

Bluetooth – Características, protocolos e funcionamento

Thiago Senador de Siqueira
RA 057642
Instituto de Computação
Universidade Estadual de Campinas
thiagosenador@yahoo.com.br

RESUMO

Bluetooth é um padrão de comunicação sem fio de curto alcance, baixo custo e baixo consumo de energia que utiliza tecnologia de rádio. Sua especificação é aberta e está publicamente disponível. Uma Bluetooth Wireless Personal Area Network (BT-WPAN) consiste de piconets. Cada piconet é um conjunto de até oito dispositivos Bluetooth. Um dispositivo é designado como mestre e os outros como escravos. Através de uma pilha de protocolos bem definida e de um conjunto mínimo de componentes de hardware, dispositivos Bluetooth têm ganhado uma parcela significativa do mercado wireless.

1. INTRODUÇÃO

Bluetooth é uma especificação industrial para Personal Area Networks (PANs), também conhecido como IEEE 802.15.1. Bluetooth provê uma forma de conectar e trocar informações entre dispositivos como PDAs, telefones celulares, laptops, PCs, impressoras, câmeras digitais dentre outros, através de frequência de rádio de curto alcance, segura, de baixo custo e globalmente disponível [1][2][5]. A especificação Bluetooth foi inicialmente projetada com o objetivo de desenvolver dispositivos interconectáveis de baixo consumo de energia, através de frequências de rádio de curto alcance – de 1 a 100 metros, dependendo da categoria do dispositivo.

Se estiverem um ao alcance do outro, dois dispositivos que implementam a especificação Bluetooth podem se comunicar, mesmo se não estiverem na mesma sala, mas, respeitando uma distância máxima de até 100 metros. A transferência de dados e de voz varia em muitos dispositivos Bluetooth dependendo de requisitos como quantidade de energia necessária na transmissão, taxa de transferência e distância [1].

Uma das grandes vantagens da utilização de Bluetooth é a possibilidade de criar PANs de forma ad-hoc, ou seja, um dispositivo que entra ao alcance de outro, automaticamente se conecta e estes constituem uma PAN.

Neste cenário, um dispositivo recebe o papel de mestre, enquanto que os outros recebem o papel de escravo. A este conjunto de mestre e escravos dá-se o nome de piconet. Cada piconet pode ter até 8 dispositivos. Quando duas piconets se conectam, através de um dispositivo em comum, forma-se a chamada scatternet.

Outra característica marcante na especificação Bluetooth é a segurança. Através de mecanismos como frequency hopping, autenticação de códigos PIN (Personal Identification Number) e criptografia de 128 bits garante-se comunicação segura e livre de interferências entre dispositivos Bluetooth [3].

Este trabalho está organizado da seguinte maneira: na seção 2 é apresentada uma visão geral da especificação Bluetooth com funcionalidades e características básicas. Na seção 3 são analisados software e hardware Bluetooth. O mecanismo de comunicação entre dispositivos Bluetooth é apresentado na seção 4. E, finalmente, na seção 5, as conclusões obtidas a respeito da especificação Bluetooth.

2. VISÃO GERAL

Bluetooth é um padrão de comunicação sem fio de curto alcance, baixo custo e baixo consumo de energia que utiliza tecnologia de rádio. Embora tenha sido imaginada como uma tecnologia para substituir cabos pela Ericsson (a maior fabricante de celulares, hoje Sony-Ericsson Corporation) em 1994, Bluetooth tem se tornado largamente utilizado em inúmeros dispositivos e já representa uma parcela significativa do mercado wireless. Dentre os dispositivos que utilizam Bluetooth podemos incluir os dispositivos inteligentes, como PDAs, telefones celulares, PCs,

periféricos, como mouses, teclados, *joysticks*, câmeras digitais, impressoras e dispositivos embarcados, como os utilizados em automóveis (travas elétricas, cd *player*, etc).

O nome *Bluetooth* nasceu no século X com o rei da Dinamarca, rei Harald Bluetooth, que se engajava na diplomacia entre os países da Europa, fazendo com que estes estabelecessem acordos comerciais entre si [3]. Os projetistas de *Bluetooth* adotaram tal nome para sua especificação pelo fato desta permitir que diferentes dispositivos possam se comunicar um com outro.

O projeto da especificação *Bluetooth* começou quando a empresa de celulares Ericsson se juntou a outras empresas como Intel Corporation, International Business Machines Corporation (IBM), Nokia Corporation e Toshiba Corporation para formarem o *Bluetooth Special Interest Group* (SIG) em 1998. Em 1999 outras empresas se juntaram ao SIG como 3Com Corporation, Lucent/Agere Technologies Inc., Microsoft Corporation e Motorola Inc. O trabalho conjunto de todos os membros do SIG permitiu o desenvolvimento da especificação *Bluetooth*, através de padrões abertos para assegurar uma rápida aceitação e compatibilidade com as tecnologias disponíveis no mercado [7]. A especificação resultante, desenvolvida pelo *Bluetooth SIG* é aberta e inteiramente disponível. *Bluetooth* já é adotada por mais de 2100 companhias ao redor do mundo. A tecnologia *Wireless Personal Area Network* (WPAN), baseada na especificação *Bluetooth*, é agora um padrão IEEE sob a denominação 802.15.1 WPANs [4].

A especificação *Bluetooth* define como dispositivos *Bluetooth* são agrupados para propósito de comunicação. Levando em consideração o alcance das ondas de rádio dos dispositivos *Bluetooth*, estes são classificados em três classes:

- Classe 3 – alcance de no máximo 1 metro;
- Classe 2 – alcance de no máximo 10 metros;
- Classe 1 – alcance de no máximo 100 metros.

Uma *Bluetooth Wireless Personal Area Network* (BT-WPAN) consiste de *piconets*. Cada *piconet* é um conjunto de até oito dispositivos *Bluetooth*. Um dispositivo é designado como mestre e os outros como escravos. Duas *piconets* podem se conectar através de um dispositivo *Bluetooth* comum a ambas (um *gateway*, *bridge* ou um dispositivo mestre) para formarem uma *scatternet*. A figura 1 mostra uma

scatternet formada por duas *piconets*. Estas *piconets* interconectadas dentro de uma *scatternet* formam uma infra-estrutura para *Mobile Area Network* (MANET) e podem tornar possível a comunicação de dispositivos não diretamente conectados ou que estão fora de alcance de outro dispositivo.

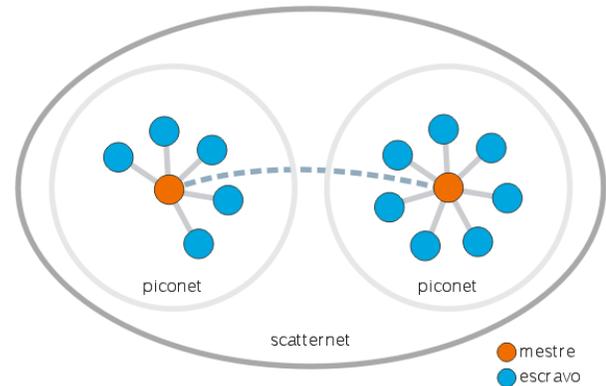


Figura 1 – Uma *scatternet* formada de duas *piconets*

Implementações atuais de dispositivos *Bluetooth* baseiam-se basicamente em conexões ponto-a-ponto. Entretanto, a especificação *Bluetooth* não define apenas soluções ponto-a-ponto como também topologias mais complexas [1]. O objetivo é a formação de *scatternets* que forneçam comunicação efetiva e eficiente através de vários de nós com tempo de resposta aceitável e baixo consumo de energia para o desenvolvimento de aplicações fim-a-fim.

3. ARQUITETURA

A arquitetura *Bluetooth* consiste basicamente de dois componentes: um *transceiver* (hardware) e uma pilha de protocolos (software). Esta arquitetura oferece serviços e funcionalidades básicas que tornam possível a conexão de dispositivos e a troca de uma variedade de tipos de dados entre estes dispositivos.

A frequência utilizada por dispositivos *Bluetooth* opera em uma faixa de rádio não licenciada ISM (*industrial, scientific, medical*) entre 2.4 GHz e 2.485 GHz. O sistema emprega um mecanismo denominado *frequency hopping*, que “salta” constantemente de frequência para combater interferência e enfraquecimento do sinal. A cada segundo são realizados 1600 saltos de frequência. A taxa de transmissão pode alcançar 1 Megabit por segundo (Mbps) ou, com o mecanismo *Enhanced Data Rate*, recentemente introduzido na última especificação *Bluetooth*, a 2 ou 3 Mbps [5][6].

Durante uma operação típica, um canal físico de rádio é compartilhado por um grupo de dispositivos que estão sincronizados a um *clock* comum e a um padrão de saltos de frequência. Um dispositivo provê a sincronização de referência e é chamado de mestre. Todos os outros dispositivos são conhecidos como escravos [1][4][6]. Como mencionado na seção anterior, um grupo de dispositivos sincronizados desta maneira forma uma *piconet*. Esta é a maneira fundamental de comunicação através de *Bluetooth*.

Dispositivos em uma mesma *piconet* utilizam um padrão de saltos de frequência que é algorítmicamente determinado por atributos na especificação *Bluetooth* e pelo *clock* do dispositivo mestre. Este salto de frequência se baseia em um algoritmo pseudo-randômico ordenando 79 frequências, em intervalos de 1 MHz, dentro da faixa ISM. O padrão de salto de frequência pode ser adaptado para excluir a porção de frequências que está sendo utilizada e interferindo os dispositivos. Este mecanismo de *frequency hopping* auxilia na coexistência de dispositivos *Bluetooth* com outros (*non-hopping*) sistemas ISM que se encontram na mesma localização.

O canal físico é sub-dividido em unidades de tempos denominados *slots*. Dados são transmitidos entre dispositivos *Bluetooth* em pacotes que são posicionados nestes *slots* [1][2][6]. Quando as circunstâncias permitem, é possível alocar um número consecutivo de *slots* em um único pacote. O mecanismo de *frequency hopping* entra em cena tanto na emissão quanto na recepção de pacotes. A especificação *Bluetooth* provê o efeito de transmissões *full-duplex* através do uso de esquemas de divisão de tempo (*time division duplex*) [4].

Dentro de um canal físico, um *link* físico é formado entre quaisquer dois dispositivos, e transmitem pacotes em ambas as direções. Em um canal físico de uma *piconet* há restrições sobre qual dispositivo pode formar um *link* físico. Existe um *link* físico entre cada escravo e o mestre. Em uma *piconet*, não há formação de *links* físicos diretamente entre escravos.

3.1 A pilha de protocolos *Bluetooth*

A especificação *Bluetooth* divide a pilha de protocolos em três grupos lógicos. São eles: grupos de protocolos de transporte, grupo de protocolos de *middleware* e o grupo de aplicação [1][4], como ilustrado na figura 2.

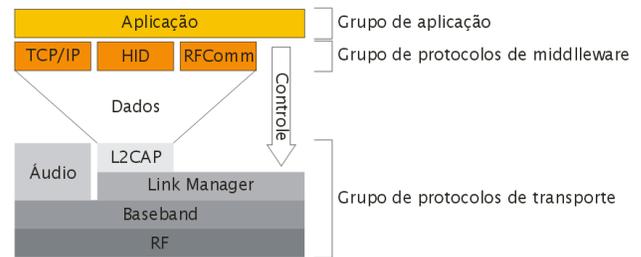


Figura 2 – Pilha de protocolos *Bluetooth*

O grupo de protocolos de transporte permite dispositivos *Bluetooth* localizar outros dispositivos e gerenciar *links* físicos e lógicos para as camadas superiores. Neste contexto, protocolos de transporte não se equivalem aos protocolos da camada de transporte do modelo OSI (utilizado na especificação de protocolos de rede). Ao invés disso, estes protocolos correspondem às camadas físicas e de enlace do modelo OSI. As camadas de rádio frequência (RF), *Baseband*, *Link Manager*, *Logical Link Control and Adaptation* (L2CAP) estão incluídas no grupo de protocolos de transporte. Estes protocolos suportam tanto comunicação síncrona quanto assíncrona e todos estes são indispensáveis para a comunicação entre dispositivos *Bluetooth* [1].

O grupo de protocolos de *middleware* inclui protocolos de terceiros e padrões industriais. Estes protocolos permitem que aplicações já existentes e novas aplicações operem sobre *links Bluetooth*. Protocolos de padrões industriais incluem *Point-to-Point Protocol* (PPP), *Internet Protocol* (IP), *Transmission Control Protocol* (TCP), *Wireless Application Protocol* (WAP), etc. Outros protocolos desenvolvidos pelo próprio SIG também foram incluídos como o RFCOMM, que permite aplicações legadas operarem sobre os protocolos de transporte *Bluetooth*, o protocolo de sinalização e controle de telefonia baseada em pacotes (TCS), para o gerenciamento de operações de telefonia e o *Service Discover Protocol* (SDP) que permite dispositivos obterem informações sobre serviços disponíveis de outros dispositivos [4].

O grupo de aplicação consiste das próprias aplicações que utilizam *links Bluetooth*. Estas podem incluir aplicações legadas ou aplicações orientadas a *Bluetooth*.

Pode-se resumir as características das camadas da pilha de protocolos *Bluetooth* da seguinte maneira [1][5][7]:

- **Camada de Rádio (RF):** a especificação da camada de rádio corresponde essencialmente

ao projeto dos *tranceivers Bluetooth* e será discutida na próxima seção;

- **Camada Baseband:** esta camada define como dispositivos *Bluetooth* localizam e se conectam a outros dispositivos. Os papéis de mestre e escravo são definidos nesta camada, assim como os padrões de saltos de frequência utilizados pelos dispositivos. Mestre e escravos só se comunicam entre si através de *slots* de tempo pré-definidos. É nesta camada também onde se definem os tipos de pacotes, procedimentos de processamento de pacotes, estratégias de detecção de erros, criptografia, transmissão e retransmissão de pacotes. Esta camada suporta dois tipos de *links*: *Synchronous Connection-Oriented* (SCO) e *Asynchronous Connection-Less* (ACL). *Links* SCO são caracterizados pela periódica atribuição de um *slot* de tempo a um dispositivo e é utilizado basicamente na transmissão de voz, que requer transmissões de dados rápidas e consistentes. Um dispositivo que estabeleceu um *link* SCO possui, em essência, determinados *slots* de tempo reservados para seu uso. Seus pacotes são tratados como prioritários e serão processados antes de pacotes ACL. Já um dispositivo que opera sobre um *link* ACL pode enviar pacotes de tamanho variável de 1, 3 ou 5 *slots* de tempo. Entretanto, este tipo de *link* não possui reserva de *slots* de tempo para seus pacotes;
- **Link Manager:** esta camada implementa o *Link Manager Protocol* (LMP), que gerencia as propriedades do meio de transmissão (ar) entre os dispositivos. O protocolo LMP também gerencia a alocação de taxa de transferência de dados, taxa de transferência de áudio, autenticação através de métodos de desafio-resposta, níveis de confiança entre dispositivos, criptografia de dados e controle do gasto de energia;
- **Camada L2CAP:** a camada L2CAP serve de interface entre os protocolos de camadas superiores e os protocolos de transporte de camadas inferiores. Esta camada também é responsável pela fragmentação e remontagem de pacotes.

3.2 Hardware Bluetooth

Todos os dispositivos que implementam a especificação *Bluetooth* devem possuir minimamente seis componentes de hardware [2], como mostra a figura 3. São eles:

- **Host Controller:** responsável pelo processamento de código de alto nível, tanto de aplicações quanto de algumas camadas inferiores da pilha de protocolos *Bluetooth* – controle de link lógico, L2CAP, RFCOMM e outras funcionalidades;
- **Link Control Processor:** um microprocessador responsável pelo processamento das camadas mais baixas da pilha de protocolos como *Link Manager* e *Link Controller*. Em algumas aplicações embarcadas, pode estar combinado com o *Host Controller* em um único chip;
- **Baseband Controller:** bloco lógico responsável pelo controle do *transceiver* de rádio frequência (RF);
- **Transceiver RF:** contém o sintetizador de rádio frequência, filtros Gaussianos, recuperação de *clock* e detector de dados;
- **RF Front-End:** contém o filtro de banda passante da antena, amplificador de ruídos e amplificador de energia. É responsável pela troca de estados – emissor x receptor.
- **Antena:** pode ser interna ou externa e pode estar integrada em componentes de terceiros.

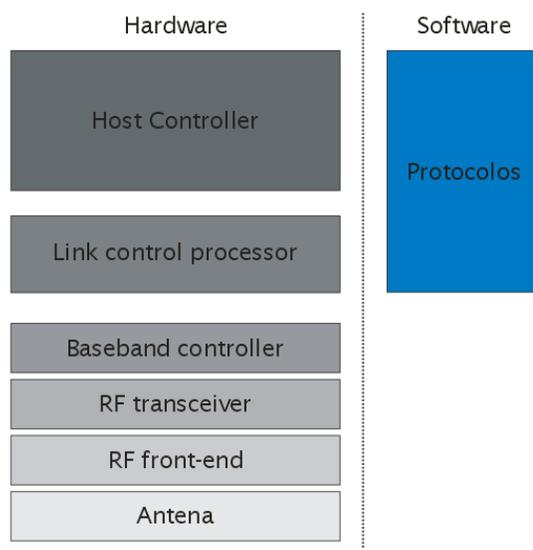


Figura 3 – Diagramas de blocos de hardware e software da especificação Bluetooth.

A maioria dos desenvolvedores de dispositivos *Bluetooth* tem adotado uma abordagem de projeto de multi-chip, utilizando componentes CMOS para o núcleo de gerenciamento de banda e microprocessadores para processamento de rádio frequência (processamento de sinais), como mostra a figura 4. Enquanto esta abordagem ajuda a simplificar o design do chip, algumas desvantagens como o alto número de componentes, espaço de placa inadequado e outras questões de integração podem aumentar os custos de implementação de forma significativa. A implementação típica de um sistema de rádio *Bluetooth* envolve um número de componentes consideravelmente caros, como dispositivos de rádio frequência e filtros de interferência.

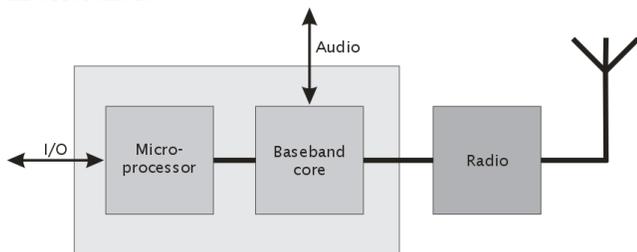


Figura 4 – Abordagem multi-chip de dispositivos *Bluetooth*

Alguns desenvolvedores de dispositivos *Bluetooth*, entretanto, têm adotado uma abordagem diferente da anterior: implementar toda a especificação em um único chip (figura 5). Nesta abordagem, todos os componentes – microprocessador, *baseband* e rádio, são implementados inteiramente em um único componente CMOS. [6] A principal vantagem desta abordagem é a redução de custos na fabricação dos chips.

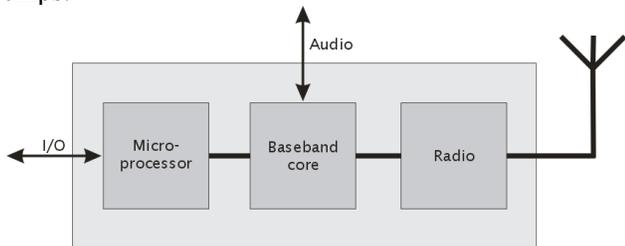


Figura 5 – Abordagem de um único chip

4. O PROCESSO DE COMUNICAÇÃO

Um *transceiver Bluetooth* é um dispositivo que opera em uma faixa de rádio não licenciada (ISM) a 2.4

GHz. Na maioria dos países, há 79 canais disponíveis. Entretanto, alguns países permitem apenas o uso de 23 canais. A taxa de transferência nominal de cada canal é de 1 MHz [1][4].

Quando conectado a outros dispositivos *Bluetooth*, um dispositivo troca de frequência a uma taxa de 1600 vezes por segundo. Cada frequência é utilizada apenas 625 microssegundos [6].

A especificação *Bluetooth* utiliza o esquema de divisão de tempo (*Time Division Duplexing* - TDD) e divisão de tempo com múltiplos acessos (*Time Division Multiple Access* - TDMA) na comunicação de dispositivos. Como discutida na seção anterior, a transmissão de dados é feita através de slots de tempos. Um único *slot* possui 625 microssegundos de comprimento, representando um pacote de dados que ocupa um único *slot*. Na camada de *baseband*, um pacote consiste de um código de acesso, um cabeçalho e *payload*, como mostra a figura 6.



Figura 6 – Estrutura de um pacote de uma *piconet*

O código de acesso contém o endereço da *piconet* (para filtrar mensagens de outra *piconet*) e possui geralmente 72 bits de comprimento. O cabeçalho possui 18 bits e inclui o endereço de um dispositivo escravo ativo na rede *Bluetooth*. O campo *payload* é onde trafega os dados da aplicação. Pode conter de 0 a 2745 bits de dados.

Em uma *piconet*, o mestre transmite em *slots* de tempo pares enquanto que os escravos transmitem apenas em *slots* de tempo ímpares. Em cada *slot* de tempo, devido ao mecanismo *frequency hopping*, um canal de frequência diferente é utilizado, ou seja, após cada envio ou recebimento de pacotes, o canal é trocado, antes mesmo da transmissão do próximo pacote.

Um dispositivo *Bluetooth* pode estar em um dos seguintes estados: espera, solicitação, página, conectado, transmissão, bloqueado, escuta e estacionado [1], como mostra a figura 7. Um dispositivo está no estado de **espera** quando está ligado mas ainda não se juntou a uma *piconet*. Este entra no estado de **solicitação** quando envia requisições de busca de outros dispositivos com os quais possa se conectar. Um dispositivo mestre de uma *piconet* existente pode também estar no estado de **página**, enviando mensagens à procura de dispositivos que possam se juntar e sua *piconet*.

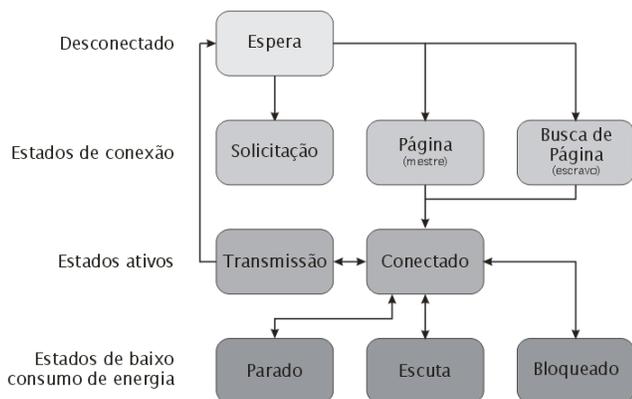


Figura 7 – Diagrama de estados da especificação Bluetooth

Quando uma comunicação é bem sucedida entre mestre e um novo dispositivo, este novo dispositivo assume o papel de escravo e entra no estado de **conectado**, e então recebe um endereço que o identifica na *piconet*. Enquanto conectado, um escravo pode transmitir dados, quando o mestre o permite fazê-lo. Durante a transmissão de seus dados, os escravos estão no estado de **transmissão**. Ao fim de sua transmissão, este retorna ao estado de conectado.

O estado de **escuta** é um estado de baixo consumo de energia onde um escravo “dorme” por um número pré-definido de *slots*. O dispositivo então acorda para realizar a transmissão de dados em seu slot de tempo apropriado. Após a transmissão o dispositivo escravo retorna então para o estado de escuta até que seus próximos *slots* de tempo designados cheguem. O estado de **bloqueado** é outro estado onde se verifica o baixo consumo de energia, em que o escravo não está ativo por um período pré-determinado de tempo. Entretanto, não há transferência de dados dentro do estado bloqueado.

Quando um dispositivo escravo não tem dados a serem enviados ou recebidos, o dispositivo mestre pode instruí-lo a entrar no estado de **estacionado**. Quando no estado de estacionado, o dispositivo escravo perde seu endereço atual na *piconet*, o qual será dado a outro escravo que o mestre está retirando do estado de estacionado.

5. CONCLUSÕES

A tecnologia sem fio *Bluetooth* aborda vários pontos-chaves que facilitam sua vasta adoção: 1) é uma especificação aberta e que está publicamente disponível; 2) sua tecnologia sem fio de curto alcance

permite dispositivos periféricos comunicarem entre si através de uma interface simples, o ar, ao contrário das tecnologias de cabos, que utilizam conectores de uma grande variedade de formas, tamanhos e números de pinos; 3) a especificação *Bluetooth* suporta transferências tanto de voz quanto de dados, tornando-se uma tecnologia ideal na comunicação de dispositivos heterogêneos; e 4) *Bluetooth* utiliza uma faixa de frequências não regulamentada e vastamente disponível em qualquer lugar do mundo.

Referências

- [1] McDermott-Wells, P. Bluetooth Overview. *IEEE Potentials Magazine*. December 2004, pp.33-35.
- [2] Johnson, D. Hardware and software implications of creating Bluetooth Scatternet devices. In: *Proceedings of the IEEE AFRICON*. 2004, pp. 211-215.
- [3] Wikipedia. Bluetooth. Disponível em <www.wikipedia.com/eng/bluetooth>. Último acesso em 12 de junho de 2006.
- [4] Bluetooth SIG. Specification of the Bluetooth System. Disponível em <www.bluetooth.com>. Último acesso em 15 de junho de 2006.
- [5] Chomienne, D. Eftimakis, M. Bluetooth Tutorial. Disponível em <www.newlogic.com/products/Bluetooth-Tutorial-2001.pdf>. Último acesso em 15 de junho de 2006.
- [6] Kardach, J. Bluetooth Architecture Overview. *Intel Technology Journal*. 2000.
- [7] Miller, B. A. Bisdikian, C. Bluetooth Revealed. *Upper Saddle River*. Prentice Hall, 2001.