UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

JUNIOR TRAJANO RODRIGUES

SEGURANÇA NA TRANSMISSÃO DE DADOS POR BLUETOOTH EM AMBIENTES MÓVEIS

CRICIÚMA, DEZEMBRO DE 2007

JUNIOR TRAJANO RODRIGUES

SEGURANÇA NA TRANSMISSÃO DE DADOS POR BLUETOOTH EM AMBIENTES MÓVEIS

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA, DEZEMBRO DE 2007

JUNIOR TRAJANO RODRIGUES

SEGURANÇA NA TRANSMISSÃO DE DADOS POR BLUETOOTH EM AMBIENTES MÓVEIS

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

_____

Profa. M.Sc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

_____

Prof. M.Sc. Paulo João Martins (UNESC)
Orientador

_____

Prof. Esp. Vilson Gruber (SATC)

_____

Prof. Esp. Arildo Sônego (UNESC)

Dedico esta conquista a meus pais, que me incentivaram e sempre me mostraram que o estudo e a busca do conhecimento constante eram o que me levaria a vitória.

AGRADECIMENTOS

Primeiramente agradeço a Deus, pois sem Ele e sem a fé que depositei em suas palavras nada disso seria possível.

Agradeço esta conquista a meus pais Valmir Augusto Rodrigues e Marta Regina Trajano Rodrigues, que são responsáveis pela minha existência e por sempre ter me incentivado em meus estudos. Sem eles nada disso seria possível. Também agradeço esta vitória a meus irmãos Diego Trajano Rodrigues e Vitor Trajano Rodrigues que sempre me deram apoio, e à minha namorada Mariana pela compreensão e paciência.

Sou muito grato, também, aos meus professores que ao longo da minha vida me ensinaram a ler, escrever, descobrir o gosto pelo esporte; e àqueles professores que, hoje, me ensinaram o que será a minha profissão, o meu futuro. Não posso esquecer também de agradecer esta conquista a todos meus amigos que no decorrer desta vida acadêmica sempre me ajudaram nos momentos difíceis, dando incentivo e conselhos para que não olhasse para trás, fazendo-me acreditar que este momento iria chegar.

Ao professor Daniel Pezzi da Cunha que me auxiliou no início das pesquisas do trabalho científico.

Agradeço também ao meu orientador Paulo João Martins por ter me direcionado para que este trabalho pudesse ser bem sucedido.

“Eu aprendi que para se crescer como pessoa é preciso me cercar de gente mais inteligente do que eu.”

William Shakespeare

RESUMO

O crescimento da tecnologia em ambientes móveis está cada vez mais presente na vida das pessoas e muitas destas tecnologias utilizam a comunicação por *bluetooth*. As pessoas que utilizam destas tecnologias visam a mobilidade, agilidade e segurança em seu uso. Este trabalho abordará a segurança como ponto principal para a utilização da tecnologia *bluetooth*, apresentando métodos e técnicas de segurança para este tipo de ambiente móvel, utilizando o *bluetooth* como objeto de estudo para comunicação. A parte prática deste trabalho consiste em um protótipo de software de prontuário eletrônico trabalhando como cliente servidor, onde o cliente será executado em um celular com tecnologia *bluetooth* que terá o objetivo de recolher dados dos pacientes em seus leitos hospitalares e em seguida enviá-los para um servidor através da comunicação por *bluetooth* que irá armazenar esses dados em um banco de dados.

Palavras-chave: Segurança, Criptografia, Autenticação, *Bluetooth*.

ABSTRACT

The growth of technology on mobile environments is each time more present at people's lives and many of these technologies are based on Bluetooth wireless communications. People who use such technologies claim for mobility, agility and security. This assignment will deal with security as the main topic for the utilization of Bluetooth technology, presenting methods and techniques of security for this type of mobile environment. The practice part of this assignment consists of a prototype of electronic medical record software operating as a client-server, in which the client will be executed on a mobile phone integrated with Bluetooth. The objective is to retain patient's data in order to send it to a server, trough Bluetooth communication technology, which will store this information in a data base.

Key-words: Security, Cryptography, Authentication, Bluetooth

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

AP	*Access Point*
BER	*Bit Error Rate*
CAs	Autoridade de Certificação
DSA	*Digital Signature Algorithm*
DSS	*Digital Signature Standart*
ER	Entidade Relacional
ESN	*Eletronic Serial Number*
HLR	*Home Location Register*
IR	*InfraRed*
MAC	*Medium Access Control*
MIN	*Mobil Identification Number*
MSC	Central de Comutação Celular
RSA	Rivest, Shamir e Adelman
UNESC	Universidade do Extremo Sul Catarinense
VLR	*Visitor Location Register*
Wi-Fi	*Wireless Fidelity*

SUMÁRIO

1 INTRODUÇÃO

Atualmente, com o constante crescimento da tecnologia em ambientes móveis, com aparelhos cada vez mais modernos que fazem uso da tecnologia *bluetooth*, surgem também os ataques e intervenções, fazendo com que dados importantes sejam capturados por outros dispositivos que estejam ao alcance do sinal *bluetooth*.

Segundo Kobayashi (2004) o *bluetooth* foi projetado para diminuir a complexidade na conexão entre dispositivos móveis. Por outro lado leva uma desvantagem no quesito segurança, por causa das características da comunicação das redes sem fio, ou seja, o ar.

Segundo Menegatti, citado por Ayres (2007), essas características, entre outras, podem explicar o fato do *bluetooth* ser responsável por 70% dos ataques em ambientes móveis.

Para fazer com que a comunicação com a tecnologia *bluetooth* torne-se segura, faz-se necessário o uso de técnicas de seguranças existente tais como criptografia, autenticação para garantir a integridade e confidencialidade dos dados. Este trabalho tem como intuito aplicar técnicas de criptografia e autenticação em um ambiente móvel, simulando uma comunicação entre cliente-servidor, onde os mesmos serão submetidos a uma interceptação por meio de ferramentas existentes de captura de dados específicos para o ambiente de comunicação *bluetooth*.

1.1 OBJETIVO GERAL

O trabalho tem como objetivo explorar as vulnerabilidades da tecnologia *bluetooth* bem como técnicas de criptografia e autenticação para fazer uma transmissão de dados segura entre os ambientes móveis, usando a tecnologia *bluetooth*.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

a) compreender e aplicar as técnicas de criptografia na transmissão de dados por *bluetooth* em ambientes móveis;

c) pesquisar e aplicar a comunicação por *bluetooth*, assim como sua segurança na transmissão;

e) pesquisar as vulnerabilidades existentes na tecnologia *bluetooth*;

d) testar soluções de segurança por meio da implementação prática no ambiente ilustrado no Apêndice A;

e) analisar os resultados dos testes práticos no emprego de soluções para segurança.

1.3 JUSTIFICATIVA

Segundo Rufino (2005) a tecnologia de comunicação que o *bluetooth* possui permite que dados importantes transmitidos possam ser capturados por outros dispositivos que estejam na área de cobertura do meio sem fio. A tecnologia *bluetooth* dispõe de níveis de segurança, e ainda assim é responsável por 70% dos ataques em ambientes móveis (AYRES, 2007).

Muitas vulnerabilidades ainda são encontradas nesta tecnologia. Muitas delas ocorrem, geralmente, por falhas no padrão, como o caso da força do gerador de números randômico e o uso de um pequeno valor para o PIN. Outro fato que contribui para esta vulnerabilidade são as falhas de implementação, bem como a flexibilidade do padrão que oferece autonomia aos fabricantes para definição de diversos procedimentos relacionados à criptografia e autenticação (ROCHA; ELIAS, 2005).

O *bluetooth* foi criado, inicialmente, para substituir cabos e para reduzir a complexidade de conectar dois ou mais dispositivos. Com seu crescimento, essa tecnologia vem sendo utilizada num âmbito maior, por causa de sua flexibilidade e baixo custo comparado com outras tecnologias. Infelizmente, a segurança nesta tecnologia não está acompanhando este crescimento, estabelecendo uma diferença muito grande entre flexibilidade e segurança das conexões (KOBAYASHI, 2004).

Diante disso, o presente trabalho propõe estudar e aplicar técnicas de segurança e intervenção de dados no ambiente ilustrado no apêndice A, e aplicar estas técnicas na transmissão de dados por *bluetooth*. O trabalho prático consiste na aplicação cliente servidor, simulando um protótipo de prontuário eletrônico onde os dados dos pacientes serão coletados em seus leitos hospitalares e, em seguida, enviados para o servidor por meio da comunicação por *bluetooth*. Logo após o recebimento dessas informações, o servidor irá armazená-las em um banco de dados.

1.4 ESTRUTURA DO TRABALHO

Este trabalho é composto por oito capítulos voltados para a segurança em ambientes móveis, distribuídos em:

1) **introdução:** apresenta ao leitor o objetivo do trabalho, fazendo um panorama do que realmente o trabalho abordará;
2) **computação móvel:** aborda o surgimento e a importância que a computação móvel trouxe para as pessoas, seu crescimento, seu futuro e as áreas nas quais esta tecnologia está sendo aplicada;
3) **redes sem fio:** apresenta as características das redes sem fio, bem como suas facilidades, vantagens e desvantagens na utilização; discorre, também, sobre os pontos de aplicações e os tipos de tecnologias sem fio existentes atualmente;
4) **bluetooth:** capítulo que apresenta a parte principal do trabalho; descreve a origem dessa tecnologia, como ocorre a sua comunicação, o funcionamento da transmissão de dados, suas características, vantagens e desvantagens e, por fim, a segurança que a tecnologia *bluetooth* possui;
5) **integridade e confidencialidade:** menciona o objetivo e a importância da segurança das informações e prevê formas de manter a integridade e confidencialidade dos dados.
6) **criptografia:** descreve as formas de obter segurança na tecnologia *bluetooth*. No decorrer deste capítulo serão abordadas várias formas e técnicas de segurança, tais como: criptografias e seus principais tipos, autenticação, assinatura digital, certificado digital e autenticação biométrica e seus principais algoritmos.

7) **vulnerabilidade em redes sem fio:** discute as vulnerabilidades nas redes sem fio onde o *bluetooth* se inclui. Apresenta, também, os métodos e técnicas de ataque a essas redes, bem como as ferramentas que hoje existem para captura de sinal, intervenção, modificação ou fabricação de acordo com o tipo de ataque aplicado neste tipo de ambiente.
8) **trabalho desenvolvido:** o oitavo e último capítulo discorre sobre a aplicação do trabalho. A teoria é transformada em prática por meio da aplicação das técnicas e ferramentas estudadas ao longo do trabalho. Esta parte do trabalho apresenta, também, a metodologia nele utilizada, bem como os resultados obtidos.

2 COMPUTAÇÃO MÓVEL

Segundo Pena e Silva (2001), o país pioneiro na tecnologia da comunicação foi o Japão, em 1979, na década de 70, onde o objetivo era voltado para comunicação de voz, caracterizando-se por ser sem fio móvel e pessoal.

O crescimento extraordinário da comunicação sem fio trouxe a praticidade de acessar informações de qualquer parte a qualquer momento. Segundo Mateus e Loureiro (2004), o objetivo geral da comunicação móvel é introduzir as facilidades e praticidades de um computador estático e distribuído para um ambiente móvel, fazendo a junção da comunicação sem fio, permitindo a mobilidade.

Segundo Mateus e Loureiro (2004), a mobilidade traz facilidades e com elas, também, alguns novos problemas de segurança e autenticação na comunicação sem fio. A facilidade de fazer interceptação de mensagens pode causar sérios problemas de segurança. Nessa ocasião, deve-se fazer uso de técnicas de criptografia ou um outro tipo de segurança disponível.

Com o surgimento de novas tecnologias e métodos de comunicação, também surgem problemas relacionados à comunicação; sistemas operacionais, banco de dados e principalmente, segurança.

A comunicação móvel apresenta características diferentes em relação a um sistema fixo como (MATEUS; LOUREIRO, 2004):

a) menor largura de banda;

b) freqüentes desconexões (voluntária e involuntária);

c) taxa de erro do canal variável e dependente da localização;

A computação móvel está sendo utilizada em diversas áreas do conhecimento humano: pode ser usada no auxílio em tomadas de decisões, gerenciamento de dados, entre outros. Uma das suas principais vantagens é a capacidade de processamento em qualquer hora em qualquer lugar, não se limitando a dispositivos fixos, e sim, nos bolsos e mãos dos usuários (ROSSO, 2005).

Os dispositivos móveis estão cada vez mais atraentes e suas tecnologias cada vez mais avançadas, permitindo que seus usuários tenham muita facilidade em fazer compras, acessar o banco, entre outras atividades, por de telefones celulares, pocket PC's, smart phones, palm pilots, PDA's etc. Muitos destes aparelhos suportam diversas linguagens de programação. Alguns suportam WAP, WML e HTML, outros suportam ambos e outros, ainda, suportam a tecnologia *bluetooth* que é uma tecnologia de curto alcance e de baixo custo, se comparada a outras tecnologias de comunicação.

A computação móvel está presente em várias áreas e profissões: na Medicina, desde o prontuário eletrônico para coleta de informações dos pacientes até o monitoramento de pacientes internados nos hospitais (este último é utilizado em um dos maiores hospitais do Brasil, o Instituto do Coração do Hospital das Clínicas, em São Paulo); na Engenharia Civil, nas visualizações de plantas e programas específicos da área. Em todas as áreas existem alguns pontos comuns. Um deles é a agilidade no processo e a facilidade de manipulação dos dados na palma de sua mão. Existem, porém, alguns pontos negativos: o baixo processamento e a capacidade de armazenamento de dados comparado ao ambiente fixo (DIAS; SADOK, 2001).

2.1 FUTURO DA COMPUTAÇÃO MÓVEL

O crescimento da computação móvel está cada vez mais avançado. O que se espera do seu futuro é que sejam inseridas todas as facilidades de um computador estático em um dispositivo móvel, com uma tendência de aparelhos cada vez menores e portáteis, com um alto processamento e armazenamento de dados.

A empresa IBM, juntamente com a empresa Taiwan Mediatek, estão juntas no desenvolvimento de *chipsets*[1] muito rápidos voltados para os dispositivos que utilizam a comunicação sem fio.

> Esse esforço colaborativo permitirá aos consumidores transferirem sem fio grandes arquivos de dados multimídia em seus escritórios e casas em questão de segundos, disse T.C. Chen, vice-presidente de ciência e tecnologia da IBM Research, que tem se engajado em tecnologia de ondas milimétricas (mmWave) há quatro anos (TAIPÉ, 2007).

Este projeto irá integrar os novos *chips* de comunicação da IBM e o sistema de encapsulamento da empresa Mediatek que possui grande experiência em *chips* de processamento de vídeo (TAIPÉ, 2007).

[1] Conjunto de circuitos de apoio utilizados na placa mãe de um computador.

3 REDES SEM FIO

As redes sem fio ganharam o mercado e estão cada vez mais se popularizando em aplicações domésticas e de trabalho. Essa tecnologia permite que o usuário goze da liberdade de se movimentar e se conectar a qualquer hora e a qualquer lugar sem ter o incômodo dos cabos (MATEUS; LOUREIRO, 2004).

As redes sem fio têm como características o seu meio físico de comunicação, ou seja, o ar. Normalmente, são utilizados quando:

a) não se faz possível a instalação de redes fixas (por cabos);

b) quando se quer obter uma rede de caráter temporário;

c) por questões de estética ou layout, normalmente vistas em grandes hotéis e restaurantes;

A Figura 1 mostra a facilidade e a comodidade de uma instalação de uma rede sem fio, sem que haja a necessidade do uso de cabos, nem o trabalho de passá-los por telhados, pisos ou paredes:

1 – dispositivos de redes sem fio;

2 – ponto de acesso sem fio;

3 – computadores em uma rede com fio (par trançado);

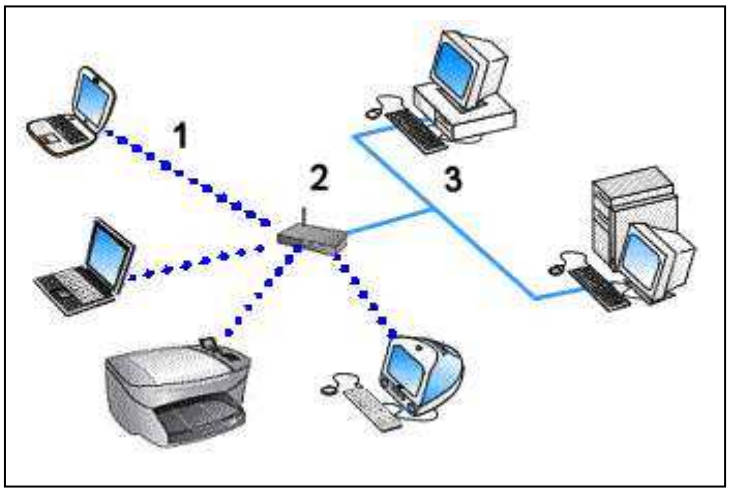


Figura 1. Ilustração de uma rede sem fio
Fonte: HP (2006)

As redes sem fio podem ser utilizadas para o uso de caráter restrito em prédios empresariais, uso doméstico ou em grandes hotéis. Também podem ser utilizadas em área pública, onde são chamados de *Hotspots*[2].

Assim como as redes sem fio têm trazido uma grande vantagem com a mobilidade, elas também trazem alguns incômodos. Os capítulos 3.1 e 3.2 a seguir, discorrerão sobre algumas vantagens e desvantagens no uso de rede sem fio.

3.1 VANTAGENS NO USO DE REDES SEM FIO

Segundo Santana et al (2004), o uso das redes sem fio tem algumas vantagens motivadoras:

a) **facilidade de instalação:** as redes sem fio podem ser instaladas de forma rápida e fácil. No caso de redes estruturadas, ou seja, aquelas em que a estação móvel está em contato direto com um ponto de acesso, normalmente ligada a uma rede fixa, onde a transmissão é superior a sem fio, basta instalar um ponto de acesso *Access Point (AP*[3]*)*, e que o mesmo esteja ligado a uma rede local ou à internet;

b) **mobilidade:** as redes sem fios têm a vantagem de permitir uma mobilidade e uma praticidade de acessar informações de qualquer parte a qualquer momento, dispensando o uso de cabos, permitindo que o dispositivo possa mudar de posição, facilitando o trabalho das pessoas que o utilizam;

c) **redução de custo:** por ter como vantagem a facilidade de deslocamento, há redução de custo, pois ela pode chegar a lugares mais facilmente do

[2] Nome dado ao local onde se encontra disponível a tecnologia Wi-Fi.
[3] Funciona como uma ponte de comunicação entre a rede sem fio e a rede convencional.

que chegaria uma rede cabeada, além do custo de manutenção e instalação que é mais baixo, comparado com uma rede fixa que requer, para sua instalação, obras civis, por exemplo;

Frente todas essas vantagens, a rede sem fio também possui um outro lado não muito agradável. No próximo capítulo são relacionadas algumas das desvantagens dessa tecnologia.

3.2 DESVANTAGENS NO USO DE REDES SEM FIO

Segundo Lima (2005), uma das grandes desvantagens do uso das redes sem fio é a questão da segurança. Além dessa, algumas outras podem ser citadas:

a) **disponibilidade de menor banda de transmissão:** as redes sem fio, comumente, possuem uma menor largura de banda comparada às redes cabeadas que atingem aproximadamente dezenas de *Gbps* em sua taxa de transmissão. As redes sem fio têm uma taxa de dezenas de *Mbps*;

b) **taxas de erro:** as redes sem fios apresentam uma taxa de erro de bit, Bit Error Rate (BER), superior às redes convencionais. Enquanto as redes de fibra óptica possuem uma taxa de erro que pode variar de 10^{-8} à 10^{-9}. Nas redes sem fio essa taxa chega variar de 10^{-4} à 10^{-6} ;

c) **endereçamento:** numa rede fixa, o endereçamento é dado pelo vínculo da estação com o endereço da rede a qual está instalada. Nas redes sem fios isso não é possível dado à mobilidade dos dispositivos que tendem a possuir inconstância na localização geográfica.

d) **interferências:** o meio é de domínio público, e por isso está sujeito a interferências;

e) **consumo de energia:** alto consumo de energia dos equipamentos portáteis;

f) **riscos à saúde:** a radiação eletromagnética pode trazer riscos à saúde;

g) **soluções proprietárias:** por motivos de lentidão no processo de padronização, muitos fabricantes desenvolvem soluções próprias com alguns itens adicionais, fazendo com que dispositivos com diferentes fabricantes não funcionem. Por isso, deve-se seguir regulamentações e padronizações únicas.

3.3 AMBIENTES SEM FIO

Mobilidade, conforto e comunicação são facilidades que fazem parte e são buscadas pela maioria das pessoas. A tecnologia e seus avanços permitiram que fosse possível eliminar cabos e permitir a troca de informações entre pessoas em toda e qualquer parte do mundo, com a tecnologia *wireless*[4].

Segundo Sacks (2003), em ambientes *wireless* existem vários tipos de tecnologias de transmissão. Nos ambientes que exigem uma camada mais baixa, normalmente são usadas as transmissões por freqüência de rádio e transmissão por *Infra-Red (IR)*, enquanto nas camadas mais altas usam-se os padrões *bluetooth* e *Wi-fi*.

[4] É uma tecnologia responsável por unir computadores entre si devido às ondas de rádio, sem a necessidade de utilizar cabos de conexão entre eles.

3.3.1 InfraRed

As redes *wireless* baseadas em *InfraRed (IR)* são usadas, normalmente, em situações onde a distância é curta, pois utilizam onda de luz e necessitam que os aparelhos estejam visíveis. Segundo Maia (2003), os sinais de IR não conseguem penetrar em objetos opacos e podem ser facilmente obstruídos. Por isso, sua utilização exige ser visada diretamente entre dois pontos a serem conectados, ou utilização de transmissão por difusão (reflexão).

3.3.2 Wireless Fidelity

Também conhecido como *Wireless Local Área Network (WLAN)* é uma tecnologia que está implementada sobre o padrão IEE 80211, que opera em uma freqüência que varia entre 2,4 *GHz* e 5 *GHz* (LIMA, 2005).

Essa tecnologia utiliza alta freqüência de ondas de rádio para a comunicação entre ambientes móveis e permite o acesso a redes públicas e privadas, permitindo a seus usuários mobilidade e comodidade (TUDE, 2006).

Segundo Toso et al (2004), a topologia *Wireless Fidelity (wi-fi)* pode ser constituída de várias formas, dependendo do tipo da rede em que ela se situa:

a) **rede local:** utiliza-se *Access Points*, que são considerados *switches*[5] de uma rede sem fio, e adaptadores *wi-fi*, simples;
b) **rede metropolitana:** utiliza-se antenas e adaptadores *wi-fi*, com *pigtails*[6]*;*

[5] Pode ser traduzido como comutador e é utilizado nas redes de computadores para reencaminhar quadros de dados entre seus diversos nós.

c) **rede ampla:** utiliza-se antenas, amplificadores, adaptadores *wi-fi* com *pigtails*.

Segundo Lima (2005), o padrão IEEE 802.11 corresponde à camada física e à sub-camada do *Media Access Control (*MAC). A Figura 2 mostra o modelo de camada de uma rede, utilizando o padrão 802.11.

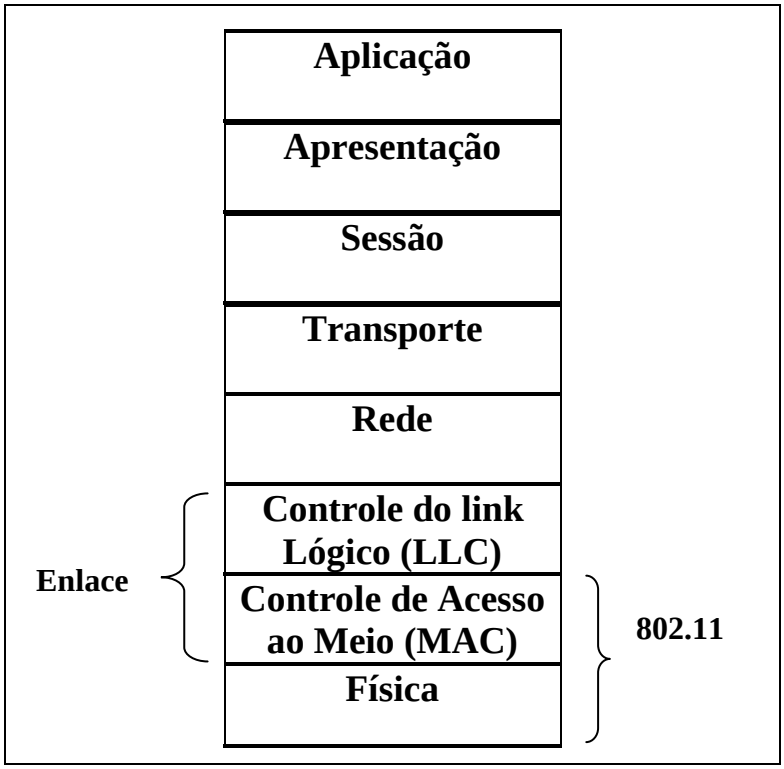


Figura 2. Modelo de uma rede utilizando o padrão IEEE 802.11.
Fonte: LIMA, J. (2005).

No próximo capítulo será visto uma outra tecnologia que se inclui neste ambiente wireless, que é o *bluetooth*, tecnologia na qual este trabalho está focado, mais especificamente, na sua segurança em transmissão de dados.

[6] É um tipo de cabo que possui uma blindagem, utilizado para conectar na placa wireless do computador.

4 BLUETOOTH

A origem do nome *bluetooth* surgiu no século X, na Dinamarca, onde existia um Rei chamado Harald Bluetooth. Um dos seus grandes feitos foi a unificação do país da Dinamarca. O Rei Harald reconstruiu igrejas e expandiu a fé cristã, fazendo com que a província dinamarquesa fosse unida sob uma única coroa. Assim como o rei Harald, a tecnologia *Bluetooth* também une pessoas, fazendo com que elas se comuniquem entre si. Por esse motivo a tecnologia recebeu o nome de *bluetooth* (MILLER, 2001).

O Símbolo ilustrado na Figura 3 representa o logotipo do *bluetooth*, que é composto pelas inicias H e B de Harald Bluetooth, na escrita alfabética dos povos germânicos, nos séculos III ao século XIV (MILLER, 2001).

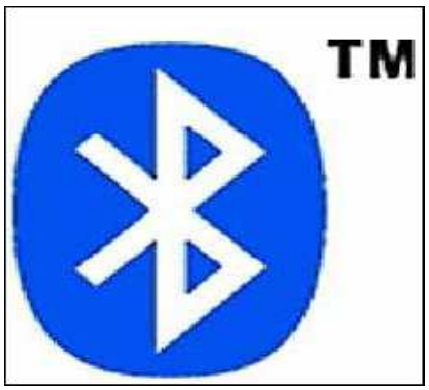


Figura 3. Logotipo do *Bluetooth*.
Fonte: MILLER, M. (2001).

Segundo Guimarães (2001), o *bluetooth* utiliza tecnologia de rádio enlace de baixo alcance. Um dos seus principais objetivos é eliminar a necessidade de cabos. Os dispositivos *bluetooth* podem detectar, conectar e descobrir os serviços oferecidos por outros dispositivos que estiverem ao alcance do sinal, apresentado de maneira bem clara na ilustração da Figura 4:

Figura 4. Integração do *bluetooth* com outros dispositivos com a mesma tecnologia.
Fonte: Modificado de KOBAYASHI, C. (2004).

4.1 COMUNICAÇÃO POR BLUETOOTH

O *bluetooth* é uma tecnologia que permite uma fácil comunicação sem fio entre diferentes dispositivos, como telefones celulares, palmtops, modems, impressoras, com um baixo custo e uma alta operabilidade. O *bluetooth* usa saltos de freqüência em uma taxa nominal de 1600 *hops/s* para sua comunicação (SACKS, 2003).

O *bluetooth* é uma comunicação não permanente (há seguidas desconexões) de curta distância (cerca de 10 metros, podendo chegar até 250 metros usando um amplificador opcional), que permite a transmissão de dados e voz, que se baseiam nas normas de padronização do IEEE 802.11 (OLIVEIRA; VENANCIO; POLIZER, 2006).

Segundo Carvalho (2003), o que caracteriza o *bluetooth* é que ele opera na freqüência de 2.45 GHz, de acordo com ilustração na Tabela 1, alcançando uma velocidade de até 723,1 Kbit/s, utiliza freqüência de saltos, suporta até oito equipamentos em uma *piconet*, utiliza a técnica de espalhamento espectral FH-SS[7], e é uma tecnologia de fácil migração para TCP/IP, regulamentada mundialmente.

Tabela 1. Alocação de Freqüência no aspecto internacional

[7] É uma técnica de espalhamento espectral utilizada para transmissão em rádio freqüência.

Região	Alocação de Freqüência	Canais *Bluetooth*
Brasil	2,4 – 2,4835 GHz	t = 2402 + KMHz k = 0 ... 78
Europa	2,4 – 2,4835 GHz	t = 2402 + KMHz k = 0 ... 78
Estados Unidos	2,4 – 2,4835 GHz	t = 2402 + KMHz k = 0 ... 78
Japão	2,471 – 2,497 GHz	t = 2473 + KMHz k = 0 ... 22

Fonte: SVERZUT, J. (2005)

A fim de não ter a possibilidade de ocorrer interferência entre protocolos, a tecnologia *bluetooth* divide a faixa em 79 canais e muda de canal até 1600 vezes por segundo.

Segundo Kobayashi (2004), o *bluetooth* foi projetado para reduzir a complexidade de conectar dois ou mais dispositivos, substituindo completamente os problemas com conexões físicas por conexão de freqüência de rádio sem fio. Uma outra característica do *bluetooth* é que os dispositivos móveis não precisam estar visíveis um ao outro para se comunicar, diferente das transmissões via infravermelho, em que se utiliza onda de luz e é necessário que os aparelhos estejam visíveis. As ondas de rádio que caracterizam a comunicação do *bluetooth* podem atravessar a maioria dos objetos sólidos.

4.2 COMO O BLUETOOTH FUNCIONA

Para explicar melhor o seu funcionamento, deve-se compreender, primeiro, o que é um *piconet*. São pequenas redes compreendidas de um dispositivo mestre conectado em qualquer lugar com um a sete dispositivos escravos (*slaves*) ativos (KOBAYASHI, 2004).

A Figura 5 está ilustrando dois *piconets,* que compartilham dois nós, o D e o E, que juntos formam um *scatternets* que são redes *wireless* criadas justamente quando ocorre essa união. Os círculos são as áreas de cobertura do *bluetooth* das quais os nós I, L, M e K não fazem parte.

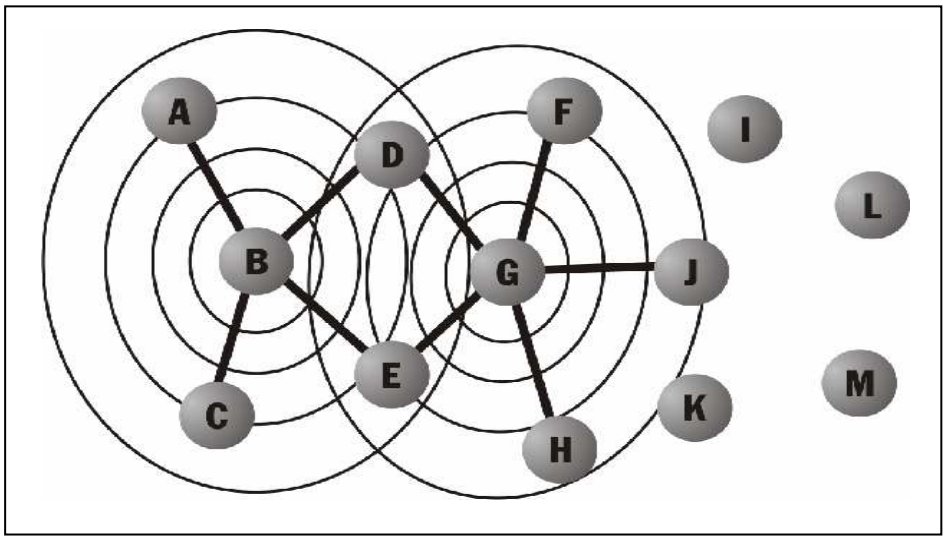


Figura 5. União de piconets
Fonte: Adaptado de OLIVEIRA, J. VENANCIO, G. POLIZER, S. (2006).

Segundo Kobayashi (2004), a tecnologia *bluetooth* possui quatro estados básicos de operação:

a) **mestre (*master*):** são os nós B e G, representados na Figura 5, que controlam um piconet;

b) **escravo ativo (*active slave*):** participam ativamente monitorando ou participando, dentro de uma rede piconet;

c) **escravo passivo (*passive slave*):** faz parte de um piconet, porém com baixa prioridade; permanece sincronizado e monitorando a rede;

d) **em espera (*standby*):** é o caso dos nós I, L, M e K, representados na Figura 5, que fazem parte do piconet, mas esperam por uma solicitação de outro dispositivo para poder se unir à rede.

4.2.1 Aplicação Bluetooth

Para entender melhor como começar uma aplicação *bluetooth* será tomado como exemplo o Prontuário Eletrônico, onde um usuário, neste caso um médico, irá passar para um servidor, através do cliente (celular), os dados coletados de um determinado paciente.

Conforme Billo (2003), para que essa aplicação funcione os seguintes passos devem ser tomados:

a) **inquiry:** pesquisa todos os pontos de acesso que estão ativos. Estes pontos encontrados respondem com o seu endereço físico que é único e é gerado do momento da fabricação de cada aparelho com esta tecnologia;

b) **paging:** nesta fase ocorre a sincronização entre o dispositivo e ponto de acesso;

c) **estabelecimento de um link:** logo após o procedimento de *paging*, é realizado o processo de estabelecimento de link. A camada responsável por este estabelecimento é a *Link Manager Protocol* (LMP);

d) **procura por serviços:** para o funcionamento correto da aplicação em questão, o próximo passa é a procura por serviços disponíveis. O meio responsável por este procedimento é o *Service Discovery Protocol* (SDP);

e) **L2CAP:** canal criado baseado nas informações disponibilizadas pelo SDP. Esse canal será responsável por estabelecer uma comunicação entre dois dispositivos;

f) **RFCOMM:** fornece uma emulação de portas seriais sobre o protocolo L2CAP. O RFCOMM é um protocolo de transporte simples e suporta até 60 (sessenta) conexões simultâneas.

Para casos que necessitam da integração com o TCP/IP, usa-se o protocolo *Point-to-Point Protocol* (PPP), que é responsável pela transmissão de pacotes através de um link serial que, no caso no *bluetooth*, é emulado pelo RFCOMM.

4.2.2 Estados para o Estabelecimento de Conexão

Segundo Cansado (2001), o *bluetooth* utiliza um diagrama de estado para resolver os problemas de estabelecimento de conexão entre os dispositivos. A Figura 6 ilustra este diagrama de todos os estados necessários para esta conexão.

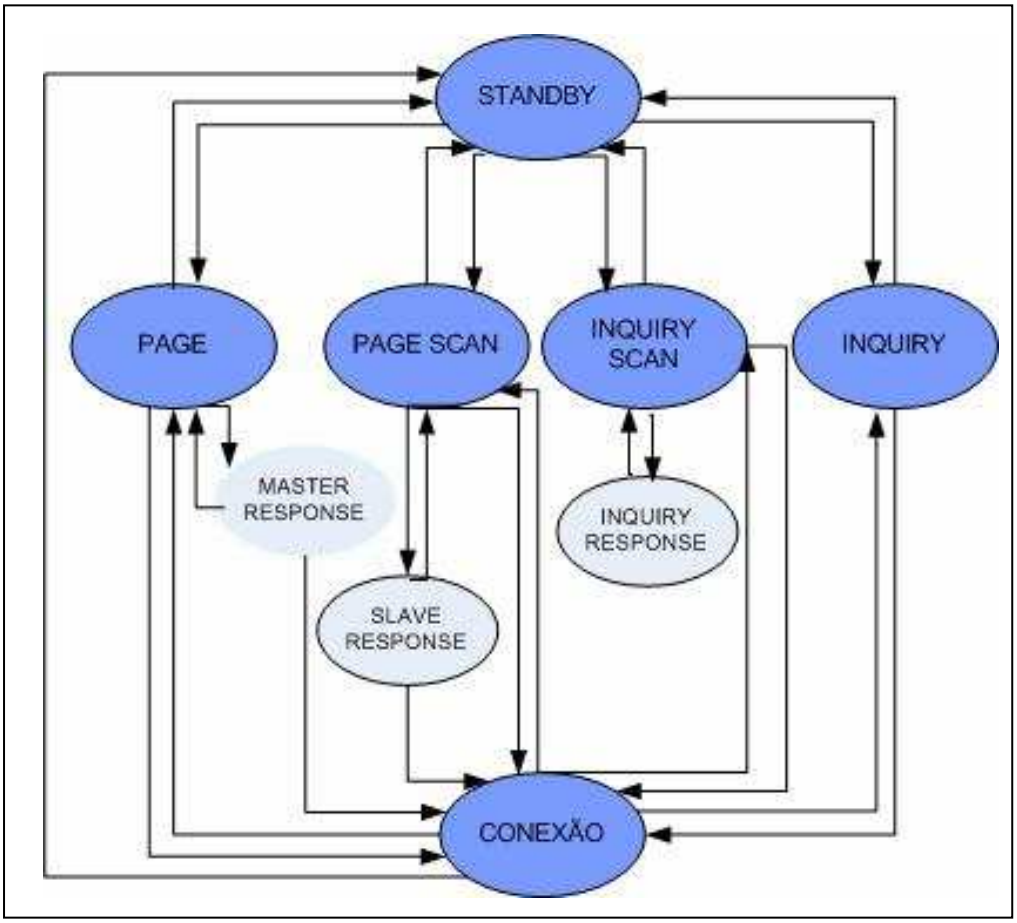


Figura 6. Diagrama de estado do controlador de ligação *bluetooth*.
Fonte: Adaptado de CANSADO, J. (2001).

Um determinado dispositivo como padrão se encontra no estado *standby*, podendo transitar entre os modos *inquiry*, *inquiry scan*, *page* e *page scan*, de acordo com a necessidade da aplicação:

a. **standby:** é um estado padrão em que todos os dispositivos se encontram antes do estabelecimento de um *piconet.* É o estado onde o consumo de potência é muito baixo, e somente o *clock* nativo do dispositivo é que fica ativo para continuar a realizar uma espécie de escuta na expectativa de receber alguma chamada (CANSADO, 2001);
b. **inquiry:** investiga os dispositivos que estão ativos na área de cobertura do sinal *bluetooth* e quais suas características, mandando um pacote especial chamado de *inquiry packet* (BILLO, 2003);
c. **inquiry scan:** segundo Cansado (2001), este estado é definido para a recepção de uma mensagem *inquiry*. De tempo em tempo, o dispositivo muda para este estado para ser descoberto por algum outro dispositivo. Se receber um pacote do tipo *inquiry packet*, o dispositivo responderá com um *inquiry response*;
d. **inquiry response:** neste estado o dispositivo que recebeu um pacote *inquiry packet* responderá com seu endereço físico para fazer com que o destinatário do pacote tome conhecimento de sua presença (BILLO, 2003);
e. **page:** utilizada pelo dispositivo que deseja estabelecer uma conexão (CANSADO, 2001);
f. **page scan:** estado é responsável por receber o pedido de estabelecimento de conexão do estado *page* (CANSADO, 2001);

4.2.3 Estrutura do Pacote de Dados do Bluetooth

Conforme Sverzut (2005), os pacotes de dados *bluetooth* são formados por campos necessários para representar as camadas requisitadas durante o processo de transação. A Figura 7 representa bem um pacote e suas composições.

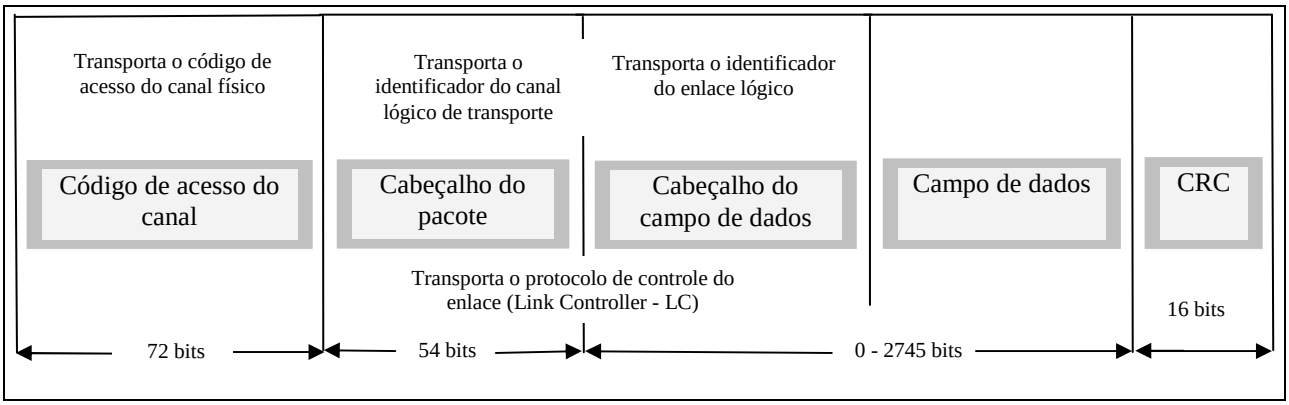


Figura 7. Estrutura básica do pacote de dados do *bluetooth*.
Fonte: Adaptado de SVERZUT, J. (2005).

O *Código de acesso do canal* representado na Figura 7 é um campo presente em todos os pacotes que identificam a comunicação em um canal físico. O código de acesso também é usado no sincronismo de tempo e nos procedimentos de descoberta e busca. É importante ressaltar que em um pacote de dados *bluetooth* não há campo identificando qual o endereço físico de cada dispositivo. Esta informação esta implícita em cada dispositivo móvel e é disponibilizada no momento que um determinado dispositivo faz a busca pelos mesmos (SVERZUT, 2005).

O *Cabeçalho do pacote* é responsável pelo transporte do endereço do canal de transporte lógico (LT_ADDR) que é utilizado por todos os dispositivos para saber se o pacote é endereçado para ele e também para encaminhar os pacotes internamente.

Segundo Sverzut (2005), o *cabeçalho do campo de dados* é um campo que inclui um identificador do enlace lógico usado para encaminhar os dados do pacote e um outro campo, identificando o tamanho dos dados.

O *campo de dados* é responsável pelo transporte de, por exemplo, voz, dados, ou ambos.

O campo da *verificação de redundância cíclica* ou *Cyclic Redundancy Check* (CRC) é usado para identificar os erros dos pacotes recebidos.

4.3 TRANSMISSÃO POR BLUETOOTH

Segundo Guimarães (2001), os sinais que a tecnologia *bluetooth* utiliza para a transmissão de dados são baseados em comutação de pacotes (os pacotes são fatiados em seu envio), ou seja, quando uma mensagem é enviada de um dispositivo A para um outro dispositivo B, ela pode ser transmitida por rotas, freqüências e ordens diferentes da original. Mas quando chega no seu destino, no caso do exemplo tomado, o dispositivo B, essa mensagem será recompilada na sua ordem original. Por outro lado, a comunicação por voz utilizada pelo *bluetooth* não é baseada em comutação de pacotes, e sim, na comunicação de circuito, onde um canal dedicado (ou circuito), é estabelecido durante a transmissão.

Segundo Oliveira (2003), a taxa de transferência total de 1Mbps da tecnologia *bluetooth* é o máximo teórico, as taxas de transferências efetivas variam de acordo com o tipo de comunicação. Por exemplo, a transmissão de dados *full duplex* (onde os sinais estão viajando simultaneamente nas duas direções) é realizada a 432,6Kbps. Já a transmissão de dados assimétrica (onde os sinais que vão em uma

direção são mais velozes que os sinais que vem na outra direção), ocorre na faixa de 721 Kbps na sua ida e 56 Hbps no seu retorno.

Se os sinais que estão sendo transmitidos forem de voz, a especificação determinada é de três canais de voz síncronos de 64 Khz cada (CANSADO; 2001).

4.4 APLICAÇÃO DO BLUETOOTH

Segundo Stallings (2002), o *bluetooth* possui três áreas de aplicação, utilizando a conectividade *wireless:*

a) **redes *Ad-hoc:*** o termo *Ad-Hoc* entende-se que pode ser algo que resolve um problema imediato, de caráter temporário que também tem como significado “apenas para este propósito”. Do Latin, *ad hoc* significa “para isto”. Em se tratando de redes, no entanto, significa muito mais do que isso. Fortes (2005), ainda afirma que numa rede *Ad-Hoc*, não se faz necessário uma pré-determinação da topologia ou configurações de pontos de acesso. Os nós ou nodos fazem parte da rede na medida em que se aproximam do sinal, não ocorrendo conexão física. Após o seu distanciamento da rede, o dispositivo não fará mais parte dela, ou seja, um dispositivo móvel equipado com a tecnologia *bluetooth* pode se comunicar com outro dispositivo desde que o mesmo esteja na área de alcance do sinal. A rede *Ad-Hoc* pode, então, ser definida como uma rede que permite que equipamentos sem fio se comuniquem sem nenhum ponto de acesso;

b) **substituição de cabos:** a tecnologia *bluetooth* possibilita ao usuário a eliminação de cabos, pois o mesmo dificulta a mobilidade, uma das

principais características das comunicações sem fios em geral. As comunicações são instantâneas e não permanentes, ou seja, ocorrem freqüentes desconexões ao longo da comunicação;

c) **suporte a comunicação de dados e voz:** permite a transferência de voz em tempo real e dados, podendo estabelecer comunicação de dispositivos móveis para fixos.

4.5 VANTAGENS E DESVANTAGENS NO USO DO BLUETOOTH

O *bluetooth*, ainda possui alguns problemas na sua utilização, segue uma lista de algumas vantagens e desvantagens no uso dessa tecnologia:

Tabela 2. Vantagens e Desvantagens do uso do *bluetooth*

Vantagens	**Desvantagens**
Tamanho reduzido.	Muitos problemas de segurança a serem resolvidos.
Dispensa o uso de cabos para se conectar.	Curto alcance (cerca de 10 à 250 metros);
Baixo custo benefício.	Limitado ao número de dispositivos para a comunicação;
Suporta comunicação de dados e voz.	Comunicação não permanente, ou seja, há seguidas desconexões.
Pode facilmente se associar a outros tipos de protocolos, por exemplos o TCP/IP.	Endereço MAC não dispõe de criptografia;
Sua comunicação se dá via ondas de rádio que permitem atravessar a maioria dos objetos sólidos.	Autonomia para os fabricantes definirem seus próprios padrões de criptografia e autenticação;

Fonte: Modificado de GORKI, S. NOVO, R. (2000).

Segundo Cronkhite e McCullough (2001), as placas de rede sem fio transmitem e recebem freqüência de rádio, e podem estar sujeitas à interrupção e ao uso de *sniffers*[8], fazendo com que informações importantes possam ser capturadas.

4.6 SEGURANÇA PARA O AMBIENTE SEM FIO

A segurança é definida como um conjunto de regras que especificam e padronizam um determinado sistema ou organização, e sua garantia é um dos processos básicos e prioritários em uma rede e em sistemas corporativos em geral (RUFINO, 2005).

Segundo Sena (2006), esse processo se apóia em três propriedades que definem a segurança: *disponibilidade* dos serviços e das informações, *integridade* e a *confiabilidade*.

A comunicação sem fio possui vulnerabilidades, pois usa do ar para se comunicar. Assim, qualquer dispositivo que estiver na área de cobertura do meio sem fio pode acessar ao meio.

4.7 SEGURANÇA PARA AMBIENTE BLUETOOTH

O tipo de comunicação que o *bluetooth* possui, ou seja, sinais de ondas de rádio, permite que os dados sejam facilmente capturados por outros dispositivos que estejam na área de comunicação. Para que isso não ocorra faz-se necessário o uso de outras tecnologias como a autenticação para prevenir as mensagens de origem duvidosa,

[8] (Analisadores de redes), ferramenta capaz de interceptar e registrar o tráfico de dados em uma rede de computadores.

Assinatura Digital e a Criptografia que permite que somente quem tenha a chave para decodificar os dados possa lê-los (OLIVEIRA, 2003).

A tecnologia *bluetooth* possui segurança que compreende os princípios básicos de integridade, confidencialidade e disponibilidade. Isso é dado pelo fato de essa tecnologia fazer o uso de procedimentos de autenticação e autorização (ROCHA; ELIAS, 2005).

O gerenciamento de chaves é utilizado para criar, armazenar e realizar a distribuição de chaves, todas derivadas da *chave de link*[9] (KARYGIANNIS, 2002).

A autenticação e autorização são dadas por meio de um sistema chamado de desafio-resposta, onde o dispositivo X quer estabelecer um link de comunicação com o dispositivo Y. Mas, antes, o dispositivo X que ter certeza que está se comunicando com o verdadeiro dispositivo Y. Para isso, X desafia Y que atua no papel de reivindicador para fazer a confirmação da chave de link que foi estabelecida entre os dois dispositivos (ROCHA; ELIAS, 2005).

Segundo Gehrmann (2004), outro processo que disponibiliza segurança na comunicação por *bluetooth* é o processo de *paring*, pois possibilita que dois dispositivos possam compartilhar uma chave secreta, denominada Inicialization Key (K_init). Após o procedimento de *paring*, os dispositivos X e Y citados no exemplo anterior terão certeza que estarão fazendo uma comunicação segura.

Segundo Kobayashi (2004), o *bluetooth* possui três modos de seguranças implementados:

a) ***sem Segurança (Non-Secure):*** normalmente é usado quando não se está transferindo ou recebendo dados importantes. Um exemplo desse modo

[9] Chave criptográfica estabelecida entre os dispositivos no processo de *paring*.

de transferência de dados sem segurança é a troca automática de cartões de negócio eletrônico;

b) **segurança estabelecida no nível do serviço (*Service Level Enforced Security*):** neste caso a segurança só é acionada depois de o dispositivo estabelecer a conexão;

c) ***segurança estabelecida no nível do link (Link Level Enforced Security):*** quando acionado esse modo, o tipo e o nível de segurança são utilizados para todo e qualquer tipo de aplicação, menos flexível do que o modo 2. Porém, ajuda a manter o padrão de segurança entre diferentes aplicações. Nesse modo o *bluetooth* aciona os métodos de segurança antes do dispositivo estabelecer a conexão;

No modo de segurança 2 é possível definir os níveis de segurança para os dispositivos e serviços, tendo dois níveis de confiança:

a) um dispositivo confiável, que possui uma relação fixa (emparelhada), é confiável e tem acesso irrestrito a todos os serviços (Kobayashi; 2004);

b) um dispositivo não confiável, que não possui uma relação fixa (mas possivelmente temporária), ou tem uma relação fixa, mas não confiável. O acesso aos serviços são restritos. Um possível refinamento é selecionar o nível de segurança dos dispositivos para serviços ou grupo de serviços. Serviços que exigem autorização (permissão ou negação de acesso a serviços), autenticação (identificação de quem está do outro lado da linha) e criptografia, são selecionados independentemente (CANSADO; 2001);

Segundo Kobayashi (2004), três níveis de segurança controlam o acesso aos serviços:

a) **serviços que exigem autorização e autenticação:** o acesso automático é apenas garantido para dispositivos confiáveis. Outros dispositivos necessitam de autorização manual;

b) **serviços que exigem apenas autenticação:** é exigida a autenticação para aqueles dispositivos que não são confiáveis**;**

c) **serviços disponíveis a todos os dispositivos:** o nível de segurança padrão é definido a partir das necessidades das aplicações herdadas. A diretriz padrão será usada a menos que outras aplicações sejam consideradas base de dados de segurança no que diz respeito a serviços, ou seja, dados de informação sobre segurança interna;

Mesmo que o *bluetooth* possua métodos de segurança citados anteriormente, muitas vulnerabilidades ainda são encontradas nessa tecnologia. Muitas delas ocorrem, geralmente, por falhas no padrão, como o caso da força do gerador de números randômico e o uso de um pequeno valor para o *PIN*. Outro fato que contribui para essa vulnerabilidade são as falhas de implementação, bem como a flexibilidade do padrão que oferece autonomia aos fabricantes para definição de diversos procedimentos relacionados à criptografia e autenticação (ROCHA; ELIAS, 2005).

Segundo Kobayashi (2004), devido ao fato do *bluetooth* utilizar ondas de rádio, muitos especialistas temem a sua segurança. Tal fato pode ser assentado por alguns aspectos:

a) a seqüência específica do *hopping* de canais é conhecida somente para emissão e para os dispositivos de recepção;

b) rotina de autentificação do tipo desafio-resposta para verificar a validade da unidade de recepção;

c) a chave de criptografia com tamanho 128-*bits* para estabelecer a transmissão entre dispositivos;

O *bluetooth* foi criado, inicialmente, para substituir cabos e reduzir a complexidade de conectar dois ou mais dispositivos. Com o seu crescimento e expansão, essa tecnologia vem sendo utilizada num âmbito muito maior, por causa de sua flexibilidade e baixo custo comparado com outras tecnologias. Por outro lado, a segurança nessa tecnologia não está acompanhando o seu crescimento, estabelecendo uma diferença muito grande entre flexibilidade e segurança das conexões (KOBAYASHI, 2004).

> Os aspectos de segurança desta tecnologia são cada vez mais necessários, devido ao aumento da aplicabilidade desta solução e a defasagem existente no aspecto da segurança. Esta relação viabilizou diversos estudos e propostas que conseqüentemente apresentaram novos problemas e possíveis soluções. (ROCHA; ELIAS, 2005, p.5).

5 INTEGRIDADE E CONFIDENCIALIDADE

A integridade e a confidencialidade estão diretamente ligadas à segurança dos dados e seu papel é o de proteger as informações contra modificações sem a permissão prévia do proprietário daquela informação. Tais modificações incluem ações como escrita, alteração no conteúdo, alteração de status, remoção e criação de informação.

A integridade deve ser observada nas mais variadas formas, como por exemplo, no armazenamento de um dado em disco ou backup: deve-se ter a garantia de que as informações contidas nesses periféricos estejam íntegras, sem modificações ou qualquer outra ação que prejudique sua integridade. Portanto, pode-se dizer que a integridade é a garantia que se tem de que uma determinada informação não foi modificada por um indivíduo que não tenha permissão (HINZ, 2000).

Segundo Sena (2006), confidencialidade significa proteger as informações contra sua revelação, leitura ou cópia por um indivíduo não autorizado. Um exemplo de confidencialidade, em se tratando de rede, é enquanto uma informação trafega na rede. Sabendo que a mesma é transmitida em partes, a garantia de proteção dessa informação tem que ser completa, pois se uma parte dessa transmissão for capturada e alterada, irá prejudicar a informação como um todo.

O objetivo da confidencialidade é proteger informações privadas (cidadãos, indústrias, governos, militar). Na comunicação a confidencialidade é garantida evitando a escuta (meio físico, topologia). Caso isso não seja possível, faz-se necessário o uso da criptografia (VELOSO, 2002).

6 CRIPTOGRAFIA

Manter a segurança das informações em um ambiente computacional é muito importante e é uma preocupação constante nas vidas das pessoas. Desde os tempos mais remotos essa necessidade de manter os dados sigilosos já existia. Nos tempos atuais com a tecnologia muito mais evoluída essa preocupação se torna ainda maior. Portanto a criptografia veio para sanar este incômodo, fazendo com que as informações tornem-se segura contra os possíveis ataques.

Segundo Hinz (2000) a criptografia é uma das técnicas mais utilizadas para fazer a segurança dos dados, utiliza algoritmos especiais de tratamento de dados, evitando que dispositivos que não conheçam esse algoritmo consigam decodificar e acessar os dados.

O objetivo geral da criptografia é fazer com que as informações que forem criptografadas sejam inviáveis de ser decifradas. A criptografia, juntamente com a criptoanálise, faz parte da área de conhecimento chamada de criptologia. A criptografia é utilizada em caráter defensivo. Tem como objetivo garantir a confidencialidade, autenticidade e a integridade das informações. Já a criptoanálise é o inverso, é a junção de ferramentas e métodos capazes de quebrar a proteção feita pela criptografia (SENA, 2006).

Com o uso da criptografia há uma redução insignificante do desempenho da rede, dado a importância e a necessidade que há em manter as informações seguras e confidenciais. Não faz sentido manter uma rede desprotegida sabendo que a performance da rede é quase imperceptível na presença da criptografia. Essas informações foram comprovadas pelo Laboratório de Pesquisa da revista Info (InfoLab), onde um arquivo de 10 MB foi transmitido com e sem criptografia, e o

resultado foi o de que quase não houve diferença perceptível no envio dos dois arquivos (COSTA, 2006).

Desse modo, deve-se estar ciente de que os ataques e invasões às informações sigilosas são possíveis, e, muitas vezes, pelas mesmas ferramentas que fazem a proteção desses dados. Ou seja, os recursos usados por aqueles que se interessam em proteger as informações são também de grande utilidade para os *crackers*[10] digitais que desejam invadir e capturas dados importantes.

A criptografia possui algumas técnicas principais que ajudam a proteger as informações: Criptografia Simétrica, Criptografia Assimétrica, Assinatura Digital, Certificação Digital e Autenticação.

6.1 CRIPTOGRAFIA SIMÉTRICA

Segundo Cavalcante (2004), é o ato de transformar uma mensagem originalmente escrita em uma mensagem cifrada, ilegível a quem não possui a chave secreta. Tal chave é gerada fazendo compartilhamento somente da origem para seu destinatário. Para tornar uma mensagem cifrada legível é aplicado o método de descriptação, usando a mesma chave usada para encriptar. Assim, tanto o emissor quanto o receptor precisam ter a mesma chave e mantê-la em segredo. Por isso que também é chamada de codificação por *chave secreta*.

Geralmente os algoritmos simétricos usados possuem dois subtipos: algoritmo de *fluxo* e de *bloco*. Segundo Cronkhite e Mccullough (2001), o algoritmo de *fluxo* funciona sobre o texto, lendo um *byte* de cada vez; e o de *bloco* trabalha sobre os blocos de texto.

[10] Termo utilizado para quem pratica a quebra de um sistema de segurança de forma ilegal.

A vantagem de utilizar a criptografia simétrica é a de que o seu processo é mais simples que a chave pública. A codificação com a chave simétrica é cerca de 1.000 vezes mais rápida do que com a pública. Por outro lado, sua desvantagem é a de que tanto o receptor quanto o emissor têm que obter uma chave comum a ambos, sem que seja comprometida, além da mensagem transitar mais vezes na rede fazendo com que haja transtornos aos usuários que estão transmitindo a mensagem (CRONKHITE; MCCULLOUGH, 2001). A Tabela 3 ilustra esse problema, onde R representa o receptor e D o destinatário.

Tabela 3. Problemas dos constantes tráfegos na rede do algoritmo simétrico

Processo de codificação de chaves do algoritmo simétrico
1º "**R**", escolhe um cadeado para a qual somente ele tem a chave;
2º "**D**", escolhe um cadeado para a qual somente ele tem a chave;
3º "**R**" tranca a mensagem em uma caixa, usando seu cadeado e manda a caixa para "**D**";
4º "**D**" adiciona sua chave a caixa e manda para "**R**";
5º "**R**" destranca seu cadeado e manda para "**D**";
6º "**D**" agora recebe a caixa contendo somente seu cadeado, bastando destrancá-la para ler a mensagem.

Fonte: BALPARDA, D. (2001).

Esse tipo de problema ilustrado na Tabela 3 é solucionado com a aplicação da chave pública.

6.2 CRIPTOGRAFIA ASSIMÉTRICA

Também conhecida como criptografia de chave pública, a criptografia assimétrica usa, para aplicar o método de decriptação e encriptação, duas chaves distintas relacionadas, uma para cada método. Essa criptografia, além da integridade da autenticação e confidencialidade, também apresenta autoria garantida, pois como o próprio nome diz, a chave pública não precisa ser mantida secreta. Para que a

mensagem possa ser enviada é necessária uma autenticidade, ou seja, deve haver a garantia de que a chave pública realmente pertence à pessoa a que será destinada a mensagem (CAVALCANTE, 2004).

A Figura 8 ilustra o processo de criptografia por chave pública, onde o emissor manda uma mensagem para um destinatário qualquer, usando a chave pública para codificar a mensagem. O destinatário, por sua vez, usa da chave privada para decodificá-la.

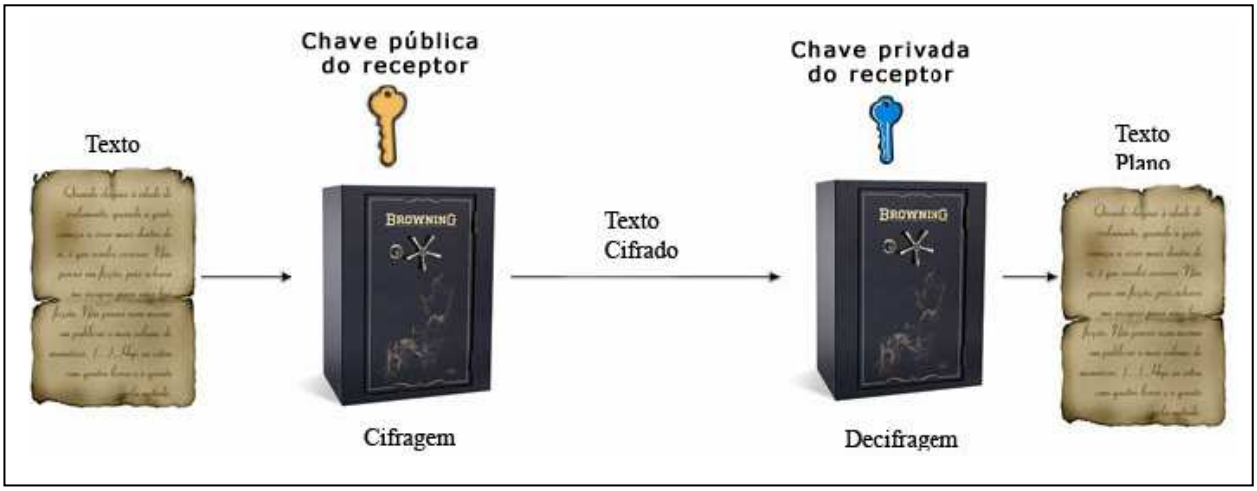


Figura 8. Processo de Criptografia por chave pública
Fonte: GASPARETO, E. (2005)

Os algoritmos assimétricos são algoritmos muito complexos que usam grandes fórmulas matemáticas. Alguns algoritmos baseiam-se em números primos, fatoração, curvas elípticas, logaritmos, treliças e outras fórmulas matemáticas. O algoritmo criptográfico por chave pública tem como objetivo tornar um problema difícil de tal maneira que seja inviável que, num possível ataque, esse problema possa ser resolvido. Pesquisadores estimam que para desvendar o sistema de *Rivest, Shamir e Adelman (RSA),* por exemplo, seria necessário cerca de 4.300 computadores em 50 anos, usando uma chave de 760 *bits*. Portanto, é possível desvendar, mas é improvável que suas informações sejam desvendadas usando esse tipo de sistema (CRONKHITE;

MCCULLOUGH, 2001). É importante salientar que os dados do exemplo acima citado, nos tempos atuais, com computadores cada vez mais modernos, não seriam reais. No entanto, a quebra da chave continuaria improvável de ser desvendada.

O algoritmo de chave pública veio para resolver o problema das chaves privadas, no que diz respeito aos constantes tráfegos na rede, como mostra a Tabela 4 onde, R representa o receptor e D o destinatário.

Tabela 4. Funcionamento de troca de mensagem por chave pública

Processo de codificação da chave pública
1) "D" escolhe um cadeado, onde somente ele tem a chave, e manda aberto para todas as pessoas que o quiserem;
2) "R" pega o cadeado aberto de "D", e tranca com o mesmo a caixa onde contém a mensagem, logo depois "R" manda a caixa para "D";
3) "D" usa sua chave para abrir o cadeado e ler a mensagem.

Fonte: BALPARDA, D. (2001).

6.3 ASSINATURA DIGITAL

Segundo Cunha (2000), além da questão da integridade da mensagem, a assinatura digital é sugerida também para prover uma outra necessidade: a garantia, por parte do receptor, da origem da mensagem. Quando uma mensagem é enviada, é necessária a garantia de que ela tenha partido realmente do emissor. Ou seja, além da integridade e privacidade da mensagem, ela também deve ser autêntica e a operação deve efetivamente ser realizada em nome do emissor, lembrando que a assinatura digital não foi criada para proteger uma mensagem contra o inimigo, mas sim, garantir que uma determinada pessoa assinou efetivamente a mensagem. O que realmente importa neste caso é que a assinatura não seja falsificada.

A utilização da Assinatura Digital tem o mesmo objetivo que uma assinatura convencional em documentos impressos com a finalidade de garantir que uma determinada pessoa escreveu ou concordou com um processo ou documento.

A assinatura digital, quando solicitada, faz cálculos de um resumo da mensagem por intermédio de uma função chamada *hash*[11], junto a ela também se adiciona a cifragem do resumo, além de outras informações. Para tudo isso se usa um algoritmo de chave pública e utiliza-se a chave privada do transmissor para fazer a operação de criptografia (BALPARDA, 2001). Para decifrar essa mensagem cifrada basta ter a chave pública do transmissor. Então, sabendo que somente o transmissor-assinante tem em poder a chave privada, se tem a garantia de que apenas ele pode ter assinado a mensagem, garantia essa que se tem pelo fato de que somente a entidade que assina a mensagem, possui o conhecimento da chave privada.

> Assinatura Digital é resultado de uma complexa operação matemática que trabalha com um conceito conhecido por criptografia assimétrica. A operação matemática utiliza como variáveis o documento a ser assinado e um segredo particular, que só o signatário eletrônico possui: a chamada chave privada. Como somente o titular deve ter acesso à sua chave privada, somente ele poderia ter calculado aquele resultado, que, por isso, se supõe ser único e exclusivo, com uma assinatura (ICP-BRASIL, 2007).

Sabendo que somente aquele que tiver em poder da chave privada do transmissor poderá cifrar a mensagem, ficará inviável que um terceiro que não conheça a chave privada altere a mensagem. Desse modo, com a assinatura digital e a presença de um resumo válido, há uma garantia da integridade da origem da mensagem.

A Assinatura Digital é semelhante aos Medium Access Control (*MACs)* porque combina o valor de *hash* da mensagem com uma chave. Os algoritmos de *RSA, Digital Signature Algorithm (DSA), e Digital Signature Standard (DSS)* são algoritmos de assinatura digital bastante utilizados (BALPARDA, 2001).

[11] É a transformação de uma grande quantidade de informações em uma pequena quantidade (Resumo).

A assinatura digital tem um grande valor para empresas que desejam agilizar alguns processos. Um pedido de venda com o valor superior a R$ 10.000,00 (dez mil reais), por exemplo; só pode ser liberado com autorização de alçadas maiores dentro da empresa. Desse modo, é feito uma assinatura digital para os responsáveis que deverão liberar ou rejeitar o pedido de venda.

Segundo Balparda (2001), existem três regras gerais para assinatura digital:

a) nunca assinar um documento do qual não se saiba a origem, pois isso viabiliza o ataque do inimigo, dando-lhe a possibilidade de capturar a chave privada;

b) assinar, preferencialmente, valores *hash* de mensagens maiores. Isso evita que sejam assinadas mensagens muito grandes, que não garantem a sua integridade;

c) quando uma mensagem exigir um valor aleatório, este nunca poderá ser reutilizado. Caso aconteça, o inimigo poderá descobrir a chave privada, tendo a liberdade de modificar tal assinatura;

Numa visão geral, a assinatura digital, normalmente, usa o mesmo esquema das chaves públicas, em que a chave privada é utilizada por quem assina um determinado documento e a chave pública é usada para garantir a autenticidade do documento assinado. As assinaturas digitais foram feitas para autenticar um documento com o objetivo de substituir eletronicamente a assinatura do mundo real (BALPARDA, 2001).

6.4 CERTIFICADO DIGITAL

A criptografia por chave púbica solucionou vários problemas com relação à criptografia por chave secreta. Surgiu, porém, um novo problema. Quando é usada a chave pública do emissor para verificar os dados ou verificar sua assinatura, surgem algumas dúvidas do tipo:

a) Será que a chave pública realmente é a qual se acredita ser?

b) A chave pública está atualizada?

c) Será que o emissor é realmente o qual se acredita ser?

O Certificado Digital ajuda a focalizar esse problema, pois oferece a certeza de que o emissor é realmente aquele que afirma ser. Essa certeza e confiança é chamada de *autoridade de certificados (CAs).*

A Figura 9 ilustra um processo de troca de mensagem, utilizando a certificação digital, em que emissor envia uma mensagem para um destinatário qualquer, utilizando o certificado digital que possui. O emissor recebe sua chave pública e envia sua mensagem juntamente com o certificado. O destinatário, ao receber a mensagem, tem dúvidas quanto à sua origem. Então, ele seleciona a opção “verificar autoridade”, e em seguida se conecta no servidor de autoridade de certificado, onde o mesmo retorna, informando que o certificado é válido, assegurando de que a mensagem realmente veio de quem acredita ter vindo.

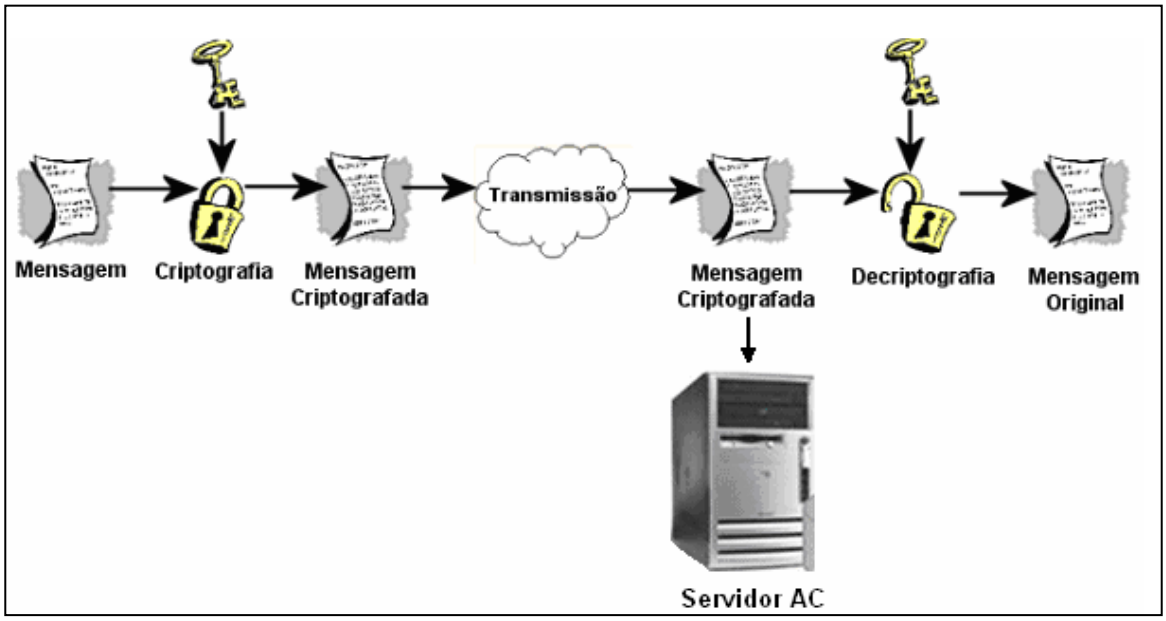


Figura 9. Processo de Certificado Digital.
Fonte: Modificado de CRONKHITE, C. MCCULLOUGH, J. (2001).

Segundo Borges (2004), o certificado digital é emitido por meio de uma Autoridade Certificadora (AC) e assinado com sua chave privada. Para isso, essa autoridade utiliza os padrões internacionais que contêm três elementos:

a) informação de atributo: são informações referentes a seus dados, por exemplo: Nome, Endereço, E-Mail, entre outros;
b) chave de informação pública: é uma chave pública da entidade certificada; pode ser qualquer chave assimétrica. Usualmente, é uma chave RSA;
c) assinatura da autoridade em Certificação: responsável por assinar os dois primeiros elementos. Logo após, é adicionada a credibilidade ao certificado.

Segundo Borges (2004), a estrutura dos Certificados Digitais é definida por um padrão chamado Padrão X.509, que atualmente está em sua versão 3. O mesmo possui várias informações a serem fornecidas para que haja a garantia de segurança nas

operações realizadas. Na Figura 10 está representada a estrutura do certificado X.509 com:

a) versão do certificado;

b) número de série: Seqüência única para cada AC;

c) identificador do algoritmo de AD: Identificador do algoritmo a ser utilizado para assinatura do certificado;

d) emissor: Nome do responsável pela emissão do certificado digital;

e) período de validade;

f) titular: Nome ou identificador do emissor do certificado digital;

g) identificador único do emissor do título: Este campo foi criado na versão 2 deste padrão com intuito de reutilização do certificado. Hoje não é mais recomendado. O que se recomenda é a emissão de um novo certificado digital;

h) extensões: campo livre. Utilizá-lo de acordo com objetivo;

i) assinatura do emissor: É a assinatura da Autoridade Certificadora.

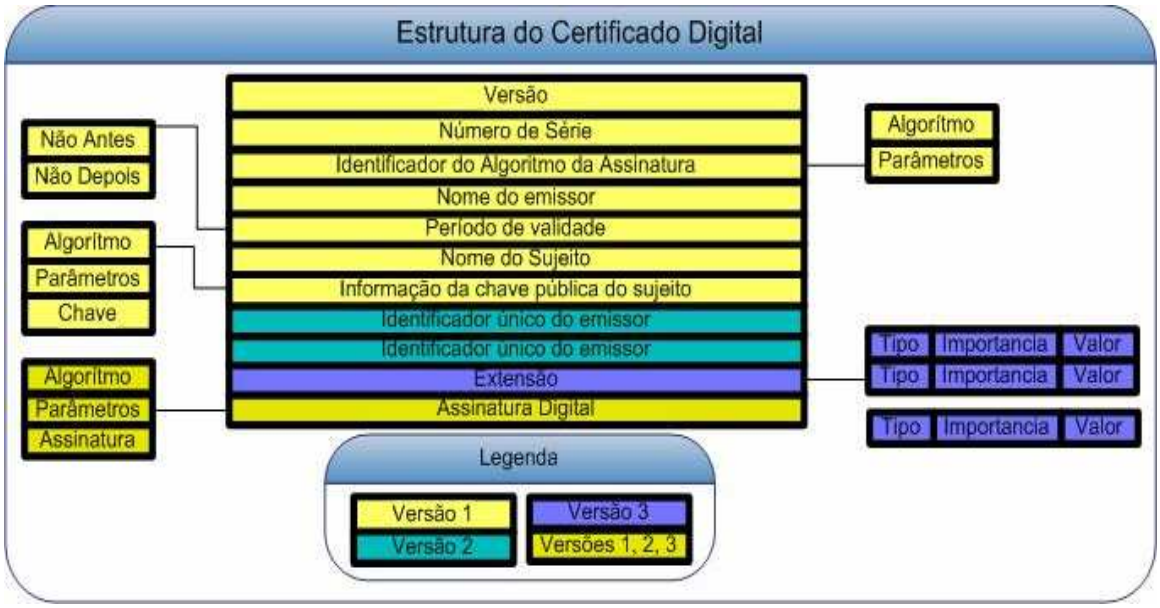


Figura 10. Estrutura do Certificado Digital Padrão X.509.
Fonte: Modificado de BORGES, R. 2004.

6.5 AUTENTICAÇÃO

Segundo Lee, Schneider e Schell (2005), a autenticação é a garantia que se tem de que a origem da mensagem é realmente confiável e verdadeira. Ou seja, garante que os dados recebidos correspondem realmente àquele que originou a mensagem. A autenticação permite que somente os dispositivos autorizados participem da comunicação, evitando mensagens de origem duvidosa e acesso não desejado a dados não autorizados como, por exemplo, ameaças por *spoofing*[12], garantindo a integridade dos dados.

A autenticidade é um serviço relacionado à identificação. Aplica-se tanto à informação em si quanto às partes que participam de uma comunicação. Na criptografia, essas duas questões são chamadas de autenticação da entidade e autenticação da origem dos dados. Esta, por sua vez, está intimamente relacionada à integridade dos dados (KIM, 2003).

Segundo Santin et al (2000), a autenticação é essencial num esquema, por exemplo, do tipo “desafio e resposta”, onde o protocolo de segurança especial é usado para saber se um dispositivo reconhece uma chave secreta compartilhada. Se os dois dispositivos reconhecerem a chave, a autenticação será bem sucedida e a comunicação será liberada. Mas, se um dos dois dispositivos não reconhecerem a chave, a comunicação será abortada.

Um exemplo simples de autenticação é a informação de senhas para se conectar a algum site ou um sistema qualquer. A Tabela 5 ilustra esse caso, onde U é o usuário que informará a senha e B é o banco de dados que faz a autenticação do usuário.

[12] Invasor fingindo ser um usuário confiável.

Tabela 5. Simulação de uma autenticação por meio de senhas

Passos de uma autenticação entre usuário e o banco de dados
1º “U” fornece a senha ao banco de dados, ou escolhe uma, caso não esteja cadastrada;
2º Caso “U“ não esteja cadastrado, “B” guarda a senha informada por “U”;
3º Caso contrário o servidor verifica a senha informada;
4º Se a senha informada for igual a que “B” possui, conexão aceita;
5º Se a senha informada por “U”, for diferente de “B”, conexão recusada;

Fonte: BALPARDA, D. (2001).

No exemplo ilustrado na Tabela 5, as senhas armazenadas no servidor ficam muito expostas a ataques, caso o invasor tenha acesso ao banco de dados. A Tabela 6 ilustra um caso correto de procedimentos que se deve tomar neste caso.

Tabela 6. Simulação de uma autenticação por meio de senhas criptografadas

Passos de uma autenticação segura utilizando a criptografia
1º “U” fornece a senha ao banco de dados ou escolhe uma, caso não esteja cadastrada;
2º Caso “U“ não esteja cadastrado, “B” criptografa a senha e armazena no banco de dados;
3º Caso contrário, o servidor verifica a senha informada, descriptografando a senha que se encontra no banco de dados e compara com a que “U” informou;
4º Se a senha informada for igual a que “B” possui, conexão aceita;
5º Se a senha informada por “U” for diferente de “B”, conexão recusada;

Fonte: BALPARDA, D. (2001).

Neste caso, mesmo que o inimigo tenha acesso ao banco de dados e às senhas dos usuários, terá dificuldades de identificá-las, dado à criptografia aplicada antes das senhas serem armazenadas no banco de dados.

Esse tipo de criptografia também é possível em ambientes móveis, segundo Lee, Schneider e Schell (2005). Certos bancos de dados de dispositivos móveis como, por exemplo, o Microsoft SQL Server CE, podem ser criptografados. Portanto, mesmo que um Pocket PC seja perdido, torna-se praticamente impossível que os dados contidos no banco de dados deste dispositivo sejam decifrados.

6.6 AUTENTICAÇÃO BIOMÉTRICA

O termo biometria vem do grego *“bios”* que significa vida e *“metron”*, medida. A autenticação biométrica foi criada com o objetivo de identificar uma determinada voz, impressão digital ou retina, através de uma amostra de propriedade biológica (GOMES, 2007).

Segundo Lee, Schneider e Schell (2005), a autenticação biométrica também ajuda a diminuir as ameaças de *spoolfing* e reduz a vulnerabilidade da aplicação corporativa em ser atacada, visto que essas técnicas de identificação são feitas com muita exatidão, reduzindo o número de erros a praticamente zero.

A autenticação biométrica pode ser classificada, conforme Gomes (2007), como comportamental ou física. A autenticação biométrica comportamental consiste em lidar com a forma com que as pessoas se comportam, como por exemplo, a voz. Já, a física, está ligada à fisionomia da pessoa, como a impressão digital, leitura da face e leitura da retina.

A autenticação biométrica dispõe de várias técnicas, dentre elas a *geometria da mão* que consiste em analisar o formato da mão através de sensores; comprimento dos dedos, linhas e características específicas. Outra técnica usada é a *impressão digital* que dispõe de dispositivos ópticos ou capacitivos para analisar as impressões digitais, traços e características dos dedos. *Reconhecimento da íris* também é um outro método de análise biométrica que está associado ao olho humano. É uma das técnicas com os melhores resultados, porém, pouco usada por necessitar um hardware de custo bastante elevado. Existem outras técnicas como o *reconhecimento da retina*, *reconhecimento facial* e *reconhecimento de voz* (GOMES, 2007).

6.7 PRINCIPAIS ALGORITMOS PARA SEGURANÇA

Um dos primeiros indícios de algoritmos de criptografia que se tem é o algoritmo de César, utilizado pelo imperador da Roma antiga Júlio César, que consistia na substituição do alfabeto em uma determinada mensagem, deslocando um caractere da mensagem três posições do alfabeto para frente, ou seja, a letra A do alfabeto substituiria pela D, a B pela E, e assim sucessivamente (Hinz, 2000).

Os algoritmos de segurança segundo Balparda (2001) tem como objetivo assegurar e manter a autenticidade, confidencialidade e integridade das informações. Cada um desses algoritmos possui suas características próprias, usando diferentes tipos de cálculos e métodos para manter essas informações seguras. A seguir, será visto alguns algoritmos e métodos de segurança.

6.7.1 Algoritmo RSA

Elaborado pelos autores que deram nome ao algoritmo: *Rivest, Shamir e Adelman* em 1977. É um dos algoritmos mais usados e testados, É muito usado em assinaturas digitais (CAVALCANTE, 2004).

A segurança deste algoritmo é dada pela dificuldade computacional em fatorar um número inteiro em primos. Com a complexidade desse cálculo, porém, também vem a lentidão ao criptografar e decriptografar uma mensagem. Por isso, o que se faz é pegar um outro algoritmo simétrico e uma chave aleatória para encriptar uma determinada mensagem. Use-se, assim, o RSA para criptografar esta chave escolhida, resolvendo o caso da demora (BALPARDA, 2001).

Segundo Barbosa et al (2003), o funcionamento do algoritmo RSA e dado da seguinte forma:

a) Primeiramente, deve-se escolher dois números primos (“x” e “y”) grandes para dificultar a sua quebra;
b) Calcular o valor de n= x * y;
c) Calcular o Φ n = (x - 1) * (y - 1);
d) Selecionar um inteiro “z”, relativamente primo à Φ n e 1 < z < Φ n;
e) Calcular k de forma que (k * z) mod Φ n = 1;

Neste algoritmo é necessário que o destinatário saiba o valor de “n” o remetente do valor de “k” e somente o destinatário saber o valor de “z”.

6.7.2 Algoritmo DES

O Data Encryption Standard (DES) foi criado pela empresa IBM, em 1977, e, segundo Silva (2000), é um dos algoritmos simétricos mais disseminado no mundo. Sua chave possui o tamanho de 56 bits e permite cerca de 70 quadrilhões de combinações ou 2^{56}. Apesar do tamanho de suas combinações serem visualmente grande, a chave de 56 bits é considerada pequena.

Segundo Livro Segurança Máxima (2000) o DES é um algoritmo matemático assim como o algoritmo de RSA, onde é baseado em funções matemáticas para criptografar e decriptar dados. O DES é um algoritmo de bloco, ou seja, atua como uma cifra em bloco de dados de tamanho determinado. O DES desempenha três operações importantes onde a primeira é a permutação inicial que consiste em trocar os bits de dados de posição, reescrevendo-a verticalmente. Como por exemplo, em uma string “THE RED CAR”, aplicando a técnica de permutação inicial, logo, ficará:

THE

RED

CAR

Logo após é reconstruída a mensagem em uma string horizontal, onde usando a continuação do exemplo citado a cima ficara:

TRC HEA EDR

Naturalmente a permutação inicial é infinitamente mais complexa do que o exemplo citado, mas ela acontece de uma maneira semelhante. Por meio dessa permutação inicial, o DES deriva um bloco de entrada. O bloco de entrada então é embaralhado por operações matemáticas bastante complexas, cujo este processo é chamado de transformação que irá produzir um bloco de pré-saídas. Por fim, o bloco de pré-saída esta sujeito ainda a outras permutações e o resultado final é o texto embaralhado, as vezes chamada de texto criptografado, mais precisamente referido como texto codificado (LIVRO SEGURANÇA MÁXIMA, 2000).

6.7.3 Algoritmo RIJNDAEL

Assim como no algoritmo do RSA, o nome que deu origem ao algoritmo de RIJNDAEL foram os nomes de seus criadores, Vincent Rijmen e Joan Daemen. Esse algoritmo fornece flexibilidade na escolha dos tamanhos das chaves que podem ser escolhidas entre 128, 192 ou 256 bits. Também assim como o algoritmo DES o RIJNDAEL é um algoritmo de bloco e utiliza de quatro funções para fazer o processo de criptografia que são elas *ByteSub*, *ShiftRow*, *MixColumm* e *AddRoundKey*, onde juntas compõem todo processo criptográfico deste algoritmo (HINZ, 2000).

Segundo Rosa e Faleiros (2003) o algoritmo de RIJNDAEL possui um número variável de *rounds*, esta variação ocorre de acordo com o tamanho da chave escolhida onde:

- *round 9* se o bloco e a chave for de 128 bits;
- *round 11* para as chaves e blocos de 192 bits, e que nenhuma for maior que isso;
- *round 13* se o bloco e a chave for de 256 bits;

Para criptografar um bloco de dados, primeiramente é executado o método *Add Round Key* que por sua vez faz uma lógica denominada *XOR*[13] entre uma sub-chave e um bloco, logo depois é executado o método *Mix Columm* que nada mais é do que a multiplicação de matrizes, após isso é executa o método *Byte Sub* que consiste na troca por seu substituto em uma outra matriz denominada de S-Box, essa troca ocorre para cada round que pode variar de acordo com tamanho da chave escolhida. Por final é executado o método *Shift Row* (HINZ, 2000).

[13] Chamada também de disjunção exclusiva, é uma operação lógica em dois operandos que resulta em um valor lógico verdadeiro se e somente se exatamente um dos operandos tiver um valor verdadeiro.

7 VULNERABILIDADES EM REDES SEM FIO BLUETOOTH

Ataques em ambientes que utilizam a tecnologia *bluetooth* vêm se tornando comuns. E o que se percebe é que os grandes ataques são realizados em celulares e não em PDAs, talvez pelo fato de as pessoas possuírem mais um do que o outro. Muitos destes ataques ocorrem por falta de configuração do aparelho. Grande parte, porém, ocorre por problemas relacionados à implementação nativa da tecnologia *bluetooth*.

Segundo Kovacs e Monteiro (2005), existem várias formas de ataques a redes *bluetooth*, uma delas é o chamado "*bluejacking*" que nada mais é do que enviar mensagem aos dispositivos que estiverem ativos. Outra forma de ataque é a negação de serviço via *bluetooth* que consiste em enviar um pacote do tipo *ping*[14] para os dispositivos, fazendo com que mais nenhum dispositivo possa se conectar ao dispositivo atacado. Existem, também, ataques que podem desabilitar ou tirar serviços de operação. O "PIN *cracking*" é um outro método de ataque. Como já foi mencionado no capítulo 4.7, o *personal identification number* (PIN) é a senha de proteção do *bluetooth*, composta por apenas 4 (quatro) dígitos. portanto com o método de ataque PIN cracking torna-se possível obter o número do PIN. Esse ataque é conhecido como força bruta. Com ele também podem ser feitas descobertas de dispositivos que se encontram ocultos e se consegue recuperar seu endereço MAC.

O endereço MAC do *bluetooth* é composto por uma seqüência de 6 bytes que identificam o dispositivo. Os primeiros três bytes são impostos pelo IEEE que identificam o fabricante do equipamento e os últimos três são atributos do próprio fabricante.

[14] Comando usado pelo protocolo ICMP para testar conectividade entre equipamentos.

Se for pensar em uma forma rápida e prática de tornar esses dispositivos mais seguros, logo será pensado em manter os dispositivos *bluetooth* no modo invisível ou desabilitado. Mas na prática isso não daria muito certo, pois já existem ferramentas que descobririam seu dispositivo. São ferramentas que utilizam o ataque do tipo "*força bruta*" para descobrir todos os dispositivos invisíveis da rede. Uma destas ferramentas tem o nome de "RedFang", criada por Ollie Whitehouse. O seu grande desafio é conseguir descobrir todos os dispositivos que estão no alcance do sinal *bluetooth* num curto espaço de tempo, cerca de 3 (três) minuto. É o tempo que se leva, em média, para verificação de um único dispositivo (KOVACS; MONTEIRO, 2005).

Um dos principais problemas da especificação *bluetooth* é que durante a comunicação entre os dispositivos pode-se facilmente obter o endereço MAC dos mesmos, já que o endereço em si não é criptografado.

Segundo Kovacs e Monteiro (2005), o tráfego e informações de um aparelho de telefone T610 da marca Sony Ericsson e outras marcas são facilmente capturados por comando. A Figura 11 mostra um comando no Linux que obtém do aparelho citado anteriormente toda a agenda telefônica nele contida.

```
# hcitool scan
Scanning .
00:0A:D9:15:0B:1C T610-phone
# obexftp -b 00:0A:D9:15:0B:1C --channel 10 -g telecom/pb.vcf -v
Browsing 00:0A:D9:15:0B:1C ...
Channel: 7
No custom transport
Connecting...bt: 1
done
Receiving telecom/pb.vcf...\done
Disconnecting...done
```

Figura 11. Comando no Kernel do Linux para captura de uma agenda telefônica de um aparelho celular
Fonte: KOVACS, B; MONTEIRO, V. (2005).

Os comandos "hcitool" e "obexftp" são comandos do Linux que servem para roubar informações de um aparelho, através da tecnologia *bluetooth*. Esta

vulnerabilidade foi descoberta por Adam Laurie e afeta diversos dispositivos. Entre eles estão:

a. **nokia:** 6310 – 6310i – 8910 – 8910i;

b. **sony ericsson:** T68 – T68i – R520m – T610 – Z600, entre outros.

7.1 TÉCNICAS DE ATAQUE PARA REDES SEM FIO

Uma rede sem fio desprovida de uma boa segurança é um risco que se tem, pois as portas ficam vulneravéis para os ataques de *hackers*[15]. Esses tipos de ataques em redes sem fio são bem conhecidos, pois têm as mesmas técnicas utilizadas para as redes cabeadas. A cada dia que passa essas técnicas são cada vez mais inovadas e aperfeiçoadas para burlar as técnicas de defesas que são desenvolvidas para amenizar os ataques e garantir a segurança desse tipo de rede.

Segundo Carvalho (2005), os intrusos podem comprometer a integridade e confiabilidade dos dados de quatro maneiras:

a) **Interrupção:** esse tipo de ataque faz com que os dados que partem da origem não cheguem ao seu destino. Veja a Figura 12:

Figura 12. Interrupção: Técnica de ataque em redes sem fio
Fonte: Modificado de CARVALHO, J. (2005).

[15] Pessoas que utilizam os seus conhecimentos na exploração e detecção de erros de concepção, dentro da lei.

b) **Intersecção:** neste tipo de ataque, ilustrado na Figura 13, o intruso captura os dados que trafegam na rede de um dispositivo para outro:

Figura 13. Intersecção: Técnica de ataque em redes sem fio.
Fonte: Modificado de CARVALHO, J. (2005).

c) **Modificação:** A Figura 14 demonstra esse tipo de ataque cujo objetivo é capturar os dados que estão sendo enviados da origem, modificando-os e após isso, enviá-los ao seu destino:

Figura 14. Modificação: Técnica de ataque em redes sem fio.
Fonte: Modificado de CARVALHO, J. (2005).

d) **Fabricação:** Nesta técnica, ilustrada na Figura 15, o intruso cria os dados e como se fosse a origem da mensagem envia-os ao dispositivo destino:

Figura 15. Fabricação: Técnica de ataque em redes sem fio
Fonte: Modificado de CARVALHO, J. (2005).

Esses tipos de ataques, como mapeamento, captura de pacotes, entre outros, são realizados com o auxílio de ferramentas especiais. No capítulo seguinte serão apresentadas algumas dessas ferramentas.

7.2 FERRAMENTAS DE ATAQUE PARA REDES SEM FIO

Com o surgimento de falhas na segurança das redes sem fio em geral, nascem as ferramentas para ataques, ou simplesmente, para monitoramento de redes. Na comunicação por *bluetooth* existem ataques específicos e, conseqüentemente, ferramentas que são utilizadas tanto para fazer o mal quanto para fazer o bem. Segundo Kovacs e Monteiro (2005), esses ataques específicos são conhecidos como:

a) **bluejacking:** são ataques que têm como objetivo enviar mensagens *spam* para dispositivos que estiverem no alcance do sinal *bluetooth*. Essa

técnica surgiu com uma brincadeira: um usuário, ao identificar um aparelho ativo ao seu redor, resolveu enviar uma mensagem que dizia “Compre Ericsson”. Essa brincadeira tornou-se séria e foi adotada por empresas de marketing que lhe deram o nome de *Bluecasting*. Aparelhos especiais disparavam mensagem de propagandas para os dispositivos que estavam passando por perto. Esse tipo de técnica é proibido em alguns países;

b) **bluesnarfing:** este tipo de técnica tem o objetivo de capturar informações como agendas telefônicas, mensagens ou catálogos de endereços dos aparelhos que estiverem ativos no meio do sinal *bluetooth*;

c) **bluetooth sniping:** esta é uma outra técnica que consiste em capturar os sinais dos aparelhos que contenham a tecnologia *bluetooth* em uma distância de um km. Obtendo suas informações, que mais tarde abrirão caminhos para facilitar as ações das técnicas *bluejacking* e *bluesnarfing*;

O primeiro vírus para *bluetooth* foi o *Carib* que, apesar de inofensivo, representava uma revolução e preocupação para os proprietários de aparelhos que continham essa tecnologia. O vírus tinha como objetivo varrer todos os dispositivos *bluetooth* ativos até encontrar algum dispositivo. Depois de encontrar, o vírus encaminha para este dispositivo uma cópia de si. Se o usuário deste dispositivo aceitar a transferência, o vírus *Carib* irá proceder da mesma forma, varrendo e transferindo.

7.2.1 Ethereal

Segundo Carvalho (2005), esta ferramenta é um *sniffer* que utilizada uma biblioteca chamada *libcap*, responsável pela sondagem e captura. Funciona tanto nas redes sem fio quanto nas redes cabeadas, nos sistemas operacionais *Windows* e *Linux*. Essa ferramenta serve para o ataque e para defesa das informações, e sua grande vantagem é a facilidade de incorporar novas funcionalidades.

Segundo Rufino (2005), dentre as ferramentas que fazem uso da biblioteca *libcap*, a ferramenta Ethereal é uma das mais completas. A figura 16 ilustra uma tela da ferramenta:

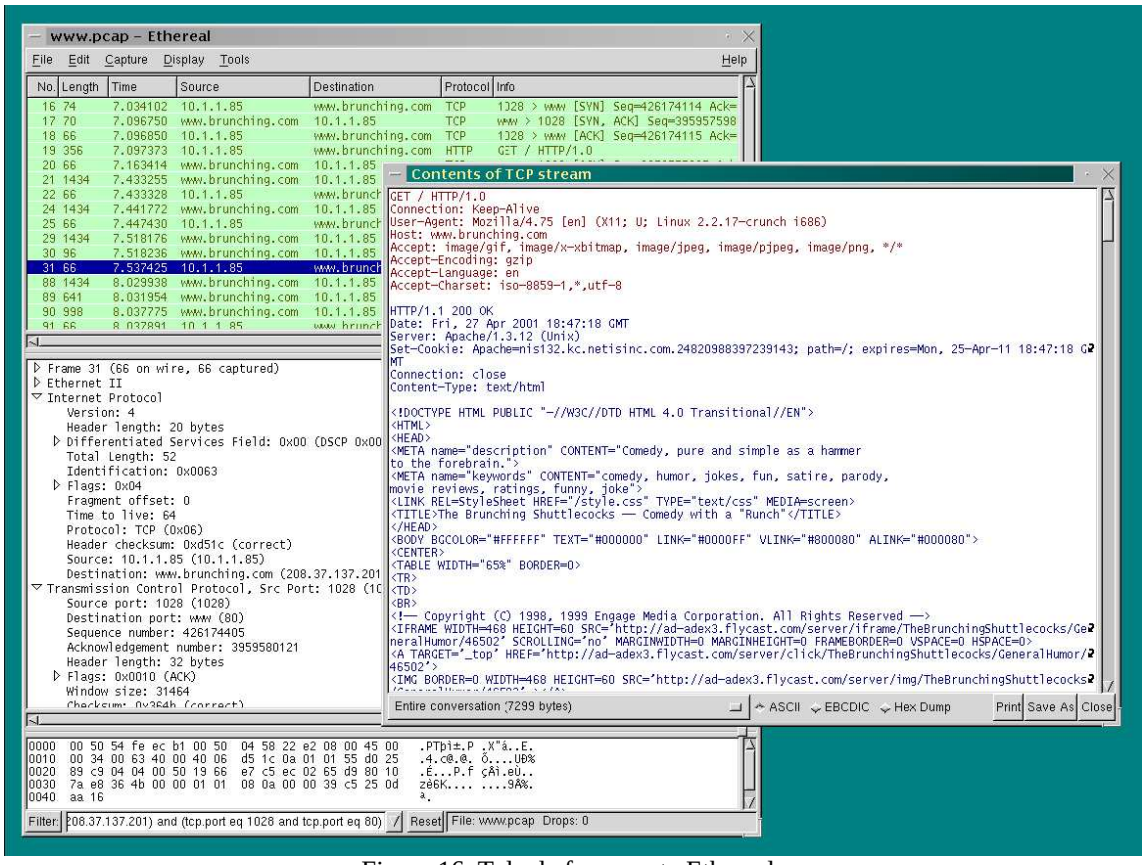


Figura 16. Tela da ferramenta Ethereal.
Fonte: CARVALHO, J. (2005).

7.2.2 NetStumbler

É um software que funciona somente no sistema operacional *Windows*, e serve como *scanner*[16] para redes sem fio, ou seja, uma ferramenta para mapeamento e identificação de redes sem fio, servindo tanto para ações maliciosas quanto para gerenciamento de redes.

Segundo Rufino (2005), a ferramenta NetStumbler leva uma grande desvantagem com relação às outras ferramentas de controle de redes sem fio:

a) Não possui métodos que fazem a quebra de chaves WEP;

b) Incapaz de capturar tráfego.

A grande vantagem dessa ferramenta é a integração com dispositivos GPS[17], a identificação e localização de pontos de redes e a possibilidade de continuar uma análise salva anteriormente.

[16] Análise feita por ferramentas especiais para testar vulnerabilidades em redes.
[17] Sistema de posicionamento por satélite, utilizado para determinar a posição de um receptor na superfície da terra ou em órbita.

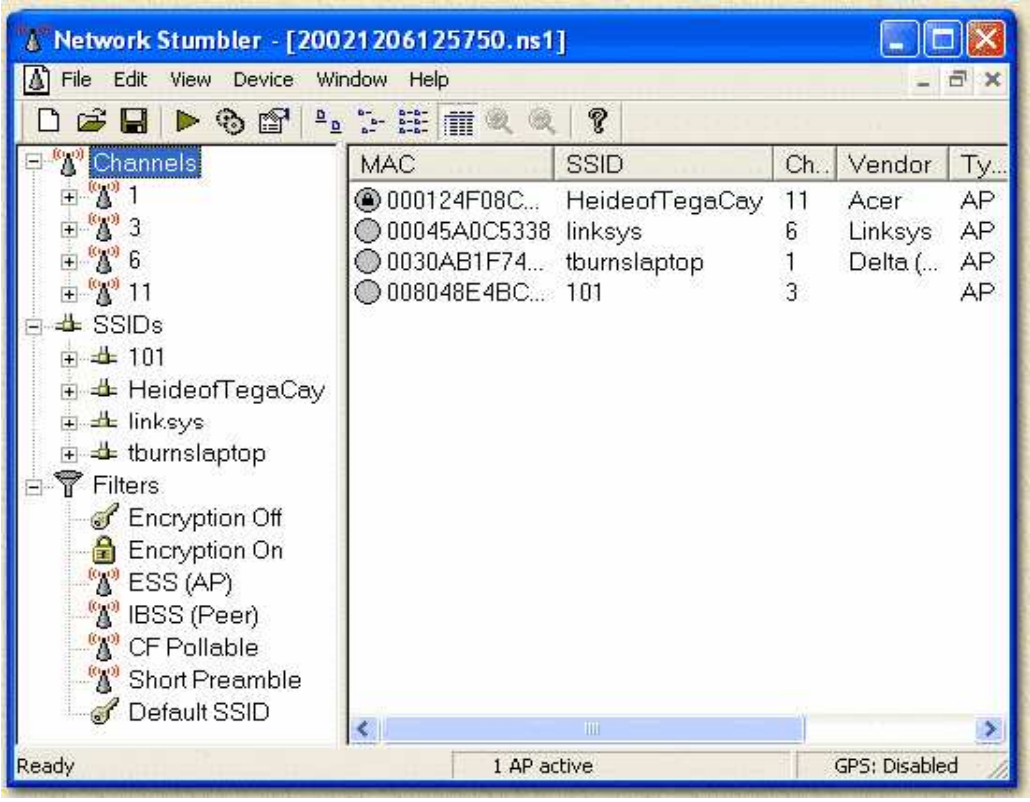


Figura 17. Tela da ferramenta NetStumbler.
Fonte: CARVALHO, J. (2005).

7.2.3 Bloover

Até o momento, foi visto ferramentas que analisam os tráfegos e capturam informações das redes sem fio. Nenhuma delas, porém, é direcionada para a tecnologia *bluetooth*, já que a mesma está exposta aos mesmos riscos do que as outras redes sem fio existentes: captura de sinais, ataques de negação de serviço, identificação dos equipamentos, ente outros.

A ferramenta apresentada neste capítulo, conforme Rufino (2005), é uma união das palavras *bluetooth* + *hoover* que foi desenvolvida na linguagem Java. Essa aplicação permite ser executada tanto em computadores convencionais quanto em celulares que suportam a tecnologia Java. A *bloover* tem o objetivo de identificar e testar as vulnerabilidades da rede *bluetooth*, conforme ilustra a Figura 18.

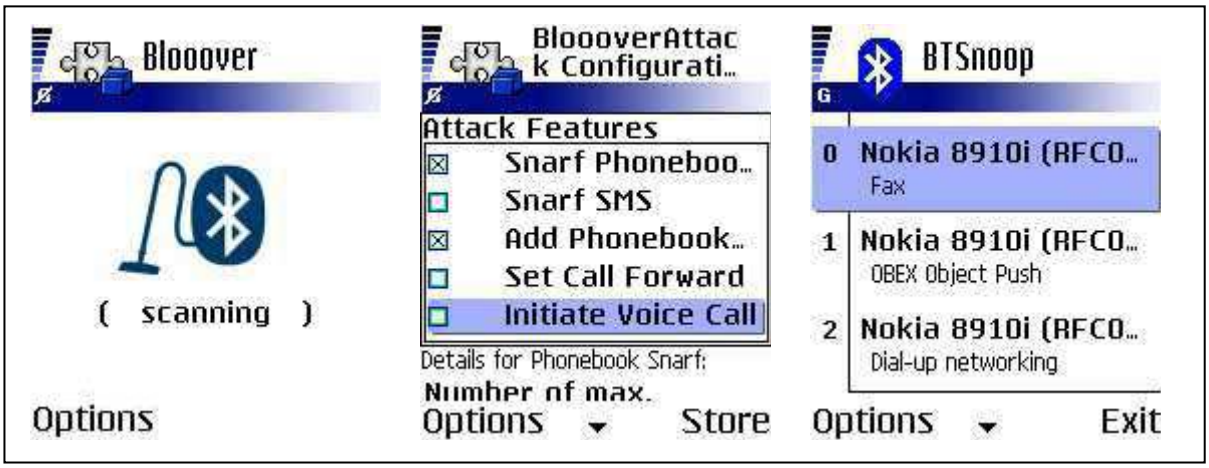


Figura 18. Tela de varredura da ferramenta bloover.
Fonte: RUFINO, N. (2005).

Essa ferramenta permite testar, também, as vulnerabilidades do *bluetooth* já citadas neste trabalho. Exemplos destes testes são as capturas de agendas telefônicas, ligações usando o dispositivo atacado, redirecionamento de chamadas telefônicas o envio de cópias de arquivos por *SMS*[18] (RUFINO, 2005).

> Apesar de programas como o *bloover*, as ferramentas atuais são ainda pouco intrusivas, em geral obtêm informações disponíveis sem necessidade de autenticação ou estabelecimento de comunicação efetiva com o dispositivo investigado, mas nada garante que esta situação perdure, principalmente se esta tecnologia passar a ser muito disseminada (RUFINO, 2005, p.201).

Esses testes citados anteriormente também podem ser feitos através de comandos nativos dos próprios sistemas operacionais como Linux e Windows. A Figura 19 apresenta testes feitos com a utilização do sistema operacional Linux, com um dispositivo *bluetooth* USB para a comunicação e o pacote Qualcomm BlueZ.

```
# hcitool scan
Scanning …
   00:60:57:DF:D1:28  Nokia  6600
```

Figura 19. Comando linux para varrer todos dispositivos ativos
Fonte: RUFINO, N. (2005).

[18] Serviço de Mensagem Curta, serviço disponível em telefones celulares, Palm, Handheld entre outros, que permite o envio de mensagens curtas entre estes dispositivos.

Assim como a ferramenta *Bloover*, existem outras que possuem características semelhantes, tais como: ferramenta *BtScanner*, projetada para extrair o máximo de informações de um dispositivo *bluetooth*; ferramentas *RedFang*, *BlueSniff*, entre outras. Todas as ferramentas citadas são voltadas para os ataques a redes *bluetooth*.

8 TRABALHO DESENVOLVIDO

A pesquisa desenvolvida simula uma transmissão de dados entre ambientes móveis através da tecnologia de comunicação *bluetooth*, visto que esta tecnologia possui falhas de segurança em seu desenvolvimento nativo, foi agregado junto a esta pesquisa métodos de segurança para tornar este tipo de transmissão de dados segura e confiável.

Nesse trabalho foi desenvolvido um protótipo de software que retrata o funcionamento de um prontuário eletrônico, funcionando como cliente-servidor onde o cliente será executado em um celular com a tecnologia *bluetooth* com o objetivo de cadastrar as informações dos pacientes nos seus leitos hospitalares, A Figura 20 apresenta a tela de prontuário eletrônico onde são informados os dados do paciente.

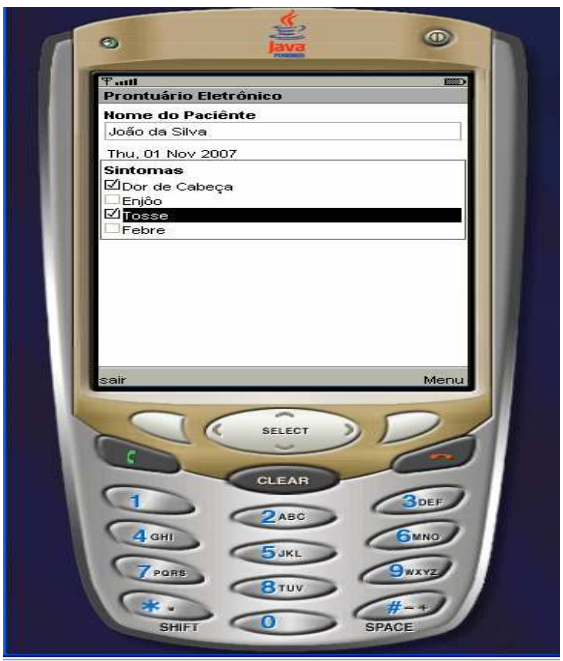


Figura 20. Tela do Prontuário Eletrônico

Após obter esses dados, o cliente encontrará o servidor por meio de uma pesquisa *inquiry scan* que lhe retornará todos os dispositivos *bluetooth* ativos que estão no alcance do sinal (Figura 21). Após localizar o servidor, os dados serão enviados e assim que o servidor recebê-los, irá armazená-los em um banco de dados, este processo pode ser melhor visualizado nos Apêndices B, C e D, onde A esta representando o diagrama de entidade relacional (ER) do banco de dados utilizado, B ilustra o processo do servidor aguardando a conexão do cliente e o Apêndice D, representando a autenticação do cliente pelo servidor, o processo de decriptação dos dados enviados pelo cliente e por fim o armazenamento das informações no banco de dados.

Figura 21. Tela de busca por dispositivos ativos

Nesse software foram aplicadas duas formas de segurança. Uma delas no cliente conforme ilustrado na Figura 22 onde o usuário para acessar a aplicação, terá que se identificar por meio de um login e senha, cadastrados previamente no próprio software.

Figura 22. Tela de login do cliente.

Outra forma de obter segurança nessa aplicação será no momento em que o cliente enviar os dados coletados para o servidor, que contará com uma criptografia conhecida somente pelo servidor.

Para desenvolver essa pesquisa foi utilizada uma biblioteca chamada *Bluecove* que fornece toda pilha de protocolo necessária para manipulação da tecnologia *bluetooth*, esta biblioteca é a responsável pela comunicação da aplicação desenvolvida com as API's do sistema operacional. Esta biblioteca também fornece suporte a métodos de segurança tais como autenticação e criptografia, onde tais seguranças foram utilizadas para prover a garantia da segurança na comunicação entre dispositivos móveis. A Figura 23 ilustra a tela de autenticação dos dispositivos quando o cliente selecionar o servidor para o envio dos dados, é importante salientar que a tela apresentada a seguir difere das demais, pois para identificar esse processo de autenticação, é preciso que a aplicação em si esteja executando em um dispositivo que contenha os serviços requeridos, serviços esses que não estão disponíveis no emulador utilizado.

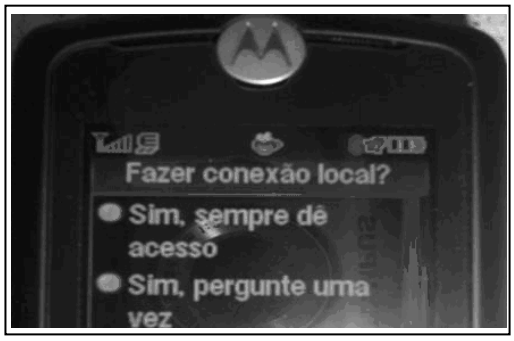


Figura 23. Processo de autenticação dos dispositivos.

Foram usados nessa pesquisa pacotes específicos para manipulação dos métodos da ferramenta Java para realizar a pesquisa por serviços, por dispositivos ativos, objeto para o estabelecimento de conexão, inicialização da pilha de protocolo do *bluetooth*, processo de autenticação e espera por pedido de serviço por parte do cliente e envio e recebimento das informações. A Figura 23 lista os principais pacotes utilizados.

```
import javax.bluetooth.BluetoothStateException;
import javax.bluetooth.DataElement;
import javax.bluetooth.DeviceClass;
import javax.bluetooth.DiscoveryAgent;
import javax.bluetooth.DiscoveryListener;
import javax.bluetooth.LocalDevice;
import javax.bluetooth.RemoteDevice;
import javax.bluetooth.ServiceRecord;
import javax.bluetooth.UUID;
```

Figura 24. Pacotes para manipulação dos métodos *bluetooth*.

Os principais métodos utilizados nesta pesquisa prática foram:

a) **deviceDiscovered:** cada vez que é encontrado um dispositivo é chamado este método, que faz a busca por serviços disponíveis para cada dispositivo e retorna uma variável do tipo RemoteDevice;

b) **servicesDiscovered:** É executado quando é encontrado um serviço, para identificar os tipos de serviços, onde o mesmo detém referências dos serviços encontrados;

c) **serviceSearchCompleted:** método chamado quando um serviço é concluído ou uma pesquisa é encerrado por causa de um erro.

d) **inquiryCompleted:** quando a busca por dispositivo é concluída o método serviceSearchCompleted é executado, onde é passado um parâmetro do tipo inteiro para identificar o motivo da finalização;

O acesso e transmissão dos dados do cliente para o servidor foram realizados pelo comando que são ilustrados na Figura 25.

```
/*************************************************
 *        IMPLENTA O ENVIO DA MENSAGEM           *
 *************************************************/

public void EnviaDados(String sDados){
    Form form2 = new Form("Enviando dados para o servidor");
    Display.getDisplay(this).setCurrent(form2);
    form2.append("Localizando Servidor ...");
    try{
        //--> Configurar a ligação Bluetooth:
        LocalDevice local = LocalDevice.getLocalDevice();
        DiscoveryAgent agent = local.getDiscoveryAgent();
        String connString = agent.selectService(new UUID("1020304060704A1B1C1DE100", false),
                                                ServiceRecord.NOAUTHENTICATE_NOENCRYPT, false);
        System.out.println(connString);
        //-->
        if(connString != null){
            try {
                conexao = (StreamConnection)Connector.open(connString);
            } catch (IOException e1) {
                 e1.printStackTrace();
            }
            //-->
            try {
                byte buffer[] = new byte[100];
                //-->
                DataOutputStream os = conexao.openDataOutputStream();
                //--> Envia dados para o servidor
                os.writeUTF(sDados);
                //-->
```

Figura 25. Código fonte do envio dos dados para o servidor.

Na Figura 25 pode ser observado que o método NOAUTHENTICATE_NOENCRYPT, foi utilizado, o que significa que o envio da mensagem esta sendo feita sem o uso de autenticação e sem o uso da criptografia, isso quer dizer que esta comunicação entre cliente e servidor está vulnerável a ataques, foi neste momento que foi utilizado para testar essas vulnerabilidades a ferramenta ilustrada no Apêndice E, onde durante a transmissão de dados entre o cliente e o servidor, essa ferramenta realizou uma varredura dos pacotes que estavam trafegando na rede, simulando um ataque à rede *bluetooth*, onde resultou na captura dos dados transmitidos. Outro método que foi utilizado foi o AUTHENTICATE_ENCRYPT que conta com a presença da criptografia e autenticação nessa transmissão, onde durante a simulação de ataque pela ferramenta de captura, esses dados também puderam ser capturados, porém com a presença da criptografia, essas informações ficaram embaralhadas não conseguindo então identifica-la, resultando em uma transmissão de dados confiável e segura.

A metodologia deste trabalho foi dada através de pesquisas por meio de livros, artigos, monografias, workshop, fóruns e *sites* nacionais e internacionais dado que este assunto abordado neste trabalho ainda não está muito disseminado no Brasil, e soluções de problemas práticos ainda são difíceis de encontrar em bibliografia da língua portuguesa.

Todos os aplicativos, código fonte e outras ferramentas que foram utilizadas no desenvolvimento deste projeto estão presentes no CD-ROM que o acompanha.

8.1 FERRAMENTAS E PERIFÉRICOS UTILIZADOS

Para o desenvolvimento deste trabalho prático foram utilizadas várias ferramentas para fazer as integrações do ambiente móvel com o ambiente fixo. A linguagem de programação escolhida foi o Java, tanto para o desenvolvimento do servidor (J2SE), quanto para o cliente (J2ME), com a ferramenta de programação IDE NetBeans versão 5.5.

Para o desenvolvimento do cliente foram necessárias as seguintes ferramentas e periféricos:

1) linguagem de programação Java (J2ME);
2) wireless Toolkit versão2.5 para fazer o gerenciamento do projeto;
3) celular com tecnologia *bluetooth* com suporte a aplicações Java e implementação da API JSR-82;

Para o desenvolvimento do servidor foi utilizado:

1) linguagem de programação Java (J2SE);
2) biblioteca *BlueCove* que implementa a pilha de protocolos do *bluetooth* e fornece funções para a manipulação da mesma;
3) dongle (dispositivo *bluetooth* USB) para permitir que um desktop possa ter o sinal *bluetooth*;
4) banco de dados Oracle XE;

Todos os materiais e fontes das quais foram obtidas as ferramentas utilizadas neste trabalho se encontram nas referências complementares.

8.2 RESULTADOS OBTIDOS

Após o conhecimento obtido por meio da realização das pesquisas científicas e práticas se chegou a um resultado com relação a segurança na transmissão de dados por meio da tecnologia *bluetooth.* Identificou-se que a grande parte desses problemas é devido a implementação nativa da tecnologia, tais como a composição de apenas quatro dígitos da senha de proteção do *bluetooth*, endereço MAC dos dispositivos não dispõe de criptografia bem como a despadronização, ou seja, os fabricantes tem a autonomia para definir diversos procedimentos relacionados à criptografia e autenticação. Esses problemas entre outros citados ao logo do trabalho ajudam a ilustrar o quadro da segurança do *bluetooth*, onde segundo Menegatti, citado por Ayres (2007), o *bluetooth* é responsável por 70% dos ataques em ambientes móveis.

Foi observado também que mesmo com a fragilidade e vulnerabilidade da tecnologia *bluetooth*, a mesma unida de técnicas de segurança externa possibilita aos usuários uma segurança das informações que estão sendo transferidas por meio dessa tecnologia.

O ambiente ilustrado nessa pesquisa demonstrou que mesmo com a interceptação de uma ferramenta externa capturando os pacotes de dados que estavam sendo transmitidos do cliente para o servidor, essas informações enviadas pelo cliente continuaram sigilosas e seguras até seu destino. Segurança esta, dada pelo fato da utilização de criptografia dos dados, não possibilitando que mesmo com a captura dos pacotes, as informações enviadas pelo cliente possam ser identificadas, dado que, somente o seu destino terá a chave de acesso para decifrar os dados.

Durante essa pesquisa foram encontradas algumas dificuldades com relação a configuração e compatibilidade das bibliotecas utilizadas. Uma delas foi a incompatibilidade da biblioteca *Bluecove* com o software *BlueSoliu* que acompanha

todos os dispositivos *bluetooth* USB da marca GoldShip, essa incompatibilidade é dada pelo fato do software *BlueSoliu* não suportar todos os serviços que a biblioteca *Bluecove* necessita para a realização da pesquisa desenvolvida. No entanto depois de muitos testes, o software que possibilitou essa comunicação e que oferecia suporte a todos os serviços necessários foi o *WIDCOMM*, permitindo assim a conclusão da implementação prática.

Pôde ser observado e comprovado por meio da implementação prática que de acordo com o objetivo da tecnologia estuda, ou seja, a facilidade de conectar dois ou mais dispositivos, que essa tecnologia é relativamente simples de ser manipulada e de estabelecer uma conexão entre dispositivos. Conseqüentemente essa simplicidade em sua arquitetura tráz também algumas vulnerabilidades que durante essa pesquisa foram sanadas por meio de uma implementação utilizando métodos de segurança, tais como a autenticação e a criptografia.

CONCLUSÃO

Esta pesquisa demonstrou os principais perigos existentes na transmissão de dados por *bluetooth*, que colocam em risco a segurança da informação podendo desencadear uma série de problemas.

O *bluetooth* foi criado, inicialmente, para substituir cabos e para reduzir a complexidade de conectar dois ou mais dispositivos, no entanto, nos tempos atuais o *bluetooth* esta sendo utilizado em um âmbito muito maior, aumentando ainda mais a necessidade de prover segurança nessa tecnologia.

O estudo das principais ameaças e técnicas de invasão na comunicação por *bluetooth* tais como *bluejacking, bluesnarfing, bluetooth sniping*, bem como as formas de acesso a conexão e transmissão de dados, foram fundamentais para mostrar a necessidade de obter segurança nesse tipo de tecnologia, e essencial para sugerir uma estrutura de segurança com os métodos adequados para suprir essa vulnerabilidade que a tecnologia *bluetooth* possui. Essa estrutura foi sugerida através da implentação prática de um software simulando um prontuário eletrônico, onde nesse software foram aplicadas técnicas de criptografia e autenticação para garantir tal segurança na transmissão de dados por *bluetooth.*

O presente trabalho abre portas para trabalhos futuros relacionados a mesma área de estudo que foi direcionada essa pesquisa, sugiro que seja feito um estudo da segurança do *bluetooth*, tomando como exemplo esse trabalho e que fosse sugeridas mudanças no padrão da tecnologia *bluetooth*, já existem trabalhos correlatos a essa pesquisa futura sugerida.

Por fim, pode-se concluir que mesmo com o surgimento de técnicas de ataques direcionadas a tecnologia *bluetooth* que possam por em risco a integridade e

confidencialidade da informação, a utilização da tecnologia *bluetooth* aliada à técnicas e métodos de segurança, pode-se minimizar senão sanar essa vulnerabilidade, garantindo assim uma transmissão de dados segura e confiável.

REFERÊNCIAS

AYRES, Marcelo. **Segurança é a preocupação constante para quem utiliza a tecnologia bluetooth**, Disponível em: <http://tecnologia.uol.com.br/produtos/ultnot/2007/08/06/ult2880u393.jhtm>. Acesso em: Nov. 2007.

BALPARDA, Daniel. **Segurança de dados com criptografia Métodos e Algoritmos**. 3.ed. Rio de Janeiro: Book Express, 2001.

BILLO, Eduardo. **Uma pilha de protocolos Bluetooth adaptáveis à aplicação**. Trabalho de Conclusão de Curso de Ciência da Computação – UFSC. Florianópolis, 2003.

BORGES, R. **Segurança de informações médicas em prontuário eletrônico utilizando Assinatura Digital**. Trabalho de Conclusão de Curso de Ciência da Computação – UNESC. Criciúma, 2004.

BUCHMANN, Johannes. **Introdução à Criptografia**. São Paulo: Berkeley, 2002.

CAMPOS, César. **Controle de Sistemas via Bluetooth**. Trabalho de Conclusão de Curso de Curso de Ciência da Computação – Faculdade de Engenharia de Sorocaba. São Paulo, 2005.

CARVALHO, C. **Análise de desempenho do tráfico de dados assíncrono sobre bluetooth**. Trabalho de Conclusão de Curso de Ciência da Computação - Universidade Estadual do Piauí. Piauí, 2003.

CARVALHO, João; **Um Estudo de protocolos empregados na segurança de dados em redes sem fio**, Trabalho de Conclusão de Curso - UNIPE (Centro Universitário de João Pessoa). João Pessoa, 2005.

CAVALCANTE, A. **Teoria dos Números e Criptografia**. Trabalho de Conclusão de Curso de Ciência da Computação - União Pioneira da Integração Social. Brasília, 2004.

CRONKHITE, Cathy; MCCULLOUGH, Jack. **Hackers acesso negado.** Rio de Janeiro: Campus, 2001.

CUNHA, Rafael. **Assinatura Digital**. Instituto Tecnológico de Aeronáutica, 2000.
DIAS, Kelvin; SADOK, Djamel. **Internet Móvel: Tecnologias Aplicações e QoS**, Trabalho de Conclusão de Curso de Curso de Ciência da Computação – Universidade Federal de Pernambuco. Pernambuco, 2001.

FORTES, D. Redes Ad-Hoc. **Revista Info** São Paulo, 12 Dez. 2005. p. 13.

GASPARETO, Eduardo; **Sistemas de Arquivos criptografados**, Trabalho de Conclusão de Curso de Ciência da Computação; UFLA; Minas Gerais, 2005.

GEHRMANN, C., Persson, J. E Smeets B. **Bluetooth Security**. Boston: Artech House. 2004.

GORKI, Starlin; NOVO, Rafael. **Segurança completa contra hackers**. Rio de Janeiro, Book Express, 2000.

GUIMARÃES, B. **Bluetooth**, 2001. 105 f. Trabalho de Conclusão de Curso (Bacharelado), Universidade Católica de Salvador, Salvador, 2001.

HINZ, Marco. **Um estudo descritivo de novos algoritmos de criptografia**. Trabalho de Conclusão de Curso de Ciência da Computação - Universidade Federal de Pelotas. Pelotas, 2000.

HP. **Introdução à rede sem fio**. Unidades All-In-One da HP, 2006.

ICPC: **International Classification for Primary Care**. Disponível em: <http://www.wonca.org/working_group/classification/wonca_classification.htm>. Acesso em: Nov. 2007.

ICP-Brasil: **Infra estrutura de chaves públicas**. Disponível em <http://www.icpbrasil.gov.br/>. Acesso em: Nov. 2007.

KOBAYASHI, Carlos. **A tecnologia bluetooth e aplicações**. Trabalho de Conclusão de Curso de Ciência da Computação; USP; São Paulo, 2004.

KOVACS, Bruno; MONTEIRO, Vanessa. **Um Estudo prático das ameaças de segurança em dispositivos portáteis com Móbile**, Trabalho de Conclusão de Curso de Ciência da Computação; PUC; Rio de Janeiro, 2005.

LEE, Valentino; SCHNEIDER, Heather; SCHELL, Robbie. **Aplicações Móveis:** arquitetura, projeto e desenvolvimento. São Paulo: Makron Books, 2005.

LIMA, João. **Um estudo de protocolos empregados na segurança de dados em redes sem fio – Padrao 802.11**. Trabalho de Conclusão de Curso de Curso de Ciência da Computação - UNIPE; João Pessoa, 2005.

MAIA, Roberto. **Bluetooth Promessa de um Nova Tecnologia**. Trabalho de Conclusão de Curso de Curso de Ciência da Computação - UFLA; Minas Gerais, 2004.

MANGANELLI, Elenice Colle; ROMANI, Juliao. **Protocolos de Sincronização de dados em ambientes wirelles:** Um estudo de caso. Trabalho de Conclusão de Curso de Ciência da Computação – UFSC. Florianópolis, 2004.

MATEUS, Geraldo; LOUREIRO, Antonio. **Introdução à computação móvel**. 2004. 84 f. Trabalho de Conclusão de Curso de Ciência da Computação – UFMG. Minas Gerais, 2004.

MILLER, M.; **Descobrindo Bluetooth**. Tradução de Altair Dias Caldas de Moraes e Cláudio Belleza. Dias Rio de Janeiro: Campus, 2001.

OLIVEIRA, José; VENANCIO, Gustavo; POLIZER, Sérgio. **Bluetooth e Tecnologia, no Ambiente de WLAN/WPANs**. Dissertação de Mestrado – USP. São Paulo, 2003.

OLIVEIRA, Junior. **Análise de tráfego de dados em redes bluetooth.** Trabalho de Conclusão de Curso de Ciência da Computação - Universidade Federal de Pernambuco. Pernambuco, 2001.

OLIVEIRA, Ricardo. **Bluetooth e Multimídia**. Centro de Ciências Exatas e Tecnologia, Anais do IV Workshop em tratamento de imagens, UFMG, 2003.

PENA, Ana Carolina; SILVA, Cláudio. **Serviço de localização baseada em comunicação móvel**. Trabalho de Conclusão de Curso Ciência da Computação - Universidade da Amazônia. Amazonas, 2001.

ROSA, Rafael; FALEIROS, Antônio. **Análise do Algoritmo vencedor do AES: RIJNDAEL**. Artigo Instituto tecnológico da Aeronáutica (ITA). São Paulo, 2003.

ROSSO, Dangelo. **Uma abordagem experimental para reintegração de dados replicados**. Trabalho de Conclusão de Curso de Ciência da Computação – UNESC. Criciúma, 2005.

RUFINO, Nelson; **Segurança em redes sem fio.** Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. 2. ed. São Paulo: Novatec, 2005.

SACKS, Anelise. **Sistema de Gerencialmente de redes e processos através de computadores portáveis via bluetooth**. Trabalho de Conclusão de Curso de Ciência da Computação – UFRJ. Rio de Janeiro, 2003.

SANTIN, Altair et al.**Um modelo de autorização baseado em redes de confiança para sistemas distribuidos de larga escala**. Trabalho de Conclusão de Curso de Ciência da Computação. UFSC. Florianópolis, 2000.

SEGURANÇA MÁXIMA: o guia de um *hacker* para proteger seu *site* na *internet* e sua rede. Rio de Janeiro: Ed. Campus, 2000.

SILVA, Igor. **Criptografia e Compreenção dos Dados**. Trabalho de Conclusão de Curso de Curso de Ciência da Computação – Universidade Católica de Salvador, Salvador, 2000.

SENA, Jansen. **Criptografia:** mocinha ou vilã? São Paulo: PC & CIA, 2006.

STALLINGS, W. **Wireless Communications and Networks**, First Edition, 2002, Prentice Hall.

SVERZUT, José. **Redes GSM, GPRS, EDGE E UMTS evolução a caminho da terceira geração [3g]**. São Paulo: Makron Books, 2005.

TOSO, et. Al. **Redes sem fio IEEE 802.11.** Trabalho de Conclusão de Curso de Ciência da Computação – UFLA. Minas Gerais, 2004.

TUDE, Eduardo. **Wireless para conexão de dispositivos a curta distância**, Informações em telecomunicação, TELECO, 2006.

BIBLIOGRAFIA COMPLEMENTAR

ARMKNECHT, F.; **A Linearization Attack on the Bluetooth Key Stream Generator**. Disponível em: <http://www.scholar.google.com>. Acesso em: Nov. 2007.

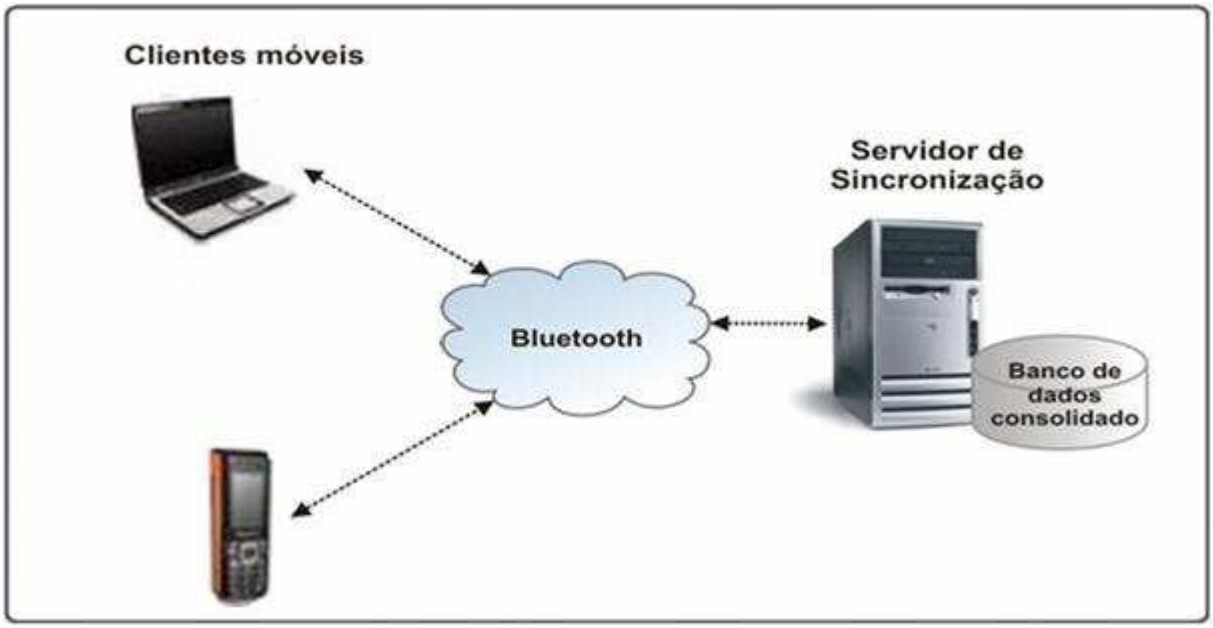
BLS, **Specification of the Bluetooth System Version 1.2**, Disponível em: <www.bluetooth.org>. Acessado em: Out. 2007.

SEGURANÇA MÁXIMA PARA LINUX: o guia de um *hacker* para proteger seu servidor e sua estação de trabalho. Rio de Janeiro: Campus, 2000.

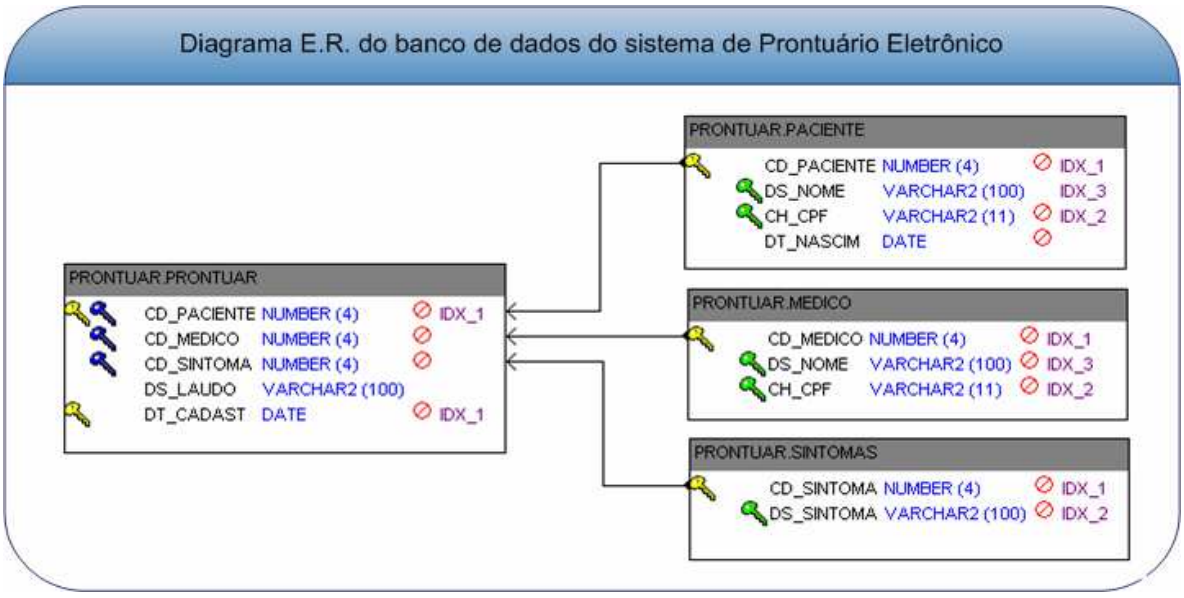
KIM, Hae. **Marca d'água Frágeis de Autenticação para Imagens em Tonalidade Contínua e Esteganografia para Imagens Binárias e Meio-Tom.** Trabalho de Conclusão de Curso (Bacharelado); Universidade de São Paulo. São Paulo, 2003.

APÊNDICE

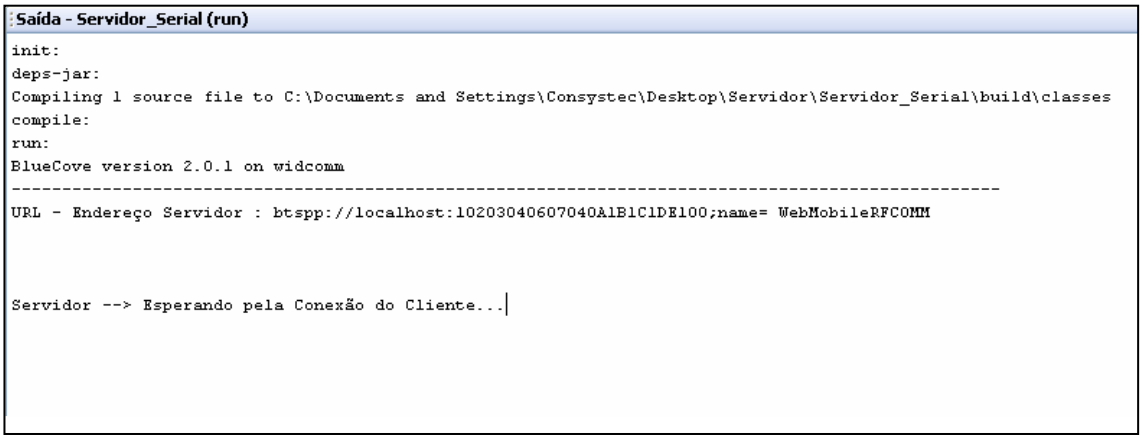
APÊNDICE A - REPRESENTAÇÃO DO AMBIENTE PROPOSTO



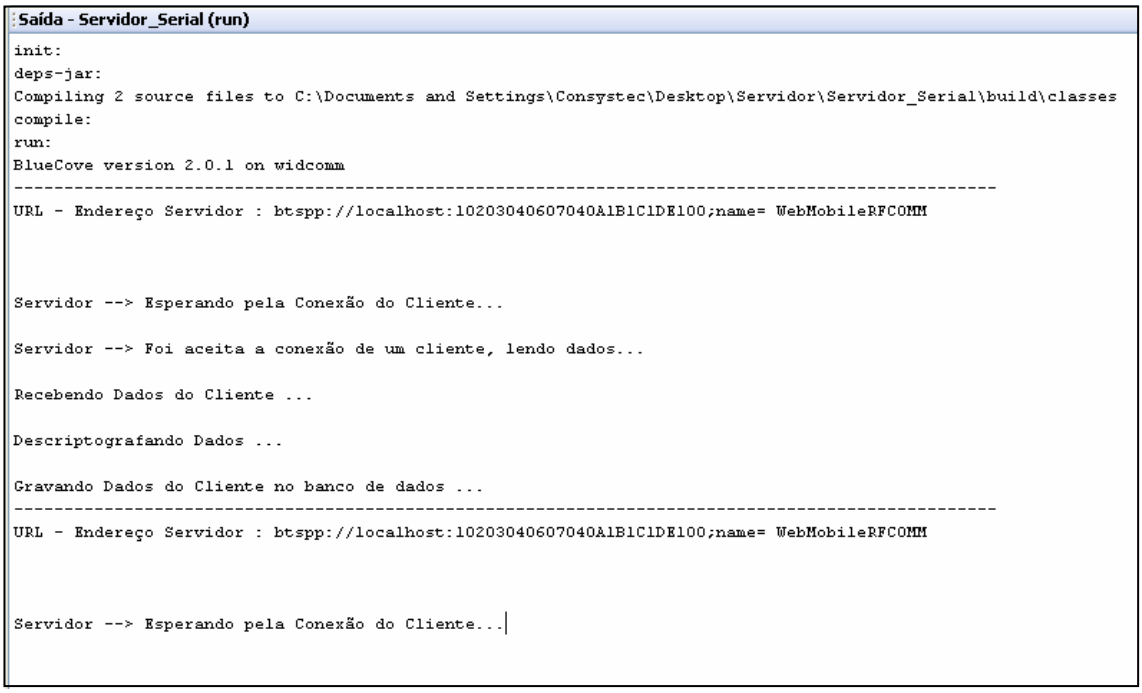
APÊNDICE B - DIAGRAMA E.R DO PROJETO PRONTUÁRIO ELETRÔNICO



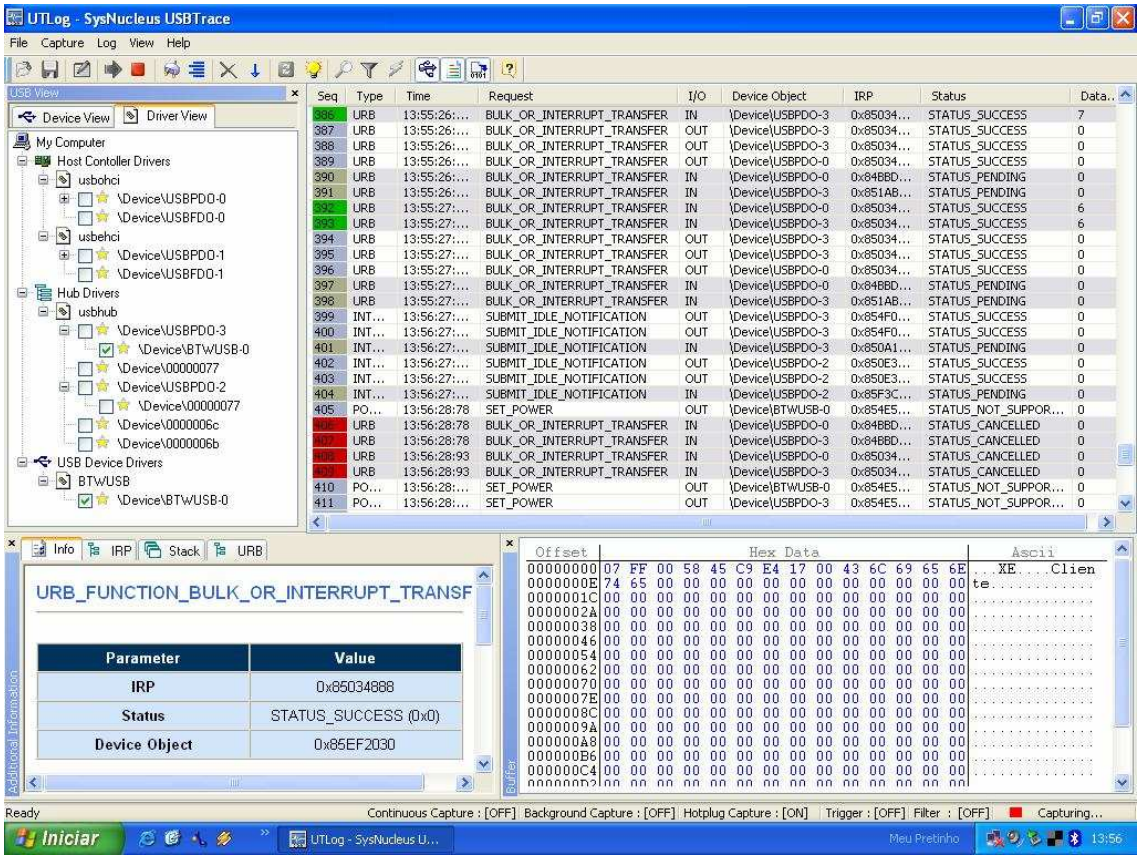
APÊNDICE C - SERVIDOR ESPERANDO POR CONEXÃO DO CLIENTE



APÊNDICE D - PROCESSO DE AUTENTICAÇÃO DO CLIENTE



APÊNDICE E - PROCESSO CAPTURA DOS DADOS



APÊNDICE F - DIAGRAMA DE ATIVIDADE DO SISTEMA DESENVOLDIDO