**BLUETOOTH**

**Juliano Sanches Maia,** **julianosam@gmail.com**

**Letícia Pizzato Conte,** **leleconte@gmail.com**

**Porto Alegre, outubro de 2008**

**Resumo**

Vamos abordar neste trabalho os aspectos gerais de uma tecnologia nova conhecida como Bluetooth. Falaremos sobre sua origem, arquitetura, conexão e segurança, além das versões que já estão disponíveis no mercado.

**I. INTRODUÇÃO**

Rei da Noruega e da Dinamarca, Harold Bluetooth, foi quem deu origem ao nome desta tecnologia. Ele ficou conhecido por unificar as tribos norueguesas, dinamarquesas e suecas.

O protocolo do Bluetooth, da mesma forma, veio para unir tecnologias móveis como celulares, headsets, computadores,...

Começando a ser desenvolvida em 1994, pela empresa Ericsson que buscava encontrar uma tecnologia de transmissão de dados de baixo custo entre telefones celulares e seus acessórios.

Em 1998, uniram-se a ela, empresas como Nokia, IBM e Toshiba, fundando assim o Bluetooth Special Interest Group – SIG, uma vez que tinham como objetivo expandir o Bluetooth e assim, estabelecê-lo como grande padrão industrial.

O grupo cresceu rapidamente, hoje conta com mais de duas mil empresas, entre elas de telecomunicação, eletrodomésticos e computação, que estão interessadas em desenvolver produtos que façam parte desta especificação.

Foi o trabalho de todas as empresas que fazem parte do SIG que permitiu o desenvolvimento do Bluetooth, juntamente com padrões abertos, que asseguraram uma rapida aceitação e compatibilidade com o mercado.

O Bluetooth é uma tecnologia sem fio que permite a transmissão de dados por ondas de rádio de curto alcance, baixo custo, seguro e que seja universal. Os dispositivos podem ser divididos em três classes conforme o alcance e a potência: 100mW com até 100 metros de alcance; 2,5mW com até 10 metros de alcance; 1mW com até 1 metro de alcance.

**II. ARQUITETURA**

Com a criação desta tecnologia, tornou-se necessário a adoção de uma frequência de rádio que fosse aberta, tendo em vista o baixo custo de utilização. Ele segue os padrões da faixa ISM (Industrial, Scientific, Medical) que opera em frequências que variam de 2,4 a 2,485 GHz.

Como este padrão pode ser utilizado por muitos sistemas de comunicação, as transmissões entre os dispositivos conectados podem tanto gerar interferências, como sofrê-las.

No intuito de amenizar este problema, o Bluetooth implementa um método chamado *Frequency Hopping*, o qual permite que a frequência utilizada para estabelecer a conexão entre os dispositivos seja dividida em diferentes canais (79 canais na América do Norte/Europa e 23 no Japão). O dispositivo que estabelece a conexão alterna entre estes canais rapidamente, diminuindo a chance de intereferências.

Além disto, o Bluetooth implementa transmissões *full-duplex* através de **divisão de tempo** (FH-TDD – *Frequency Hopping Time Division Duplex*). Este modelo de transmissão permite que um dispositivo envie e receba pacotes de dados alternando a transmissão entre dois slots: um para transmissão e outro para recebimento de dados. Cada slot é divido em períodos de 625µs, de forma que, a cada alternância de frequência ocorra a transmissão de um slot de dados.

 A arquitetura desta tecnologia, conforme o SIG, está dividida em dois grupos: o **core** (núcleo) e os **profiles** (perfis). O **core** define o funcionamento geral do sistema (protocolos, camadas, especificações). Já os diferentes **perfis** determinam como os elementos que compõe o sistema devem funcionar para que a função desejada seja realizada.



Figura 1: Pilha de protocolos sugeridos pela SIG

* + Bluetooth Radio: representa a camada física do modelo OSI, lidando diretamente com a transmissão de dados via radiofrequência e sua modulação.
	+ Basehand: descreve a especificação do Controlador de Enlace (LC). É responsável pelo protocolo de controle e por algumas rotinas de enlace de baixo nível.
	+ LMP (Link Manager Protocol – Protocolo de Gerenciamento de Enlace): responsável pela configuração e controle dos Protocolos de Gerenciamento.
	+ HCI (Host Controller Interface – Interface de Controle do Host): provê às camadas superiores uma interface de acesso ao Gerenciador de Enlace e ao Controlador.
	+ L2CAP (Logical Link Control and Adaptation Protocol – Protocolo de Adaptação e Controle do Enlace Lógico): segmenta e dessegmenta, multiplexa e desmultiplexa os pacotes e também lida com requisitos de qualidade do serviço.
	+ RFCOMM (Radio Frequency Communication): emula uma porta serial convencional e permite que os dispositivos já existentes passem a fazer parte do sistema.
	+ SDP (Service Discovery Protocol – Protocolo de Descoberta do Serviço): permite descobrir os serviços disponíveis nos dispositivos Bluetooth e quais são as características de cada um.

Analisando a *Figura 1* nota-se a existência de uma linha branca separando as implentações de hardware e de software. Abaixo dessa linha temos as funcionalidades de hardware, e acima, a proposta de protocolo adaptável à aplicação, onde são disponibilizados diferentes módulos que possibilitam a cada nova aplicação selecionar e utilizar apenas aqueles que correspondem aos seus requisitos específicos, não sendo necessários reescrevê-los.



Figura 2: Módulos de serviços utilizados pelos perfis

 Pilhas de protocolo sugeridas para cada Perfil:

* Perfil de Acesso Genérico: base para a realização de aplicações reais. Sua base é estabelecer e manter enlace entre o dispositivo mestre e os escravos.
* Perfil de Descoberta de Serviço: usado para que um dispositivo descubra os serviços disponíveis por outros dispositivos.
* Perfil de Porta Serial: protocolo de transporte que emula uma porta serial (muito utilizada por outros perfis).
* Perfil de Intercâmbio Genérico de Objetos: define um relacionamento entre os dispositivos cliente/servidor para troca de dados (muito utilizada por outros perfis).
* Perfil de Acesso a LAN: permite que um notebook ou um PDA se conecte a uma LAN fixa.
* Perfil de Rede Dial-up: permite que um notebook se conecte a um telefone móvel que possua modem interno sem fio.
* Perfil de Fax: permite que um aparelho de Fax, faça e receba mensagens utilizando um telefone móvel sem fio.
* Perfil de Telefonia Sem Fio: permite que um telefone móvel sem fio se conecte a sua estação na base.
* Perfil de Intercomunicação: permite que dois telefones se conectem como intercomunicadores.
* Perfil de Fone de Ouvido: permite a comunicação sem o uso das mãos.
* Push de Objetos: fornece um meio de intercambiar objetos simples.
* Perfil de Transferência de Arquivos: fornece um recurso mais geral de tranferência de arquivos.
* Perfil de Sincronização: permite sincronizar, por exemplo, um PDA a um computador.

**III. CONEXÃO**

O controlador Bluetooth possui dois principais estados: o “stand by”, onde apenas o relógio do dispositivo permanece ativo e é considerado o estado padrão de baixo consumo, e o “conexão” que é o estado onde um dispositivo pode se comunicar com outros.

No “estado de conexão” existem outros sub-estados como é mostrado no diagrama abaixo:



Figura 3: Diagrama de estados do Controlador Bluetooth

Para estabelecer uma conexão, os dispositivos Bluetooth devem executar uma sequência de passos padrão, definida pelo protocolo. Primeiramente, o dispositivo que quer estabelecer conexão (dispositivo master), manda uma mesagem *INQUIRY*  para descobrir quais dispositivos econtram-se em sua área de alcance e quais suas caracterísiticas. O dispositivo (slave) que deseja receber esta mensagem deve estar no estado de *INQUIRY*. Após executar este procedimento, o dispositivo altera seu status para *INQUIRY RESPONSE,* enviando um pacote de resposta FHS (Frequency Hopping-Synchronization), contendo sua identidade e as informações para estabelecerem o sincronismo. Uma vez reunida as informações sobre os dispositivos que se encontram ao seu alcance, o próximo procedimento executado pelo dispositivo que deseja estabelecer uma conexão é chamado de *PAGING*.

Neste momento, o dispositivo master deve enviar um pacote do tipo *PAGE* (pacote do tipo ID com o DAC do dispositivo destino), para o destino. Caso o relógio destes dispositivos não estejam sincronizados, este mesmo pacote é reenviado em outras frequências, obtidas durante o processo de *INQUIRY*.

Para que um dispositivo possa responder uma mensagem de PAGE, ele deve estar no modo *PAGE SCAN*, onde faz a escuta de um canal com mensagens contendo seu DAC. Uma vez recebida uma mensagem deste tipo, altera novamente seu estado para *SLAVE RESPONSE,* onde irá trasnmitir uma mensagem de resposta contendo o DAC de sua unidade, utilizando uma sequência de frequências (*page response hopping sequence*). O dispositivo master ao receber este pacote de dados, entra no estado de *PAGE MASTER RESPONSE*, enviando ao destino outro pacote, chamado de FHS, utilizando uma outra sequência de frequências chamada *page hopping sequence*.

No momento em que o dispositivo destino recebe este pacote, ele deve responder com outro pacote ID contendo o seu DAC, isto o torna slave do dispositivo ao qual respondeu. E assim que o dispositivo receber esta última mensagem como resposta, passará a atuar como master.

Durante o estado de conexão, são trocados mensagens de controle definindo links SCO (Synchronous Connection Oriented) ou ACL (Asynchronous Connection-Less) e somente após estes links estabelecidos poderão trocar informações.

Modos de operação que um dispositivo poderá se encontrar durante um estado de conexão:

* Active: modo em que uma unidade participa ativamente do canal.
* Sniff: a unidade slave escuta o canal com uma taxa reduzida (economiza energia). O tempo do sniff é ajustável, sendo dependente da aplicação.
* Hold: modo intermediário de gasto de energia.
* Park: o único procedimento que é realizado é a manutenção do sincronismo com o dispositivo master, onde as unidades slaves nao participam do tráfego do canal. Para ocorrer esta manutenção ocorre a escuta ocasional de mensagens. Os dispositivos slaves perdem os rotulos e para poderem participar novamente do canal, precisam reobte-los. Oferece o menor consumo de energia dentre os outros.

Também durante este estado, o dispositivo master envia pacotes POLL para verificar sua ligação com outros dispositivos. Caso não obtenha resposta, durante um número de slots, estes dispositivos deverão reestabelecer a conexão.

**IV. SEGURANÇA**

A segurança em tecnologias que utilizam radiofrequência é um dos fatores mais críticos. O meio utilizado (ar) é de livre acesso tornando fácil a interceptação. As questões mais importantes se referem a autenticação, autorização e encriptação de dados.

 A segurança entre dispositivos Bluetooth, inicia quando decide-se como estes dispositivos irão implementar suas opções descoberta e conectivadade. Diferentes combinações dessas capacidade, pode ser divididas em três níveis e em três modos.

Os três níveis são:

* Silencioso: não faz nem autenticação nem autorização. O dispositivo simplesmente monitora o tráfego do Bluetooth.
* Privado: aceita autenticação, mas não aceita autorização.
* Público: necessita tanto de autenticação como de autorização.

Os três modos são:

* Sem segurança: não garante nenhum tipo de segurança e permite que os dados sejam facilmente acessados por outros dispositivos.
* Nível de Serviço: segurança obrigatória no nível de serviço, isto é, concede acessos por serviço individual.
* Nível de Conexão: segurança é obrigatória ao nível de link, ou seja, a segurança começa a existir no início da conexão, sendo comum para todas.

E os dispositivos podem ser divididos em dois grupos:

* Confiávéis: possuem relacionamento fixo e acesso permatente aos dispositivos.
* Não confiáveis: não possuem relacionamento permanente e restrições de acesso ao serviço.

**V. VERSÕES**

* 1.0: primeira versão. Com ela os fabricantes encontravam problemas que dificultavam a interoperabilidade entre dispositivos e a implementação.
* 1.1: (fev/2001) representa o estabelecimendo do Bluetooth como um padrão 802.15. Muitos problemas da v1.0 foram solucionados. Implementado suporte ao RSSI.
* 1.2: (nov/2003) conexão mais rápida, proteção mais forte contra interferências, suporte a scatternet aperfeiçoado e processamento de voz avançado.
* 2.0: (nov/2004) diminuição do consumo de energia, aumento na transmissão de dados para 3Mbps, correção de falhas da v1.2 e melhor comunicação entre os dispositivos.
* 2.1: (ago/2007) acréscimos de informações ao sinal *INQUIRY* antes de efetivamente estabelecer uma conexão, melhorias na segurança e melhor gerenciamento de energia.

**VI. CONCLUSÃO**

Definitivamente o ponto forte da tecnologia Bluetooth está na definição do seu protocolo de comunicação em camadas, e na organização de perfis de utilização. Através de uma estrutura organizada em módulos, é possível configurar as aplicações de maneira que sejam utilizados/oferecidos apenas os serviços pertinenetes ao funcionamento de cada uma destas, o que sem dúvida acarreta em ganho singnificativo de eficiência na utilização desta tecnologia.

Atualmente, o mercado encontra-se aquecido quando o assunto é tecnologias móveis. Nos últimos anos, houve um crescimento significativo na procura por dispositivos desta família, onde é cada vez mais comum encontrarmos a tecnlogia Bluetooth disponível, como em celulares, notebooks e PDAs. Isso nos leva a crer que está sendo configurado um cenário favorável para a expansão da tecnologia Bluetooth, podendo ser adotada, em pouco tempo, como padrão de comunicação sem fio de baixo alcance.

Referências:

[1] [www.wikipedia.com/Bluetooth.html](http://www.wikipedia.com/Bluetooth.html)

[2] <http://www-usr.inf.ufsm.br/~aldacir/Bluetooth.html>

[3] <http://www.boadica.com.br/layoutdica.asp?codigo=383>

 [4] <http://www.infowester.com/bluetooth.php>

[5] <http://www.mundowireless.com.br/bluetooth>

[6] <http://www.timaster.com.br/revista/artigos/main_artigo.asp?codigo=407>

[7] <http://www.gta.ufrj.br/seminarios/semin2003_1/stein/controle_canal.html>

[8] <http://www.bluetomorrow.com/content/section/99/316/>

[9] Morrow, Robert K. Bluetooth operation and use.  New York, NY : McGraw-Hill, c2002.  567 p. : il.