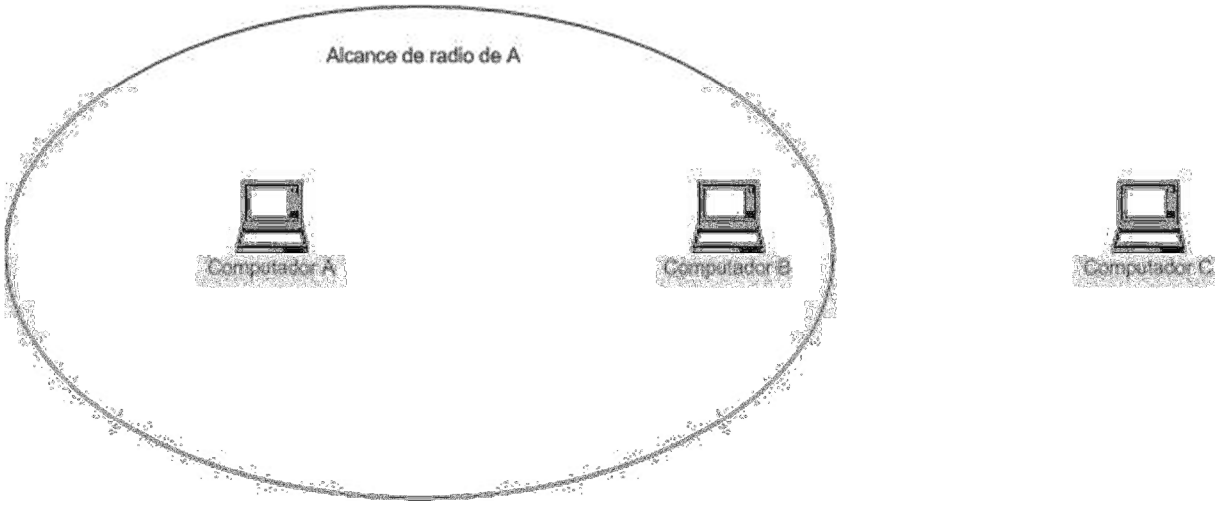

Figura 11 - Problema de estação exposta

Fonte: Tanembaum, 2003

Para enviar os problemas mencionados acima o padrão IEEE 802.11 utiliza um quadro de controle curto chamado *request to set* (RTS) e um quadro de controle chamado *clear to send* (CTS) que servem para reservar acesso ao meio. O remetente envia primeiramente um quadro RTS ao AP demonstrando o tempo total para transmitir, quando o AP recebe este quadro RTS responde fazendo uma transmissão de *broadcast* de um quadro CTS, este quadro tem duas finalidades, a primeira é dar permissão ao remetente para enviar os quadros e a segunda finalidade é dizer aos outros dispositivos para não enviar dados durante este tempo reservado (KUROSE; ROSS, 2006).

2.4 ESPECTRO ELETROMAGNÉTICO

Os elétrons quando se movem criam ondas eletromagnéticas podendo se propagar no espaço livre, inclusive no vácuo. Freqüência, é o número de vezes que a onda eletromagnética oscila por segundos, ela é medida em Hz. O comprimento de onda é a distância entre dois pontos, máxima ou mínima.

Na figura 12, logo abaixo, podemos ver as porções de rádio, microondas, infravermelho e luz visível, as quais podem ser utilizadas na transmissão de informações, isto quando feito a modulação da amplitude, a freqüência ou a fase das ondas e na parte baixa da imagem é mostrado as bandas ou faixas.

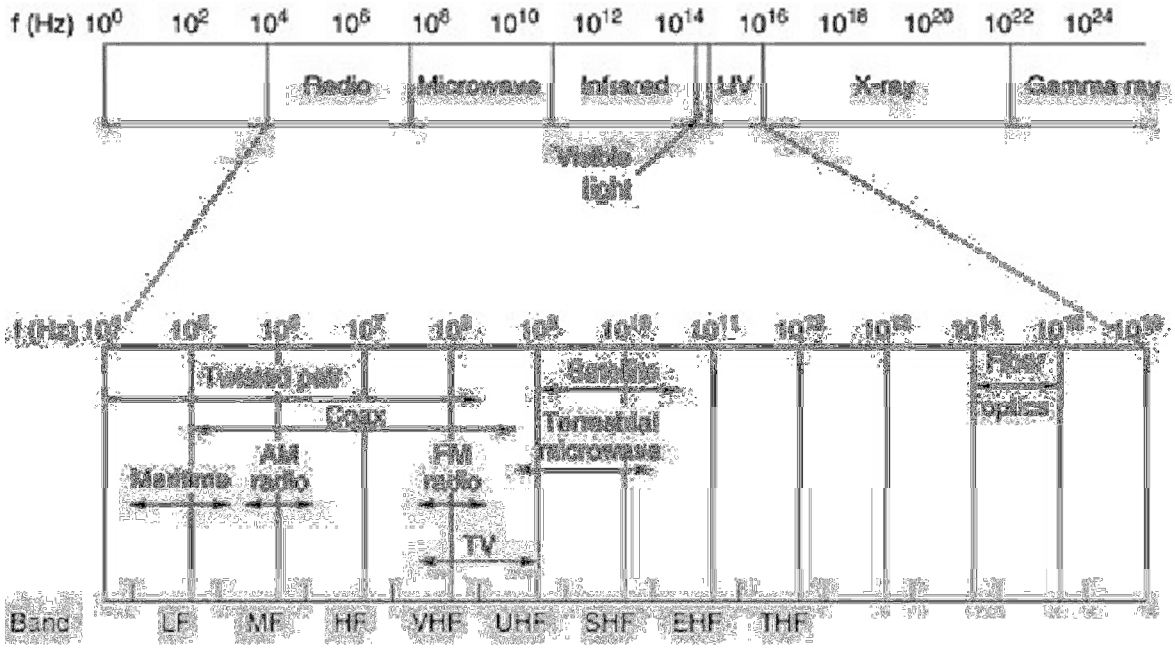

Figura 12 - Espectro eletromagnético e como é utilizado

Fonte: Tanembaum, 2003

As técnicas de espectro eletromagnético das redes sem fio normalmente são utilizadas em conjunto com técnicas de modulação e multiplexação, tendo a finalidade de melhorar o sinal antes de transmiti-lo ao meio, reduzindo interferências, reduzir o índice de erros e outras finalidades, resumindo melhorar a confiabilidade de transmissão. A seguir serão apresentadas as técnicas de espectro eletromagnético das redes sem fio (STALLINGS, 2005) (COMER,2007).

2.4.1 FHSS

No *Frequency Hopping Spread Spectrum* ou no português espectro de dispersão de saltos de frequência (FHSS), o espectro é obtido devido aos saltos frequentes da frequência de portadora para outra frequência, com isso, caso ocorra alguma interferência ou queda de desempenho isso afetará apenas uma fração da transmissão. O FHSS é a técnica de espectro mais simples e foi utilizada pelos dispositivos que haviam implementado as primeiras versões de redes sem fio e

também é utilizada pelo *Bluetooth*, outra aplicação é em enlaces entre edifícios, por ser insensível à interferência de radio.

A banda ISM é dividida em 79 canais com 1MHz ou 2MHz de largura, dando inicio na parte baixa da banda ISM de 2,4 GHz, sua frequência pode variar de 2,4GHz até 2,483GHz. Para produzir a sequencia de frequência de saltos um gerador de números pseudoaleatório é utilizado e seu período de gasto de cada frequência pode ser ajustado, mas deve ser menor que 400 ms.

Como desvantagem o FHSS apresenta baixa largura de banda e desperdício de banda disponível, devido a isso, geralmente os sistemas que utilizam essa técnica acabam sendo mais lentos que os que utilizam a técnica DSSS que será abordada a seguir. Uma de suas vantagens é a parte de segurança onde a mesma é muito robusta, pois receptores indesejados que não conhecem a sequencia de saltos ou tempo de parada não conseguem interferir nas transmissões (STALLINGS, 2005) (TANEMBAUM, 2003).

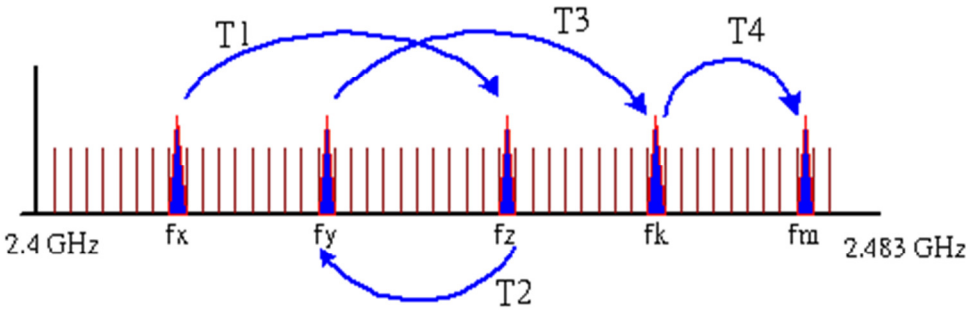

Figura 13 - Técnica de FHSS

Fonte: Stallings, 2005

2.4.2 DSSS

O *Direct Sequence Spread Spectrum* ou no português espectro de dispersão de sequencia direta (DSSS), originalmente foi implementada nas primeiras versões do padrão IEEE 802.11, ele é restrito a mesma largura que o FHSS, largura de 1MHz ou 2MHz e utiliza a banda ISM de 2,4 GHz.

O DHSS mapeia cada bit para uma string de bits, com isso ele consegue aumentar a velocidade de dados em um sinal, para isso é necessário uma largura de banda maior (STALLINGS, 2005) (TANEMBAUM, 2003).

A banda ISM é dividida em 11 subcanais, cada subcanal com 11MHz, e o sinal resultante é espelhado. Com isso a interferência mútua entre os canais pode ocorrer, dependendo da largura de espectro do sinal resultante (STALLINGS, 2005).

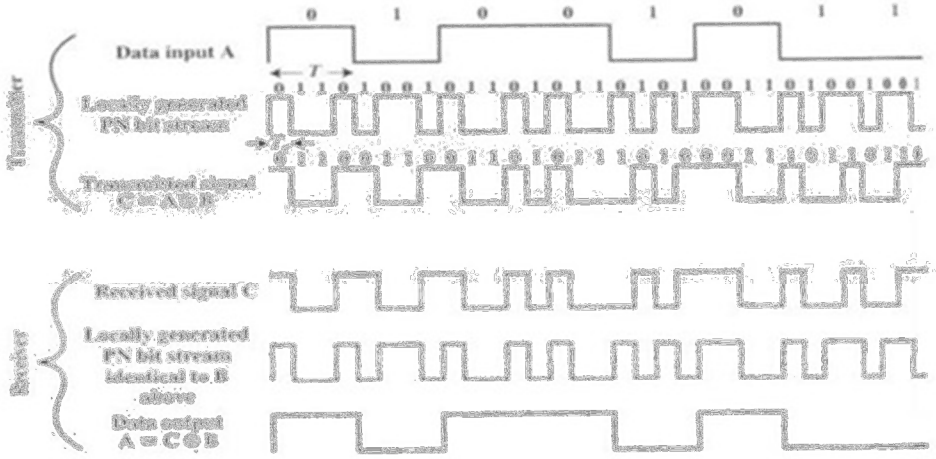

Figura 14 - Técnica DSSS

Fonte: Stallings, 2005

2.4.3 OFDM

A técnica chamada de *Orthogonal Frequency Division Multiplexing* ou em português multiplexação ortogonal por divisão de freqüência (OFDM), pode transmitir até 54Mbps na banda ISM mais larga de 5GHz. Sua freqüência é semelhante ao modo *Asymmetric Digital Subscriber Line* (ADSL). O OFDM utiliza 52 freqüências diferentes, sendo 48 para dados e 4 para sincronização. É considerada a técnica de espectro de dispersão mais diferente do CSMA e FHSS, devido suas transmissões estarem presentes em várias freqüências ao mesmo tempo. Essa divisão de sinal em varias bandas estreita proporciona vantagens fundamentais no uso de uma única banda larga, tendo melhor imunidade a interferência de banda estreita e possibilidade de usar bandas não contíguas, com isso podem dizer que esta técnica

tem boa eficiência de espectro em relação de bits/Hz e melhor imunidade de esmaecimento de vários caminhos (TANEMBAUM, 2003).

Para alcançar velocidades de até 18 Mbps é utilizado um sistema complexo de codificação, baseado na modulação por deslocamento de fase. Em 54 Mbps, 216 bits de dados são codificados em 288 bits de símbolos (TANEMBAUM, 2003).

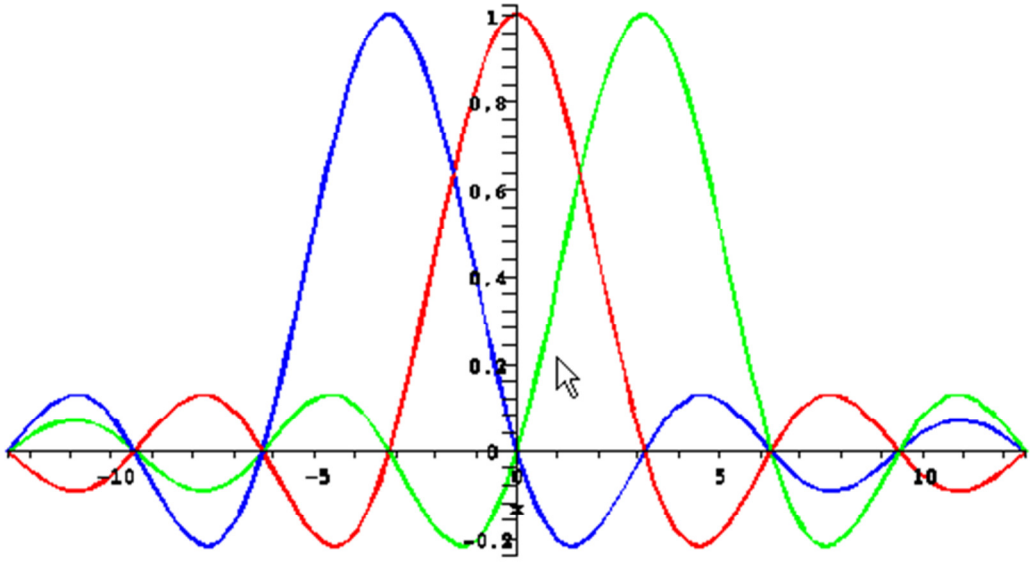

Figura 15 - Técnica OFDM

Fonte: http://www.gta.ufrj.br/grad/04_1/redesplc/3.html

3 DESENVOLVIMENTO

Este capítulo de número 3 abordará a parte de desenvolvimento. Será realizado a analise das ferramentas utilizadas, possíveis problemas ou dificuldades que foram encontradas durante a analise das ferramentas, como utilizar as ferramentas, o que eles podem fazer, quais são as vulnerabilidades que eles conseguem demonstrar em relação ao *Bluetooth* e as possíveis formas de se corrigir as vulnerabilidades.

3.1 FERRAMENTAS E EQUIPAMENTOS

Para o desenvolvimento da pesquisa serão utilizadas várias ferramentas com o intuito de identificar vulnerabilidades na rede *Bluetooth*. Todas as ferramentas são gratuitas e desenvolvidas em diversas plataformas e para diversos sistemas operacionais. A seguir serão detalhadas todas as ferramentas utilizadas.

Para a analise das ferramentas será necessário equipamentos que possuem a tecnologia *Bluetooth*, entre eles serão utilizados um notebook e um celular com suporte a tecnologia Java.

3.2 SUPER BLUETOOTH HACKER 1.8

Figura 16 - Logo da ferramenta super Bluetooth hacker

Fonte: http://www.baixebr.org/celular/celularaplicativos/Bluetooth-hack-18-aplicativo-para-celular/

O Bluetooth hacker é uma das ferramentas mais conhecidas e utilizadas devido a sua fácil utilização e por quem procura conseguir dados de outros celulares. Ela é baseada na tecnologia Java e a versão 1.8 já esta disponível em português e é uma versão gratuita.

A ferramenta promete, depois de conectado a outro equipamento via *Bluetooth,* as seguintes possibilidades de acesso ao outro dispositivo:

- Ler mensagens;
- Fazer ligações;
- Alterar configurações;
- Desligar o celular;
- Restaurar ao padrão de fabrica;
- Baixar musicas e fotos;
- Ver contatos;

Para os testes utilizamos um notebook com a tecnologia *Bluetooth* e um celular que suporte a tecnologia Java e utiliza o *Bluetooth.*

Primeiramente é necessário baixar o *software* que tem o tamanho de aproximadamente 111 kb e transferir o arquivo para o celular via *Bluetooth* ou cabo de dados, nesta pesquisa utilizamos via *Bluetooth* conforme demonstra a figura 15 a seguir.

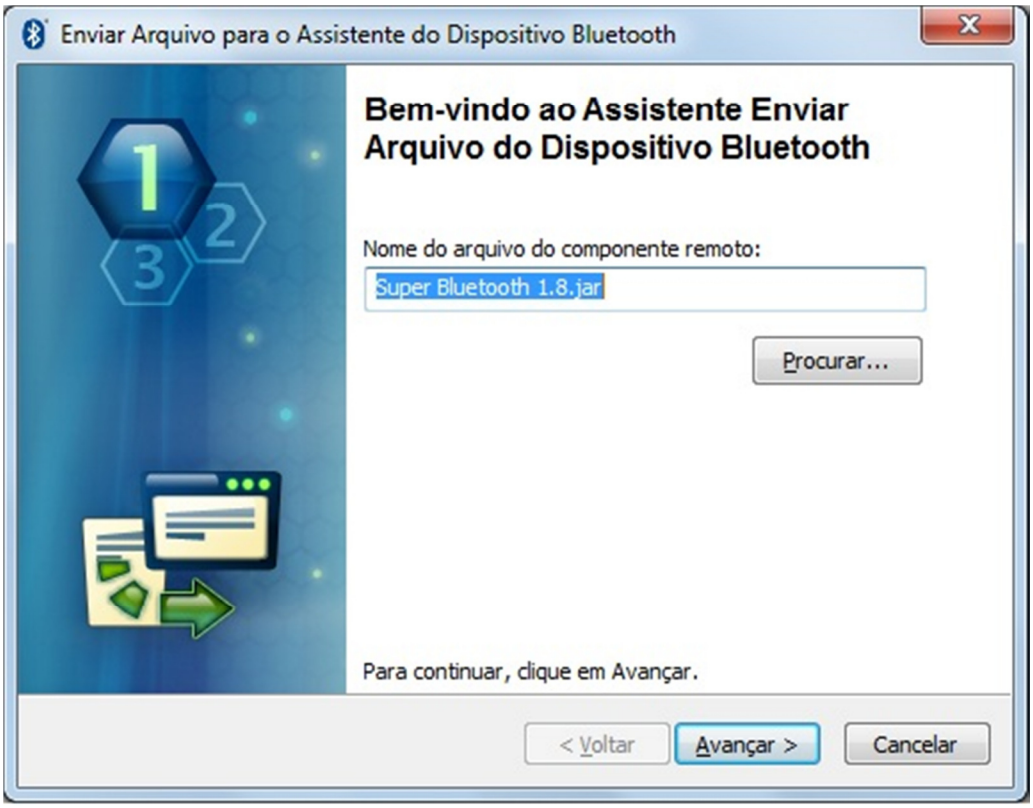

Figura 17 - Transferência de arquivo do notebook para celular

Fonte: do autor

Após a transferência do arquivo para o celular é necessário instalar a ferramenta no aparelho, no equipamento utilizado como testes, logo após baixar o arquivo a ferramenta foi instalada automaticamente, caso não seja instalada automaticamente basta ir até o local onde foi salvo o arquivo e executá-lo.

Com a ferramenta devidamente instalada no celular é necessário conferir se o *Bluetooth* está configurado e ativado no aparelho, cada aparelha a configuração e ativação são feitas de forma diferente, caso necessário deve ser verificado o manual do aparelho para maiores informações de como proceder. Conferido as devidas configurações agora é só utilizar a ferramenta, primeiramente é necessário fazer uma varredura para encontrar dispositivos com *Bluetooth* ativo, isto pode ser feito acessando a opção conectar do primeiro menu, logo em seguida acessar a opção inquérito de dispositivos, como demonstra a figura 17.

Figura 18 - Inquérito de devices: opção para localizar equipamentos

Fonte: do autor

Depois de encontrado o dispositivo é necessário se conectar a ele, infelizmente nos testes realizados é necessário fazer o pareamento dos aparelhos para conseguir acessar as funcionalidades do aparelho atacado, o pareamento entre os aparelhos nada mais é que se conectar ao aparelho, mas utilizando uma “chave” ou senha fornecida pelo aparelho que foi atacado, esta chave deve ser colocada no aparelho do atacante, feito isto se torna possível acessar varias funcionalidades do aparelho atacado. Nos testes realizados foi possível alterar configurações do aparelho tais como: idioma, volume de toque, tipo do toque e etc, os testes também proporcionaram a realização de uma ligação, infelizmente não é possível conversar pelo aparelho do atacante, outro ponto ruim é referente as alterações feitas no aparelho é possível vê-las sendo feita no exato momento, na verdade este *software* é como se estivesse controlando remotamente o outro aparelho.

3.3 BT BROWSER

O BT Browser é uma ferramenta baseada na tecnologia Java disponível para celulares que suportem esta tecnologia e a tecnologia *Bluetooth,* a versão instalada foi uma versão gratuita e em inglês, sem a possibilidade de escolher outra linguagem.

A ferramenta faz a descoberta de dispositivos que tenham a tecnologia *Bluetooth,* trazendo detalhes de cada dispositivo e seus serviços, não é uma ferramenta de ataque a outro dispositivo Bluetooth, mas serve para iniciar um ataque devido aos detalhes que esta ferramenta consegue extrair dos dispositivos capturados.

Para os testes foi utilizado um notebook para transferência do arquivo .jar e celulares com a tecnologia Java e *Bluetooth.*

Nos testes realizados a ferramenta cumpriu com o que promete, trazendo vários detalhes sobre os dispositivos encontrados. A ferramenta é simples de ser utilizada, como todas as ferramentas o primeiro passo é encontrar os dispositivos, este passo leva alguns segundos, após isto é só analisar os detalhes que a ferramenta trás, são diversos detalhes e serviços onde podem ajudar a realizar outro ataque com a utilização de outra ferramenta. Nos testes realizados não foi necessário o pareamento entre os aparelhos.

Figura 19 - Lista de serviços do Bt browser.

Fonte: do autor.

3.4 BLOOOVER2

Blooover é uma ferramenta muito conhecida na *Internet*, baseado na tecnologia Java, onde é possível ser instalada em qualquer aparelho que de suporte

a esta tecnologia, a versão instalada foi uma versão gratuita e em inglês, sem outras opções de linguagens.

A ferramenta possui vários ataques cada um para determinado tipo ou marca de celular, podendo escolher qual ataque utilizar e podendo configurar o ataque, como demonstram as figuras 19 e 20.

Figura 20 - Configurando ataque no blooover

Fonte: do autor

Figura 21 - Tela de configuração de ataques blooover

Fonte: Rufino, 2007

Para os testes foi utilizado um notebook para transferência do arquivo .jar e celulares com a tecnologia Java e *Bluetooth.* Depois de transferido o arquivo e instalado no aparelho é necessário verificar as configurações de ataque do aparelho utilizando a opção *settings* no menu principal, nesta opção você pode escolher qual ataque realizar entre outras configurações, recomenda-se deixar desmarcado a

opção de ataque *hellomoto*, nos testes realizados sempre quando iniciados por esta opção os aparelhos travavam sendo necessário desligar e ligar novamente, voltando a tela principal é hora de buscar os dispositivos utilizando a opção *find devices* com demonstra a figura 21.

Figura 22 - Menu principal blooover

Fonte: do autor

Nos testes realizados a ferramenta foi instalada em três celulares de marcas diferentes e utilizado todas as formas de ataques disponibilizadas na ferramenta, mas não foi possível ter êxito em nenhum dos ataques, todos falharam, a mensagem de falha apresentava que a ferramenta funciona melhor em outros modelos de aparelhos celulares.

3.5 EASYJACKV2

A ferramenta easyjackv2 é baseada em Java e possível de instalar em qualquer dispositivo que suporte à esta tecnologia. A versão baixada é uma versão *trial* sendo possível enviar apenas 10 mensagens, a versão é em inglês e não tem opção de outras linguagens.

A ferramenta promete o envio de mensagens SMS para qualquer celular que utilize a tecnologia *Bluetooth*.

Para os testes foram utilizado três aparelhos celulares e um notebook, o mesmo necessário para a passagem do arquivo .jar aos celulares.

Após passagem e instalação da ferramenta no celular é necessário fazer a busca dos equipamentos próximos, que estão com o *Bluetooth* ativo, selecionando a opção do menu *device search*, após encontrado os dispositivos selecionamos um deles e escolhemos a opção *send messege* onde é possível escrever uma mensagem de até 120 caracteres. Esta ferramenta não oferece nenhum tipo de ataque, mas pode ser usada para realizar uma engenharia social, podendo insinuar o usuário a digitar uma chave quando lhe for solicitado. Como exemplo é possível enviar uma mensagem dizendo sobre alguma promoção e quando foi solicitado uma senha em seu aparelho digitar 1234, assim é possível utilizar outro *software* que necessite fazer a paridade e esperar que algum usuário digite a chave descrita na mensagem e fazer a paridade com o aparelho atacado sendo possível obter todos os dados que aquela ferramenta proporciona.

Figura 23 - Menu principal

Fonte: http://www.4allmobile.eu/viewtopic.php?f=39&t=4642

3.6 BT FILE MANAGE

O Bt File Manage é uma ferramenta desenvolvida em Java que utiliza a conexão *Bluetooth* para obter quaisquer arquivos de outros celulares, também é possível deletar, mover, renomear e enviar arquivos utilizando esta ferramenta. A versão testada foi uma versão gratuita e não tem versão em português, pode ser baixada de qualquer sitio da *Internet*.

Para os testes realizados, foram utilizados três aparelhos celulares de marcas distintas e um notebook para baixar o arquivo e fazer a transferência para os celulares.

Após a transferência e instalação da ferramenta no celular, é necessário fazer a busca dos dispositivos mais próximos utilizando a opção do menu BT *devices* e depois a opção *search devices*, com os dispositivos encontrados agora é necessário fazer o pareamento entre os dispositivos, será solicitado ao dispositivo que esta sendo atacado para que digite uma chave e a mesma deve ser repetida no dispositivo do atacante, feito isto foi possível fazer tudo o que a ferramenta promete renomear arquivos, copiar, deletar entre outras possibilidades sem nenhuma dificuldade, ferramenta muito fácil de utilizar.

Figura 24 - Menu da ferramenta BT File Manage

Fonte: http://www.razerweb.wz.cz/index.php?l=en&p=bt_file_manager

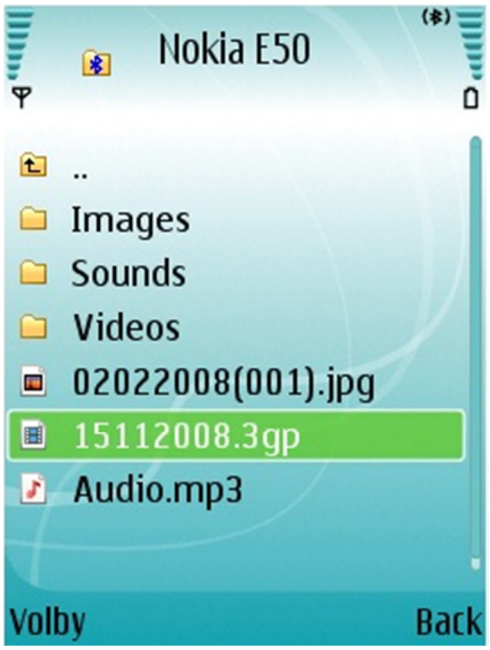

Figura 25 - Arquivos de um celular atacado

Fonte: http://www.razerweb.wz.cz/index.php?l=en&p=bt_file_manager

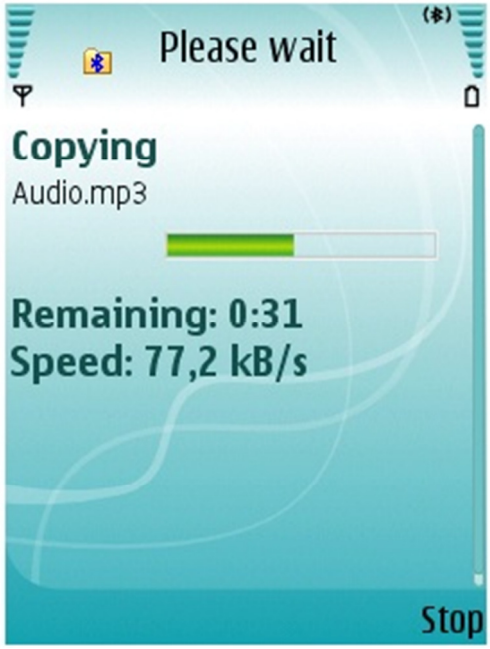

Figura 26 - Copiando arquivo de dispositivo atacado

Fonte: http://www.razerweb.wz.cz/index.php?l=en&p=bt_file_manager

4 CONCLUSÃO

Com o passar dos anos a tecnologia sem fio tem evoluído cada vez mais principalmente no que diz respeito à segurança destas redes. As redes *Bluetooth* não ficam atrás neste aspecto, ela vem se popularizando e estão cada vez mais presentes em nosso cotidiano, podendo ser utilizada de diversas formas e em diversos equipamentos. As empresas fabricantes de equipamentos que utilizam esta tecnologia investem muito na parte de segurança, para dificultar cada vez mais que informações possam ser obtidas devido a ataque de pessoas má intencionadas.

Foi realizada uma pesquisa com o intuito de descobrir ferramentas que exploravam vulnerabilidades das redes sem fio *Bluetooth*, foram encontradas diversas ferramentas e feito a analise e estudo das ferramentas encontradas. Grande parte das ferramentas analisadas promete invadir com facilidade dispositivos que utilizam a tecnologia, nos testes realizados foi possível analisar que a grande parte das ferramentas necessita que seja feito o processo de paridade entre os dispositivos o que acaba dificultando o ataque, mas quando a paridade já esta feita é possível realizar vários ataques e controlar o outro dispositivo de várias maneiras e pegar praticamente todos os dados pertencentes a este dispositivo atacado. Uma das formas de se realizar a paridade é utilizando alguma ferramenta e fazendo uma engenharia social, uma das ferramentas apresentadas nesta pesquisa pode ser utilizada para este tipo de ataque, onde é possível enviar uma mensagem sem a necessidade de parear um dispositivo, induzindo ao usuário que quando for solicitada uma chave ou senha em seu celular digite um determinado número, com isso após enviar a mensagem é só utilizar uma das ferramentas de ataque e torcer para que o usuário utilize a senha mencionada na mensagem, sendo possível fazer a paridade. Outro ponto analisado é que alguns *softwares* funcionam melhor em determinados tipos ou marcas de dispositivos e possuem ataques pré-determinado a uma determinada marca.

Para evitar que ataques sejam realizados com êxito nos equipamentos que utilizam a tecnologia *Bluetooth* algumas medidas devem ser levadas em consideração, como: apenas realizar o pareamento a dispositivos que sejam conhecidos, deixar o *Bluetooth* desativado se não estiver utilizando, ativar o *Bluetooth* apenas quando necessário e após a utilização desativá-lo, quando não for

possível desativar o *Bluetooth* e seja necessário utiliza-lo, recomenda-se deixar desmarcado a opção de visualizado por todos, estar com o *software* e firmwares sempre atualizados e por ultimo, verificar autenticidade de mensagens enviadas solicitando que seja colocado algum tipo de senha quando seu celular solicitar.

Com isto é possível afirmar que a tecnologia *Bluetooth* tem certa segurança principalmente pelas empresas fabricantes investirem pesado nesta área e utilizando medidas simples podem ajudar a evitar que seus dados pessoais sejam roubados por pessoas má intencionadas.

REFERÊNCIAS

4 ALL MOBILE. Disponível em <http://www.4allmobile.eu/viewtopic.php?f=39&t=4642> acessado em: 19/11/2011.

BAIXEBR TRUQUES E DICAS. Disponível em < http://www.baixebr.org/celular/celularaplicativos/Bluetooth-hack-18-aplicativo-para-celular/> acessado em: 07 nov. 2011

CLAYTON, ANDERSON. Disponível em: <http://www.nokiatividade.com/aplicativo-quickbt-Bluetooth-onoff-com-um-toque> acessado em: 27 out. 2011

COMER, DOUGLAS E. **redes de computadores e internet.** 4 ed. Porto Alegre: Bookman, 2007.

ERASALA, NAVEEN. YEN, DAVID**. Bluetooth technology: a strategic analysis of its role in global 3G wireless communication era.** Oxford, 2002. Disponível em: <http://www.periodicos.capes.gov.br.ez48.periodicos.capes.gov.br/index.php?option=com_pmetabusca&mn=70&smn=78&metalib=&func=meta-1&type=m&mn=88&smn=89> acesso em: 09 out. 2011.

GIL, A. C. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2007.

GTA UFRJ. Disponível em <http://www.gta.ufrj.br/grad/04_1/redesplc/3.html> acessado em: 25 nov. 2011

KUROSE, JAMES F. ROSS, KEITH W. **Redes de computadores e a internet.** 3. ed. São Paulo: Pearson Addison Wesley, 2006.

MORIMOTO, CARLOS EDUARDO. **Redes guia pratico.** Porto Alegre: Sul Editores, 2008.

RAPPAPORT, T. S. **Comunicações sem fio princípios e práticas.** 2. ed. São Paulo: Pearson, 2009.

RAZER'S WEB. Disponível em <http://www.razerweb.wz.cz/index.php?l=en&p=bt_file_manager> acessado em: 20/11/2011

RUFINO, N. M. DE O. **Segurança em redes sem fio.** 2. ed. São Paulo: Novatec, 2007.

RUFINO, N. M. DE O. **Segurança em redes sem fio.** 3. ed. São Paulo: Novatec, 2011.

STALLINGS, WILLIAN. **Redes e sistemas de comunicação de dados.** 5. ed. Rio de Janeiro: Elsevier, 2005.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 2003.