INSTITUTO NACIONAL DE TELECOMUNICAÇÕES

INATEL

Introdução ao Bluetooth

Autores: Ronaldo Sampei
Eduardo Moreira de Freitas

Orientador: Eduardo Pina

INSTITUTO NACIONAL DE TELECOMUNICAÇÕES
INATEL

CURSO DE PÓS-GRADUAÇÃO
ENGENHARIA DE REDES e SISTEMAS DE TELECOMUNICAÇÕES

Introdução ao Bluetooth

Autores: Ronaldo Sampei
Eduardo Moreira de Freitas

Orientador: Eduardo Pina

Monografia submetida ao Instituto Nacional de Telecomunicações como requisito para conclusão do curso de especialização Engenharia de Redes e Sistemas de Telecomunicações.

INSTITUTO NACIONAL DE TELECOMUNICAÇÕES
INATEL

Introdução ao Bluetooth

Autores: Ronaldo Sampei
Eduardo Moreira de Freitas

Orientador: Eduardo Pina

BANCA EXAMINADORA

_____
Prof. Examinador 1

_____
Prof. Examinador 2

_____
Prof. Examinador 3

Santa Rita do Sapucaí, 10 de Maio de 2002.

RESUMO

A quantidade de dispositivos de computação e de telecomunicações está crescendo e, como conseqüência, cresce também o interesse em como interconectá-los. O uso de cabos é em geral complicado porque requer software de configuração e um cabo específico para que os dispositivos possam ser conectados. A solução através de luz infravermelha elimina a necessidade do cabo, mas requer visada direta. Para resolver estes problemas, foi desenvolvida uma nova tecnologia chamada Bluetooth. Com o Bluetooth, os usuários podem conectar uma grande variedade de dispositivos de computação e de telecomunicações de maneira fácil e simples, sem a necessidade de conectar cabos. A tecnologia determina como unidades podem se comunicar a distâncias de até 10 metros umas das outras. Ela também define como algumas aplicações devem ser mapeadas para que sejam compatíveis com o Bluetooth. A grande vantagem da solução Bluetooth é a utilização de chips pequenos, baratos e de baixo consumo. Este trabalho apresenta uma introdução à tecnologia do Bluetooth, descrevendo sua arquitetura, seus protocolos, modelos de aplicação, tipos de processos, e aspectos de mercado.

ABSTRACT

The amount of computation and telecommunications devices is growing and, as consequence, also grows the interest in how to interconnect them. The use of cables is in general complicated since it requires configuration software and a specific cable to interconnect the devices. Infra red light solutions eliminate the need of cables, but require line of sight. To solve these problems, a new technology called Bluetooth was developed. With Bluetooth, users can connect a great variety of computation and telecommunications devices in an easy and simple way, without the need of cables. The technology determines how units can communicate with each other within a 10-meter range. It also defines how some applications must be mapped to be compatible with Bluetooth. The advantage of the Bluetooth solution is that it uses small, cheap and low power consumption chips. This document presents an introduction to the Bluetooth technology, describing its architecture, protocols, models of application, types of processes, and market aspects.

Índice Analítico

Lista de Figuras

Lista de Tabelas

1. INTRODUÇÃO

O crescimento da quantidade de dispositivos de computação e de telecomunicações está incentivando o desenvolvimento de soluções que permitam conectar estes dispositivos entre si. A solução usual consiste em conectar os dispositivos através de cabos para tornar possível a transferência de arquivos e a sincronização. A transferência de arquivos é necessária para que o usuário possa, por exemplo, digitar um documento em um PDA e transferi-lo depois para um PC. Existe também a necessidade de sincronização de eventos nos calendários dos diversos dispositivos. A solução para estas exigências tem sido conectar os dispositivos por um cabo ou, às vezes, usando luz infravermelha.

A solução via cabos é sempre complicada porque requer um cabo específico para os dispositivos a serem conectados, bem como software de configuração. A solução através de luz infravermelha elimina a necessidade do cabo, mas requer visada direta. Uma nova tecnologia foi desenvolvida para resolver estes problemas: o Bluetooth. O Bluetooth provê os meios para a solução via enlace de rádio de curto alcance. Ele é o resultado de um esforço conjunto entre empresas que buscam uma solução barata, simples, de baixo consumo, e com suporte do mercado mundial.

Com o Bluetooth, os usuários terão a possibilidade de conectar uma grande variedade de dispositivos de computação e de telecomunicações de maneira fácil e simples, sem a necessidade de conectar cabos. A tecnologia determina como unidades podem se comunicar a distâncias de até 10 metros umas das outras. Ela também define como certas aplicações devem ser mapeadas para que sejam compatíveis com o Bluetooth. Se esta compatibilidade for alcançada, a tecnologia assegura que um dispositivo possa operar com outros dispositivos e aplicações do Bluetooth independente de seu fabricante. A tecnologia pode também viabilizar a comunicação entre várias unidades, como pequenas LAN's via rádio. Isto permitirá ao usuário implementar um grande número de aplicações.

O ponto forte da concepção Bluetooth é que os chips Bluetooth podem ser muito pequenos; eles são baratos e de baixo consumo. Além disto, existe o suporte para a tecnologia através de uma grande variedade de empresas. Ela não é suportada apenas pelas industrias de PC e telefones celulares, mas também conta com o apoio de diversas outra industrias.

Este trabalho tem como objetivo dar uma visão geral da concepção Bluetooth. Ele tenta cobrir aspectos técnicos relativos a hardware, software e aplicativos Bluetooth. Ele também mostra aspectos de marketing em relação às tecnologias concorrentes.

O trabalho começa com uma introdução onde a origem e a organização de padronização Bluetooth são descritos. O capítulo 2 (“Bluetooth”) apresenta os benefícios e as possibilidades que a tecnologia pode prover ao usuário. Este capítulo também mostra uma visão sobre a posição de mercado do Bluetooth. O capítulo 3 (“Arquitetura Bluetooth”) descreve as camadas de protocolos Bluetooth e suas configurações. Os capítulos seguintes descrevem com mais detalhes os recursos, protocolos e aplicações Bluetooth, bem como sua interface aérea. No capítulo 5 (“Por quê Bluetooth – Aspectos Técnicos”) são apresentadas as tecnologias concorrentes e os pontos fortes da concepção Bluetooth.

1.1. Origem

A tecnologia e o padrão Bluetooth fornecem o meio para a substituição do cabo que conecta um dispositivo ao outro, através de um enlace universal de rádio de curto alcance. A tecnologia foi inicialmente desenvolvida para a substituição dos cabos, porém tem sido agora desenvolvida não apenas para isso, mas também como uma técnica para estabelecer conexão entre diversas unidades. Por exemplo, ela mostra como criar uma pequena LAN de rádio.

Em 1994, a Ericsson iniciou um estudo para desenvolver uma interface de rádio – de baixo consumo e baixo custo – entre telefones móveis e seus acessórios. Foram definidas condições e requerimentos relativos a preço, capacidade e tamanho para que a nova técnica apresentasse vantagens sobre todas as soluções existentes que utilizam de cabos na conexão de dispositivos móveis. Inicialmente, uma interface adequada de rádio e uma faixa de freqüência de operação tinham que ser especificadas. Alguns critérios também foram definidos relativos a tamanho, capacidade e uniformidade global: a unidade de rádio deveria ser pequena e de baixo consumo, permitindo sua instalação dentro de unidades portáteis; a solução também deveria permitir a transmissão de voz e dados e, finalmente, deveria operar mundialmente.

O estudo mostrou logo que a solução de um enlace de rádio com curto alcance era possível. Quando projetistas da Ericsson começaram a trabalhar no chip transmissor, a Ericsson percebeu que eles precisavam de parceiros para desenvolver a nova tecnologia. Os sócios ajudariam não apenas para aprimorar as soluções técnicas, mas também a criar um sólido e amplo suporte de marketing nas áreas de negócios referentes a hardware de PC, computadores portáteis e telefones móveis. O interesse em evitar o surgimento de um mercado com um número alto de soluções incompatíveis baseadas no uso de cabos – onde um cabo seria projetado especificamente para

um determinado par de equipamentos – foi um dos motivos que levaram empresas concorrentes a se unirem ao projeto.

Ericsson, Intel, IBM, Toshiba e Nokia formaram um Grupo de Interesse Especial ("Special Interest Group" – SIG) em 1998. Este grupo representava a diversidade de suporte de mercado necessária para gerar um boa base para a nova tecnologia. A intenção do consórcio, existente até hoje, é desenvolver um padrão para a interface aérea do Bluetooth e um software que o controla, permitindo alcançar uma interoperabilidade entre diferentes equipamentos de diferentes fabricantes de computadores portáteis, telefones móveis e outros dispositivos. O nome escolhido para a tecnologia, Bluetooth, se baseou nesta funcionalidade: o nome Bluetooth veio de um rei e viking dinamarquês, chamado Harald Blåtand (Bluetooth em inglês), que viveu no final do século 10. Harald Blåtand uniu e controlou a Dinamarca e a Noruega.

1.2. Bluetooth SIG

Em Fevereiro de 1998, o Grupo de Interesse Especial Bluetooth, SIG, foi fundado. No começo, ele era formado pelas 5 empresas mencionadas anteriormente: Ericsson, Intel, IBM, Toshiba e Nokia. Hoje, mais de 1.300 empresas juntaram-se ao SIG trabalhando para um padrão aberto da concepção Bluetooth. Através da assinatura de um acordo de custo zero, empresas podem se juntar ao SIG e se qualificar para terem licença de produzir produtos baseados na tecnologia Bluetooth.

Para evitar interpretações diferentes do padrão Bluetooth relativos à maneira como uma aplicação específica deverá ser mapeada, o SIG definiu uma série de aplicativos e recursos. Eles são descritos com mais detalhes nos capítulos seguintes.

O SIG também trabalha com um processo de qualificação. Este processo define o critério para a qualificação de novos dispositivos, garantindo que produtos aprovados estão adequados às especificações do Bluetooth.

2. BLUETOOTH

2.1. Por quê Bluetooth – Aspectos de Marketing

A idéia de remover as conexões via cabos entre os telefones móveis e seus acessórios deram originem à concepção do Bluetooth. O Bluetooth eliminaria o emaranhado de fios necessário para conectar um computador com um teclado, um mouse, um par de alto-falantes, um PDA etc.. Além disso, a necessidade de manter todos estes diferentes dispositivos próximos uns aos outros seria eliminada. Em vez disso, a localização do dispositivo dependeria apenas do ponto de alimentação.

Outra vantagem da tecnologia Bluetooth se refere à conexão e configuração de dispositivos móveis. Com a tecnologia convencional (via cabos), a conexão de um novo dispositivo requer um cabo específico de acordo com a marca do dispositivo. Estabelecida a conexão física entre os dispositivos, segue-se um procedimento de configuração complicado. A substituição dos cabos por uma conexão via rádio elimina estes problemas, embora exija o desenvolvimento de técnicas que garantam a segurança das informações transmitidas. Esta questão, de privacidade e segurança, também é estudada no desenvolvimento da tecnologia Bluetooth.

A introdução do Comunicador Nokia 9000 também foi descrito como um evento que aumentou o interesse no desenvolvimento do Bluetooth. O Comunicador reduziu a complexidade de conexão entre o telefone móvel com o computador ao disponibilizar a unidade 2 em 1 para resolver o problema. Isto mostrou que um dos caminhos mais fáceis para tráfego de dados via GSM era a compra de um Comunicador, e não de um cartão de interface de dados GSM com cabos de interligação entre o telefone e computador. A combinação de dois dispositivos em um foi vista como uma ameaça para os maiores fabricantes de PC's portáteis. O que poderia acontecer se as pessoas começassem a comprar Comunicadores de fabricantes de telefones ao invés de PC's portáteis da IBM e Toshiba? Além disso, a introdução dos Comunicadores poderia criar um impacto na venda de processadores centrais da Intel, que domina o mercado de PC's, mas não tem um produto competitivo para os telefones inteligentes ou PC's de mão. Portanto, um desenvolvimento que mantenha a forte posição de mercado dos PC's portáteis é essencial para a indústria de PC.

Outros motivos para a nova técnica de substituição de cabos são:

- O número de usuários de PC's portáteis está aumentando. Isto indica um amplo mercado para conexão de dispositivos sem o uso de cabos;
- A constante diminuição das dimensões dos PC's portáteis levou ao surgimento de soluções em que dispositivos como um drive de CD-ROM são externos, e precisam ser conectados facilmente ao PC;
- Computadores móveis já competem com computadores de mesa em performance. É cada vez menos necessário possuir um PC fixo no escritório e um PC portátil para viagem.

A técnica Bluetooth fornece uma solução para os problemas descritos acima. O Bluetooth elimina o problema de cabos e sua limitação referente ao alcance e à flexibilidade (sempre específico para fabricante ou par de dispositivos). Porém, o Bluetooth significa mais do que isto. A tecnologia fornece um meio para a conexão de diversas unidades Bluetooth como em uma instalação de uma pequena LAN via interface aérea. Um grande número de aplicações de usuários já foram descritas. Elas criam possibilidades que vão muito além da simples eliminação do cabo de conexão ponto-a-ponto.

2.2. Exemplos de Aplicações Bluetooth – O Futuro é Agora

Renata, gerente de vendas e marketing de uma empresa de consultoria em software, está trabalhando em um importante documento em seu PC. Sua empresa fica localizada em São Paulo. Não existem cabos no escritório da Renata, exceto os de alimentação de energia. Telefone, teclado, alto-falantes, monitor e o próprio PC são todos conectados através do Bluetooth. A eliminação dos cabos mostrou novas maneiras de mobiliar o escritório, uma vez que a CPU não precisa mais ficar próxima do teclado e do monitor.

Quando o Sr. Braga liga, Renata atende apertando um botão no seu fone de ouvido Bluetooth. O Sr. Braga é um dos organizadores de uma exposição no Rio de Janeiro. Ele pergunta se Renata pode discursar na exposição e apresentar uma visão da empresa sobre a nova técnica para pequenas LAN's. Ao checar sua agenda, Renata percebe que o horário desta apresentação coincidiria com uma reunião marcada na mesma exposição. Mesmo assim, Renata aceita fazer a apresentação. Enquanto ela caminha para a agência de viagens, que fica no mesmo andar de seu escritório, o organizador da reunião liga para conversar com a Renata sobre alguns dos itens que serão discutidos na reunião. Durante a conversa, o agente de viagens finaliza a reserva do vôo e

Renata o instrui para lhe enviar o bilhete mais tarde na forma de bilhete eletrônico (“e-ticket”). Após terminar o trabalho e verificar se a apresentação está em ordem, Renata guarda seu computador no bolso e caminha para o carro.

Enquanto Renata dirige, o e-ticket para o Rio de Janeiro é recebido em seu “smartphone”. Quando Renata chega ao estacionamento do aeroporto de Congonhas, o número de seu cartão de crédito é transmitido via Bluetooth para o sistema do estacionamento. Naturalmente, Renata pagará tanto o estacionamento como o aluguel de carro no Rio de Janeiro através do navegador WAP ou mesmo diretamente de seu smartphone. No guiché da companhia aérea, a identificação e o check-in são feitos via Bluetooth. Depois do check-in, Renata se dirige para a sala executiva do aeroporto. A porta da sala se abre automaticamente quando o equipamento Bluetooth na sala detecta o cartão eletrônico de embarque da Renata. Para obter o mapa da área de exibição, Renata se conecta à Internet através da LAN da sala usando Bluetooth.

No avião, Renata encontra uma velha amiga. Como estão sentadas em poltronas distantes, elas começam a conversar usando seus PC’s portáteis. Elas conversam sobre um novo jogo de computador que a Renata não conhecia. Depois de receber o jogo de sua amiga, elas começam a jogar. Após uma leve refeição no avião, Renata escreve um e-mail para enviar para casa. O e-mail será transmitido quando o avião pousar e a Renata tiver ligado novamente seu smartphone.

Já na área de exibição da exposição no Rio, Renata encontra a sala 2, onde os palestrantes estão reunidos. O organizador dá a Renata e aos outros palestrantes uma senha que lhes permite usarem o projetor de vídeo principal. Como sempre, os palestrantes usam microfones sem fio Bluetooth em suas apresentações e a convenção segue conforme planejada. Depois, Renata encontra com o Sr. Souza e outros 4 participantes em um empreendimento conjunto. Ela e os outros trocam cartões vCards através de seus smartphones usando Bluetooth. Todos os presentes na reunião estão usando a tecnologia Bluetooth, que permite a formação de uma rede com seus PC’s de forma que todos possam trabalhar em um mesmo documento ao mesmo tempo. Após algumas pequenas discussões, eles terminam seus trabalhos da especificação de multimídia sobre Bluetooth e Renata pode voltar correndo para o aeroporto.

2.3. Uma Introdução da Interface Aérea do Bluetooth

Para adequar os requerimentos da interface aérea, uma banda de freqüência entre 2,4 e 2,5 GHz foi selecionada. Esta banda de freqüência é especificada pela indústria médica, chamada de banda ISM (Industrial-Scientific-Medical) e abrange, na Europa e nos Estados Unidos, de 2.4 até

2.4835 GHz; na França e na Espanha apenas parte desta banda está disponível. Dessa forma, os requerimentos relativos a operação mundial, suportando tanto dados como voz, além da limitação em relação às características físicas (tamanho e energia consumida) foram cobertos. Como resultado, dispositivos Bluetooth deverão atuar na faixa de 2.4 a 2.5 GHz. A banda ISM é aberta para qualquer sistema de rádio. Telefones sem fio, controle de portas automáticas de garagens e fornos microondas operam nesta banda, onde o forno microondas é a maior fonte de interferência.

Unidades Bluetooth conectam-se umas à outras formando uma rede chamada "piconet", consistindo de até 8 unidade Bluetooth ativas. Isto é descrito no capítulo 5 ("A Interface Aérea do Bluetooth").

3. ARQUITETURA BLUETOOTH

Este capítulo descreve a arquitetura do Bluetooth. A pilha completa de protocolos compreende, como mostrado na figura 1, tanto os protocolos definidos como os não definidos pelo Bluetooth. Na figura 1, os protocolos não definidos são sombreados.

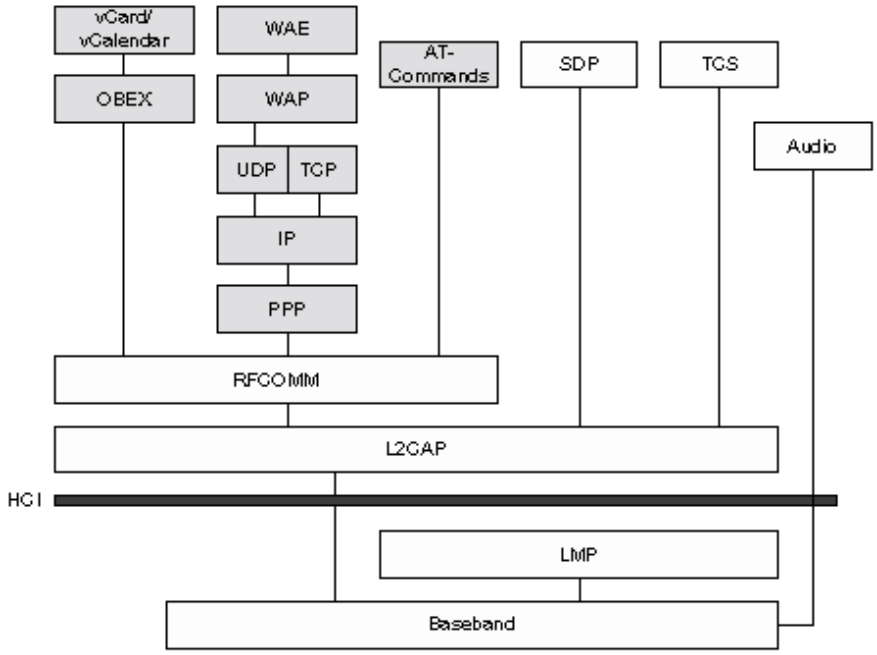

Fig. 1 – Pilha de Protocolos do Bluetooth

Diferentes aplicativos podem ser executados sobre diferentes pilhas de protocolos. Apesar disso, cada uma destas diferentes pilhas de protocolos usa uma conexão de dados Bluetooth e uma camada física comuns (veja mais detalhes na seção 4.4 – Protocolos Bluetooth). A figura 1 mostra a pilha completa de protocolos do Bluetooth como identificado na especificação, sobre a qual os aplicativos interoperacionais que suportam modelos de uso do Bluetooth são montados. Nem todos os aplicativos fazem uso de todos os protocolos mostrados na figura 1. Em vez disso, aplicativos rodam sobre um ou mais segmentos verticais desta pilha de protocolos. Tipicamente, segmentos verticais adicionais são para serviços que sustentam a aplicação principal, como a Especificação de Controle de Telefonia (Telephony Control Specification - TCS Binary) ou o Protocolo de Serviço de Descobrimento (Service Discovery Protocol – SDP). Vale a pena mencionar que a figura 1 mostra a relação de como os protocolos estão usando os serviços de

outros protocolos quando carga útil precisa ser transferida via interface aérea. No entanto, os protocolos podem também ter outras relações com outros protocolos. Por exemplo, alguns protocolos (L2CAP, TCS) podem usar o Protocolo de Controle de Enlace (Link Manager Protocol – LMP) quando existe a necessidade de controle de gerência de conexão.

3.1. Estratégia da Arquitetura Bluetooth

O projeto dos protocolos e da pilha de protocolos teve como princípio maximizar o aproveitamento de protocolos já existentes para diferentes finalidades nas camadas mais altas. Ou seja, procurou-se não "reinventar a roda". A reutilização de protocolos também ajuda a adaptar aplicativos existentes (legado) para trabalhar com a tecnologia Bluetooth e garantir a operação e interoperabilidade desses aplicativos. Deste modo, muitos aplicativos já desenvolvidos por fornecedores podem fazer uso de imediato de sistemas de hardware e software compatíveis com a especificação Bluetooth. A especificação também é aberta, o que permite que fornecedores implementem livremente protocolos proprietários ou protocolos de uso comum sobre protocolos específicos do Bluetooth. Assim, a especificação aberta permite o desenvolvimento de uma grande quantidade de novas aplicações que aproveitam ao máximo a capacidade da tecnologia Bluetooth.

A especificação do Bluetooth define vários "profiles" – que chamaremos de "recursos" neste trabalho – que descrevem como devem ser implementados os modelos de usuários. Modelos de usuários descrevem uma série de cenários de aplicações onde o Bluetooth executa a transmissão via rádio. Um recurso pode ser descrito como uma "fatia" vertical através da pilha de protocolos. Ele define faixas de parâmetros para cada protocolo. O conceito de recurso é usado para minimizar o risco do surgimento de problemas de interoperabilidade entre produtos de diferentes fabricantes.

Existem quatro recursos gerais definidos – como mostra a figura 2 – sobre os quais alguns dos aplicativos prioritários e suas funcionalidades são diretamente baseados. Estes quatro modelos são: Recurso de Acesso Genérico ("Generic Access Profile" – GAP), Recurso de Porta Serial ("Serial Port Profile"), Recurso de Serviço de Pesquisa/Descobrimento ("Service Discovery Application Profile" – SDAP) e Recurso de Troca de Objeto Genérico ("Generic Object Exchange Profile" – GOEP).

O SIG também identifica alguns aplicativos como fundamentais. Este aplicativos são destacados na documentação do Bluetooth. Alguns destes aplicativos e suas funcionalidades são descritos

nos capítulos seguintes, sendo que para todo aplicativo existe um ou mais recursos correspondentes.

A figura 2 ilustra a estrutura de recursos Bluetooth e as dependências entre eles. Um recurso é dependente de outro se ele reutiliza partes desse outro recurso, implícita ou explicitamente fazendo referência a ele. A figura 2 ilustra estas dependências: um recurso depende dos recursos em que ele está contido – direta e indiretamente.

Protocolos como OBEX e UDP foram incluídos na arquitetura para facilitar a adaptação de aplicativos que já usam estes protocolos existentes. Isto fornece uma interface para a tecnologia Bluetooth a vários aplicativos existentes que suportam UDP.

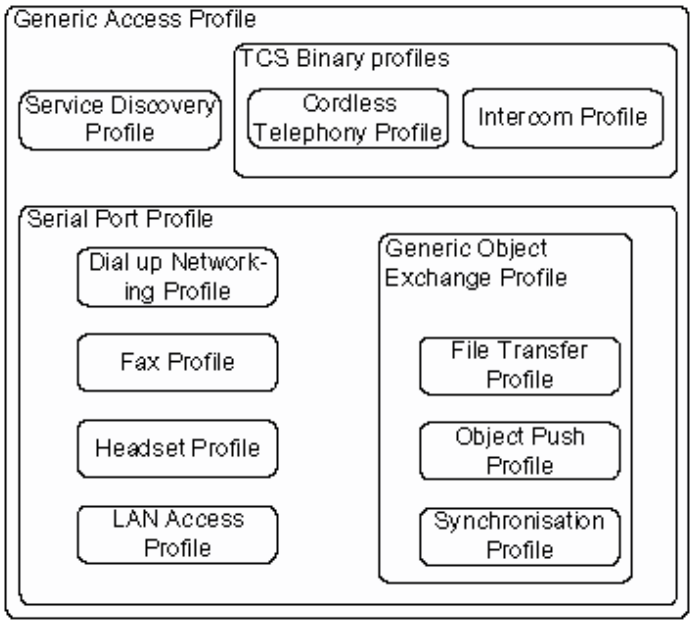

Fig. 2 – Recursos (Profiles) Bluetooth

Exemplo:

O recurso definido para troca de informações Vcard é ilustrado na Figura 3, onde a aplicação Vcard é definida para operar sobre um certo subgrupo (OBEX, RFCOMM e assim por diante) da pilha de protocolos Bluetooth.

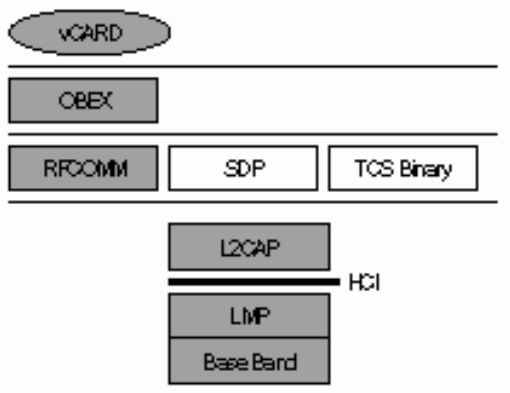

Fig. 3 – Recurso de Troca de Objeto

O objetivo da especificação é permitir que os aplicativos sejam desenvolvidos de maneira que se conformem com a especificação para operarem entre si. Para permitir esta interoperabilidade, aplicações idênticas em dispositivos remotos (ex.: aplicação cliente-servidor correspondente) devem rodar sobre pilhas de protocolos idênticas.

3.1.1. Camadas de Protocolos Bluetooth

A pilha de protocolos Bluetooth pode ser dividida em 4 camadas de acordo com suas finalidades:

Protocol layer	Protocols in the stack
Bluetooth Core Protocols	Baseband, LMP, L2CAP, SDP
Cable Replacement Protocol	RFCOMM
Telephony Control Protocols	TCS Binary, AT-commands
Adopted Protocols	PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC, WAE

Tabela 1 – As camadas e os protocolos do Bluetooth

Além das camadas de protocolos acima, a especificação também define uma Interface Controladora do Host ("Host Controller Interface" – HCI), que fornece uma interface de comandos para o controlador de banda base, controlador de enlace, e acesso ao status de hardware e controle de registros.

Os “Bluetooth Core Protocols” incluem somente protocolos específicos do Bluetooth desenvolvidos pelo SIG. Os protocolos RFCOMM e TCS binary também foram desenvolvidos pelo SIG, mas são baseados nas recomendações ETSI TS 07.10 e ITU-T Q.931, respectivamente. Os “Bluetooth Core Protocols” (mais a parte de rádio do Bluetooth) são requeridos pela maioria dos dispositivos Bluetooth, enquanto o resto dos protocolos são utilizados apenas quando necessário.

Juntas, a camada de substituição do cabo (“Cable Replacement Layer”), a camada de controle de telefonia (“Telephony Control Layer”) e a camada de protocolos adotados (“Adopted Protocol Layer”) formam protocolos orientados a aplicação, permitindo aos aplicativos serem executados sobre os protocolos do Bluetooth. Como mencionado anteriormente, a especificação Bluetooth é aberta e protocolos adicionais (ex. HTTP, FTP, etc.) podem operar sobre protocolos de transporte específicos do Bluetooth ou sobre os protocolos orientados a aplicação mostrados na figura 1.

3.2. Recursos (Profiles) Bluetooth

Os recursos descritos nesta seção formam a base para os aplicativos e suas funcionalidades e também fornecem a fundação para aplicativos e recursos futuros.

3.2.1. Recurso de Acesso Genérico (GAP)

O recurso GAP (“Generic Access Profile”) define como duas unidades Bluetooth descobrem e estabelecem uma conexão entre si. O GAP garante que quaisquer duas unidades Bluetooth, independente de fabricante e aplicação, possam trocar informações através do Bluetooth para descobrir que tipo de aplicações as unidades suportam.

Os propósitos do GAP são:

- Definir os requerimentos referentes a nomes, valores e esquemas de codificação usados como parâmetros e procedimentos no nível de interface de usuário.
- Definir modos de operação genéricos a todos os recursos (ou seja, modos não relacionados a algum serviço ou recurso específico).

- Definir os procedimentos gerais que podem ser usados para obter identificação, nomes e funcionalidades básicas de outros dispositivos. São especificados somente procedimentos que não usam estabelecimento de canal ou conexão.
- Definir o procedimento geral para interconectar dispositivos Bluetooth.
- Descrever os procedimentos gerais que podem ser usados para estabelecer conexões com outros dispositivos Bluetooth.

Dispositivos Bluetooth que não estão em conformidade com algum outro recurso Bluetooth têm que estar em conformidade com o GAP para garantir a interoperabilidade básica e coexistência.

Aspectos da Interface de Usuário

O GAP especifica os termos genéricos que devem seu utilizados no nível da interface de usuários.

Representação de parâmetros Bluetooth

- Endereço de dispositivo Bluetooth (BD_ADRR) – é o endereço exclusivo de um dispositivo Bluetooth. Ele é recebido de um dispositivo remoto durante o procedimento de pesquisa/descobrimento de serviços. Este endereço é definido no nível de banda base como um endereço de 48 bits (12 caracteres hexadecimais).
- Nome do dispositivo Bluetooth ("user friendly name") – é uma string com até 248 caracteres.
- Chave Bluetooth ("Bluetooth Pass-Key – PIN number") – O PIN (número de identificação pessoal) é usado para autenticar dois dispositivos Bluetooth (que não haviam trocado chaves de conexão previamente) e estabelecer uma conexão confiável entre eles. O PIN pode ser inserido no nível de interface usuário mas também pode ser armazenado no dispositivo. Ele é chamado de Bluetooth Pass-Key no nível de interface usuário.
- Classe de dispositivo Bluetooth ("Device Type") – é um parâmetro recebido durante o procedimento de pesquisa/descobrimento, indicando o tipo de dispositivo e quais tipos de serviço são fornecidos.

Procedimentos de estabelecimento

Estabelecimento de enlace

O propósito do procedimento de estabelecimento de enlace é estabelecer um enlace físico (assíncrono, ACL) entre dois dispositivos Bluetooth. Ele tipicamente envolve duas etapas: paging e setup de conexão.

Estabelecimento de canal

O propósito do procedimento de estabelecimento de canal é estabelecer uma conexão lógica entre dois dispositivos Bluetooth. O estabelecimento de canal se inicia após a conclusão do estabelecimento de conexão.

Estabelecimento de conexão

O propósito do procedimento de estabelecimento de conexão é estabelecer uma conexão entre aplicações em dois dispositivos Bluetooth.

Estabelecimento de conexões adicionais

Quando um dispositivo Bluetooth estabeleceu uma conexão com outro dispositivo Bluetooth, ele pode estar disponível para o estabelecimento de:

- uma segunda conexão no mesmo canal, e/ou
- um segundo canal no mesmo enlace e/ou
- um segundo enlace físico.

3.2.2. Recurso de Serviço de Descobrimento (SDAP)

Espera-se que a quantidade de serviços fornecidos em conexões Bluetooth cresça de forma surpreendente. Portanto, procedimentos devem ser estabelecidos para auxiliar o usuário de um dispositivo Bluetooth a pesquisar uma variedade cada vez maior de serviços disponíveis. Mesmo que muitos serviços Bluetooth ainda possam ser desenvolvidos, é possível estabelecer um procedimento padrão para localizar e identificar serviços.

A pilha de protocolos Bluetooth contem um protocolo de descobrimento de serviços ("Service Discovery Protocol" – SDP) que é usado para localizar serviços disponíveis em (ou via) dispositivos na vizinhança de um dispositivo Bluetooth. Após a identificação dos serviços disponíveis em um dispositivo, o usuário pode optar por utilizar um ou mais deles. O SDAP ("Service Discovery Application Profile") define os protocolos e procedimentos que devem ser usados por uma aplicação de descobrimento para localizar serviços em outra unidade Bluetooth através do protocolo de descobrimento de serviços (SDP).

O SDP provês suporte para os seguintes tipos de pesquisa de serviços:

- busca de serviços por classe de serviços;
- busca de serviços por atributos de serviços e
- pesquisa de serviços.

Os primeiros dois casos representam a busca por serviços conhecidos e específicos. Eles fornecem respostas para perguntas do tipo: "O serviço A, ou o serviço A com as características B e C, está disponível?". O último caso representa uma busca genérica de serviços e fornece respostas para perguntas do tipo: "Quais serviços estão disponíveis?" ou "Quais serviços do tipo A estão disponíveis?".

3.2.3. Recurso de Comunicação Interna

Este recurso define os protocolos e procedimentos que serão utilizados pelos dispositivos para implementação da Comunicação Interna do aplicativo Telefone 3 em 1. O Telefone 3 em 1 é uma solução para prover um modo extra de operação para os telefones celulares, usando o Bluetooth para acessar os serviços da rede de telefonia fixa, através de uma estação base. O recurso de Comunicação Interna depende apenas do recurso de Acesso Genérico.

A figura abaixo apresenta a configuração típica dos dispositivos, onde o recurso de Comunicação Interna é aplicado.

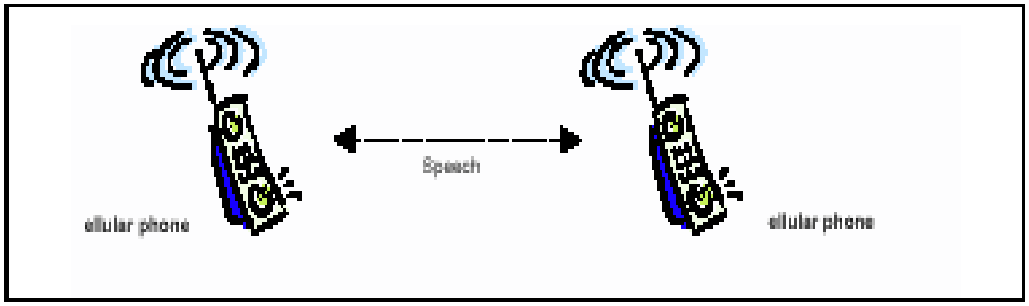

Fig. 4 – Recurso de Comunicação Interna - Exemplo

Como aplicação de Comunicação Interna é simétrica, os dispositivos que suportam este recurso são definidos como terminais (TL).

Neste caso, os cenários alvos são aqueles onde a conexão direta de voz é necessária entre 2 dispositivos (telefone, computador, etc.), baseado na utilização de sinalização telefônica. O cenário típico é o seguinte:

- 2 usuários de telefones celulares ocupados numa ligação de voz, numa conexão direta telefone-a-telefone usando apenas Bluetooth.

Princípio de Funcionamento

Aqui está descrito um breve resumo das interações que acontecem quando um terminal quer estabelecer uma comunicação interna com outro terminal. Na descrição abaixo, os termos "iniciador" (lado A) e "receptor" (lado B) serão utilizados para estabelecer o sentido da ligação.

1. Se o iniciador da comunicação interna não tem o endereço Bluetooth do receptor, ele terá que obtê-lo, por exemplo usando o procedimento de Descobrimento de Dispositivo do recurso de Acesso Genérico.

2. Este recurso não tem um modo de segurança particular. Se os dispositivos dos usuários (iniciador ou receptor) quiserem ter segurança na execução deste recurso, o procedimento de autenticação tem que ser executado afim de criar uma conexão segura.

3. O iniciador estabelece uma conexão e um canal CO do protocolo L2CAP. Agora, baseado nos requerimentos de segurança pretendidos pelos usuários dos 2 dispositivos, o processo de autenticação pode ser executado e a criptografia pode ser habilitada.

4. A comunicação interna é estabelecida.

5. Depois da ligação ter terminado, o canal e a conexão são liberados.

3.2.4. Recurso Telefone Sem Fio

Este recurso define os protocolos e os procedimentos que serão utilizados pelos dispositivos para implementação do aplicativo Telefone 3 em 1. O escopo deste recurso inclui os seguintes protocolos/recursos: banda base, LMP, L2CAP, SDP, TCS e recurso de Acesso Genérico.

O Telefone 3 em 1 é uma solução para prover um modo extra de operação para os telefones celulares, usando o Bluetooth para acessar os serviços da rede de telefonia fixa, através de uma estação base. Contudo, o Telefone 3 em 1 também pode ser aplicado em telefones sem fio residenciais ou comercias. Este aplicativo inclui fazer chamadas, via estação base, entre 2 terminais e acessar serviços adicionais providos por uma rede externa.

A estrutura de recursos e suas dependências são mostradas na Fig.2 deste documento. Um recurso é dependente de um outro recurso, quando ele reutiliza partes diretamente ou indiretamente deste outro recurso. Como pode ser visto na figura, o recurso Telefone Sem Fio é dependente apenas do recurso de Acesso Genérico.

As seguintes 2 terminologias/funções são definidas neste recurso:

- Gateway (GW) – atua como um ponto terminal pelo ponto de vista da rede externa. Agora, com relação às chamadas externas, ele é um ponto central, pois lida com toda requisição de chamada destinada ou originada pela rede externa. Com respeito ao recurso de Telefone Sem Fio, o GW tem a funcionalidade de suportar múltiplos terminais sendo ativados um por vez. Com isso ele não suporta múltiplas chamadas ativas ou serviço envolvendo mais de um terminal simultaneamente.
- Terminal (TL) – é o terminal sem fio do usuário, que pode ser um telefone sem fio, um telefone celular/sem fio ou um PC.

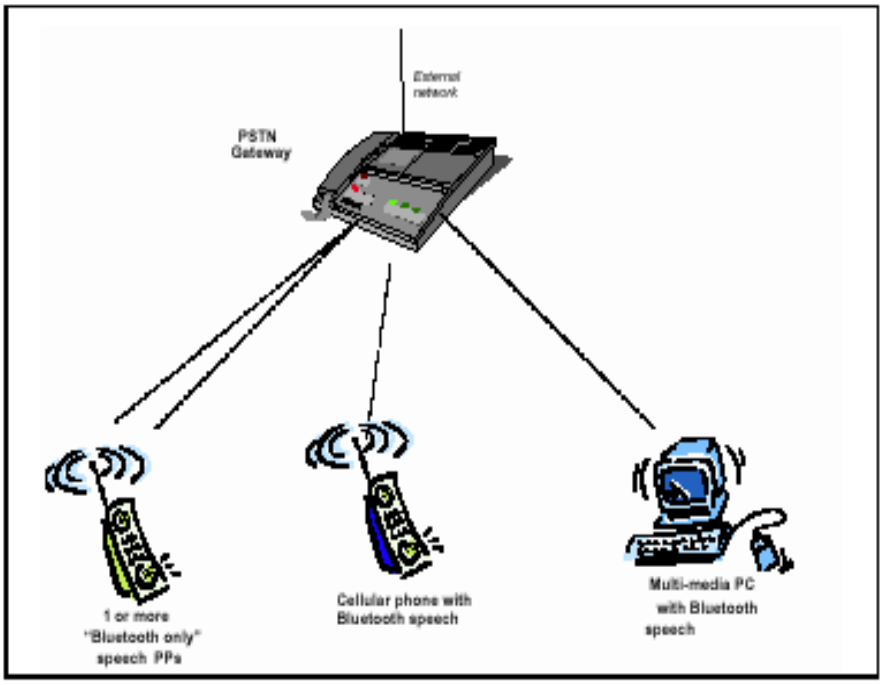

Fig. 5 – Configuração de sistema, exemplo

Alguns cenários:

1. Fazer chamadas do TL para um usuário da rede com a qual o GW está conectado.

2. Receber chamadas da rede em que o GW está conectado.

3. Fazer chamadas diretas entre 2 terminais

4. Utilizar serviço adicionais providos pela rede externa através de sinalização DTMF.

Princípio de Funcionamento

O GW normalmente é o mestre dentro da piconet do recurso de Telefone Sem Fio. Como mestre, ele controla o modo de potência do TLs e pode enviar informações via broadcast para os TLs.

O TL que está fora de alcance do GW procura periodicamente por ele, na tentativa de se conectar. O GW tem que dedicar o máximo de sua capacidade livre para procurar chamadas de conexão, com a finalidade de permitir que os TLs que entram dentro da piconet possam ser

encontrados o mais rápido possível. Este cenário minimiza a "poluição aérea" e apresenta um tempo razoável de acesso ao GW.

Quando o TL tem sucesso na conexão ao GW, a chave mestre/escravo tem que mudar, visto que o GW será sempre mestre. O canal CO e possivelmente o canal CL do protocolo L2CAP são estabelecidos para utilizar a sinalização TCS durante a sessão Telefone Sem Fio.

O TL que está dentro do alcance do GW, normalmente está no modo de espera, quando não tem nenhuma chamada. Este modo é eficiente no consumo de energia e permite receber informações de broadcast e realizar setup de chamadas. Agora, quando chega uma chamada ou o TL quer fazer uma chamada, o GW precisa colocá-lo no modo ativo. O canal L2CAP então será usado para sinalização TCS. Para segurança, a autenticação é usada tanto no lado do cliente como no GW, sendo que todos os dados são criptografados.

3.2.5. Recurso de Porta Serial

O recurso de porta serial define os protocolos e procedimentos que devem ser usados por dispositivos que utilizem o Bluetooth para emulação de cabo serial RS-232 (ou similar). A figura 4 ilustra os protocolos e entidades usadas nesse recurso.

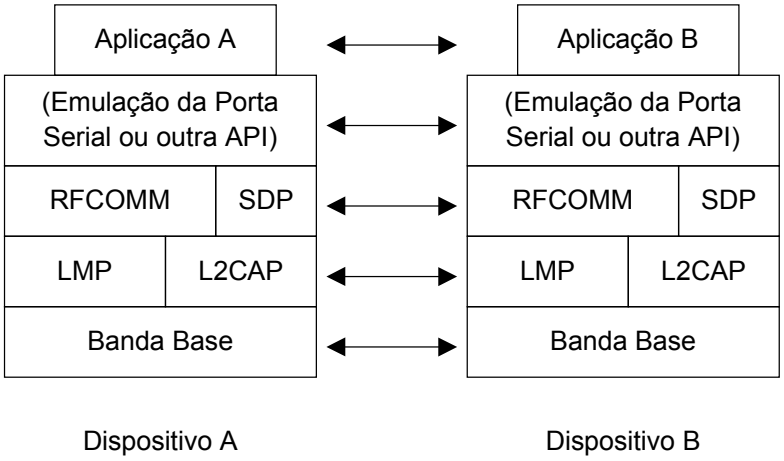

Fig. 6 – Modelo de protocolo

Banda base, LMP e L2CAP são os protocolos Bluetooth correspondentes às camadas 1 e 2 do modelo OSI. RFCOMM é a adaptação feita no Bluetooth da GSM TS 07.10, fornecendo um protocolo de transporte para a emulação de porta serial. A camada de emulação de porta mostrada na figura 4 é a entidade emulando uma porta serial, ou fornecendo uma API para aplicações.

O recurso de porta serial requer suporte para o uso apenas de pacotes simples (que utilizam apenas um intervalo de tempo). Isto significa que o recurso garante taxas de até 128 kbps. Taxas maiores são opcionais.

O recurso de porta serial lida com apenas uma conexão de cada vez. Consequentemente, somente conexões ponto-a-ponto são consideradas. No entanto, múltiplas execuções deste recurso podem ser executadas paralelamente no mesmo dispositivo.

O recurso de porta serial é executado sobre o recurso de acesso genérico (GAP).

3.2.6. Recurso de Rede Via Dial-Up

Este recurso define os protocolos e procedimentos que serão utilizados pelos dispositivos para implementação do aplicativo chamado Internet Bridge. Os exemplos mais comuns de dispositivos são modems e telefones celulares.

A figura baixo apresenta os protocolos e entidades utilizadas.

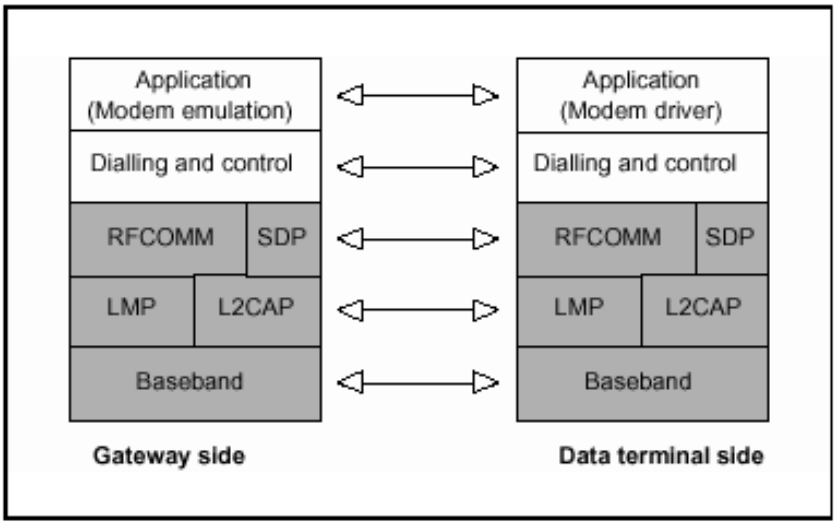

Fig. 7 – Modelo de protocolo do recurso de rede dial-up

Os protocolos Banda base, LMP, L2CAP correspondem as camadas 1 e 2 do modelo OSI. O protocolo RFCOMM está numa camada de adaptação, sendo utilizado para emular uma porta serial. O SDP é o protocolo usado para descobrir serviços. A Discagem e Controle são comandos e procedimentos usados para discagem e controle automático sobre a conexão serial assíncrona fornecida pelas camadas inferiores.

A camada de aplicação tem a função de emular um modem no lado do gateway, enquanto que no lado do terminal de dados existe o software de driver do modem.

As seguintes 2 terminologias/funções são definidas neste recurso:

- Gateway (GW) – este é o dispositivo que fornece acesso à rede pública (DCE). Os dispositivos atuando como gateways são tipicamente telefones celulares e modems.
- Terminal de Dados (DT) – este é o dispositivo que utiliza os serviço dial-up do gateway (DTE). Os dispositivos atuando como terminais de dados são tipicamente laptops e desktops.

Os cenários cobertos por este recurso são os seguintes:

- Uso do telefone celular ou modem (GW) pelo computador (DT) como modem sem fio para conexão a um servidor de internet via acesso discado dial-up.
- Uso do telefone celular ou modem (GW) pelo computador (DT) para receber dados.

Seguem abaixo algumas restrições:

- Este recurso suporta apenas um slot no pacote, isto significa que ele garante uma taxa de 128kbps para transferência de dados. Suporte para taxas mais altas é opcional.
- Apenas 1 chamada por vez é suportada.
- O recurso apenas suporta configurações ponto-a-ponto.

Princípio de Funcionamento

Antes que o DT possa utilizar os serviços do GW pela primeira vez, os 2 dispositivos devem ser inicializados. A iniciação inclui troca dos código PIN, criação de chaves de conexão e descobrimento de serviços.

A conexão tem que ser estabelecida, antes que a chamada possa ser inicializada ou recebida. Isto requer troca de mensagem com o outro dispositivo. O estabelecimento da conexão é sempre iniciado pelo DT.

Não existem regras de mestre/escravo.

O GW e DT fornecem um emulador de porta serial. Para este emulador é utilizado o recurso Porta Serial, sendo que o mesmo é usado para transportar dados do usuário, sinalização de controle do modem e comando AT entre o GW e DT. Os comando AT são analisados pelo GW e as respostas são emitida para o DT.

A conexão SCO ("Synchronous Connection Oriented" – ver seção 3.4.1) é utilizada para transporte de áudio.

Os mecanismos de autenticação e criptografia da banda base e LMP são utilizados, para propósitos de segurança, sendo que todos os dados do usuário são criptografados.

3.2.7. Recurso de Fax

Este recurso define os protocolos e os procedimentos que serão utilizados pelos dispositivos para implementação do aplicativo fax. O telefone celular ou modem Bluetooth podem ser, através de um computador, um modem-fax sem fio para enviar e receber mensagens.

O recurso de Fax depende do recurso de Porta Serial e de Acesso Genérico, conforme indicado na figura 2. Os protocolos, entidades e terminologia utilizadas são os mesmo usados no recurso de Rede via Dial-up.

A figura baixo apresenta os protocolos e entidades utilizadas.

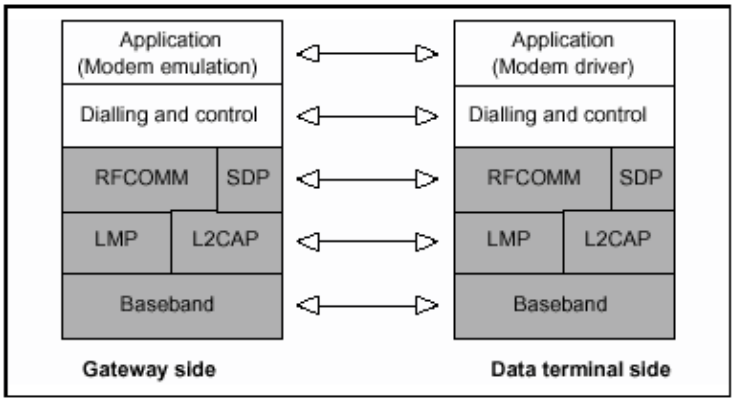

Fig. 8 – Modelo de protocolo do recurso de fax

Os protocolos banda base, LMP, L2CAP correspondem às camadas 1 e 2 do modelo OSI. O protocolo RFCOMM está numa camada de adaptação, sendo utilizado para emular uma porta serial. O SDP é o protocolo usado para descobrir serviços. A Discagem e Controle são comandos e procedimentos usados para discagem e controle automático sobre a conexão serial assíncrona fornecida pelas camadas inferiores.

A camada de aplicação tem a função de emular um modem no lado do gateway, enquanto que no lado do terminal de dados existe o software de driver do modem.

As seguintes 2 terminologias/funções são definidas neste recurso:

- Gateway (GW) – este é o dispositivo que fornece acesso a rede pública (DCE). Os dispositivos atuando como gateways são tipicamente telefones celulares e modems.
- Terminal de Dados (DT) – este é o dispositivo que utiliza os serviço dial-up do gateway (DTE). Os dispositivos atuando como terminais de dados são tipicamente laptops e desktops.

O cenário para este recurso é:

- Uso do telefone celular ou modem (GW) pelo computador (DT) como modem sem fio para enviar e receber mensagens de fax.

Seguem abaixo algumas restrições:

- Este recurso suporta apenas um slot no pacote, isto significa que ele garante uma taxa de 128kbps para transferência de dados. Suporte para taxas mais altas é opcional.
- Apenas 1 chamada por vez é suportada.
- O recurso apenas suporta configurações ponto-a-ponto.

Princípio de Funcionamento

Aqui está descrito um breve resumo das interações que acontece quando um terminal (DT) quer utilizar os serviços de fax do modem (GW).

1. Se o DT não tem o endereço Bluetooth do GW, ele terá que obtê-lo, por exemplo usando o procedimento de Descobrimento de Dispositivo do recurso de Acesso Genérico.

2. Este recurso ordena a utilização de uma conexão segura. Com isso os mecanismos de autenticação e criptografia da banda base e LMP são utilizados, para propósitos de segurança, sendo que todos os dados do usuário são criptografados.

3. O estabelecimento da conexão é sempre iniciado pelo DT.

4. Não existem regras de mestre/escravo.

5. A chamada de fax é estabelecida.

6. O GW e DT fornecem um emulador de porta serial. Para este emulador é utilizado o recurso Porta Serial, sendo que o mesmo é usado para transportar dados do usuário, sinalização de controle do modem e comando AT entre o GW w DT. Os comando AT são analisados pelo GW e as respostas são emitida para o DT.

7. Uma conexão SCO opcional pode ser usada para transportar o retorno de áudio do fax.

8. Depois da chamada de fax ter terminado, o canal e a conexão são liberados.

3.2.8. Recurso de Fone de Ouvido

O recurso de fone de ouvido ("headset") define os protocolos e procedimentos que devem ser usados por dispositivos que implementem o modelo chamado "Ultimate Headset". Os exemplos mais comuns de tais dispositivos são fones de ouvido, computadores pessoais e telefones celulares.

O headset pode ser conectado via interface aérea com o objetivo de atuar como mecanismo de entrada e saída de áudio do dispositivo Bluetooth, fornecendo áudio full duplex. O headset garante mobilidade ao usuário enquanto mantém a privacidade das chamadas.

O recurso de headset depende tanto do recurso de porta serial como do recurso de acesso genérico (GAP), como ilustra a figura 2.

A figura 9 apresenta os protocolos e entidades utilizadas neste recurso:

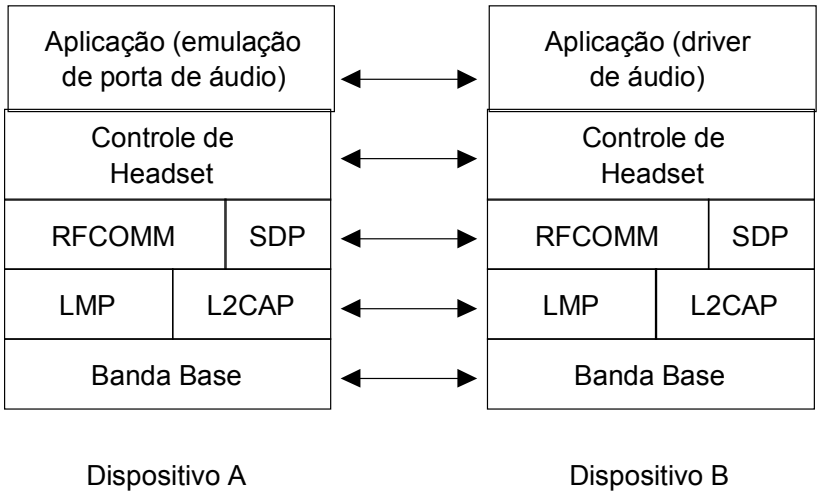

Fig. 9 – Modelo de protocolo

Controle de Headset é a entidade responsável pela sinalização de controle específica de headset; esta sinalização é baseada em comandos AT.

Embora não mostrado pela figura 9, assume-se que o Controle de Headset tenha acesso a algum procedimento de camadas baixas (como o estabelecimento de conexão síncrona SCO).

A camada de emulação de porta de áudio é a entidade que emula a porta de áudio no telefone celular ou PC, e o driver de áudio é o software de áudio no fone de ouvido.

Requerimentos de usuário e cenários

As seguintes condições se aplicam a este recurso:

- assume-se que o modelo de uso "Ultimate Headset" seja o único modelo ativo entre os dois dispositivos;
- somente uma única conexão de áudio é permitida por vez entre o fone de ouvido e o gateway de áudio;
- o gateway de áudio controla o estabelecimento e o término da conexão SCO. O fone de ouvido conecta (ou desliga) o fluxo de áudio interno após o estabelecimento (ou término) da conexão SCO. Uma vez estabelecida a conexão SCO, a transmissão de voz é feita nos dois sentidos;

- o recurso oferece somente interoperabilidade básica – o gerenciamento de múltiplas chamadas no gateway de áudio, por exemplo, não está incluído;
- a única suposição na interface de usuário do fone de ouvido é a possibilidade de detecção de uma ação iniciada pelo usuário (ex.: pressionar um botão).

3.2.9. Recurso de Acesso a LAN

O recurso de acesso a LAN ("LAN Access Profile") consiste de duas partes. Primeiramente, o recurso define como dispositivos Bluetooth podem ter acesso a serviços de uma LAN usando o PPP. Em segundo lugar, ele mostra como os mesmos mecanismos do PPP são usados para formar uma rede de dois dispositivos Bluetooth.

Dispositivos Bluetooth podem desempenhar dois papéis neste recurso: ponto de acesso LAN ("LAN Access Point" – LAP) e terminal de dados ("Data Terminal" – DT). O LAP é o dispositivo Bluetooth que provê acesso a uma LAN. O LAP provê os serviços de um servidor PPP. A conexão PPP é realizada sobre o protocolo RFCOMM. O RFCOMM é utilizado para transporte dos pacotes PPP e também pode ser usado para controle de fluxo dos dados PPP. O terminal de dados, DT, é o dispositivo que usa os serviços do LAP. Dispositivos típicos que atuam como DT's são notebooks, PC's e PDA's. O DT é um cliente PPP. Ele forma uma conexão PPP com um LAP para obter acesso a uma LAN.

O recurso de acesso a LAN define como uma rede PPP pode ser estabelecida nas seguintes situações:

- acesso a LAN para um único dispositivo Bluetooth – Neste cenário, um único DT usa o LAP como um meio de se conectar a uma LAN via interface aérea. Uma vez conectado, o DT irá operar como se estivesse conectado à LAN via conexão dial-up. O DT tem acesso a todos os serviços fornecidos pela LAN;
- acesso a LAN para múltiplos dispositivos Bluetooth – Neste cenário, múltiplos DT's usam o LAP como um meio para se conectar a uma LAN via interface aérea. Uma vez conectados, os DT's operarão como se estivessem conectados à LAN via conexão dial-up. Os DT's têm acesso a todos os serviços fornecidos pela LAN. Eles também podem comunicar-se entre si através do LAP;
- PC para PC (usando uma rede PPP sobre emulação de cabo serial) – Aqui, dois dispositivos Bluetooth podem estabelecer uma conexão simples entre si. Isso é similar a uma conexão

direta via cabo normalmente usada para conectar dois PC's. Neste cenário, um dos dispositivos faz o papel de LAP, e o outro é o DT.

3.2.10. Recurso de Troca de Objeto Genérico (GOEP)

O recurso GOEP ("Generic Object Exchange Profile") define o conjunto de protocolos e procedimentos a serem utilizados pelos aplicativos que lidam com a troca de objetos. Alguns aplicativos, descritos no capítulo de Aplicativos Bluetooth, são baseados neste recurso, por exemplo os aplicativos de transferência de arquivo e sincronização. Unidades típicas Bluetooth usando este recurso são notebook, PDA's, celulares, etc..

Aplicações usando o GOEP assumem que enlaces e canais são estabelecidos como definido pelo Protocolo de Acesso Genérico ("Generic Access Protocol" – GAP). O GOEP descreve o procedimento para enviar e receber dados de uma unidade Bluetooth para outra. O GOEP é dependente do Recurso de Porta Serial.

As seguintes funções são definidas para este recurso:

- Servidor – este é o dispositivo que provê um servidor de troca de objetos para e de onde objetos de dados podem ser "pushed" and "pulled", respectivamente;
- Cliente – este é o dispositivo que pode realizar as operações de "push" e/ou "pull" para e do servidor.

Os cenários previstos por este recurso são os seguintes:

- uso de um servidor por um cliente para realizar a operação de "push" de objeto(s) de dados;
- uso de um servidor por um cliente para realizar a operação de "pull" de objeto(s) de dados.

Algumas restrições se aplicam a este recurso. Por exemplo, somente configurações ponto-a-ponto são permitidas, e a interação do usuário é requerida para colocar o servidor no modo inicial.

3.2.11. Recurso de Transferência de Arquivos

Este recurso define os requerimentos de protocolos e procedimentos que serão utilizados pela aplicação de Transferência de Arquivos. Este recurso faz uso do recurso de Troca de Objeto Genérico (GOEP) para definir os requerimentos de interoperabilidade dos protocolos necessários

pela aplicação. Os dispositivos mais comuns utilizados nesta aplicação podem ser notebook, PDAs e PCs.

O recurso de Transferência de Arquivos depende dos recursos de Troca de Objeto Genérico (GOEP), Porta Serial e Acesso Genérico, conforme figura 2.

A figura baixo apresenta os protocolos e entidades utilizadas.

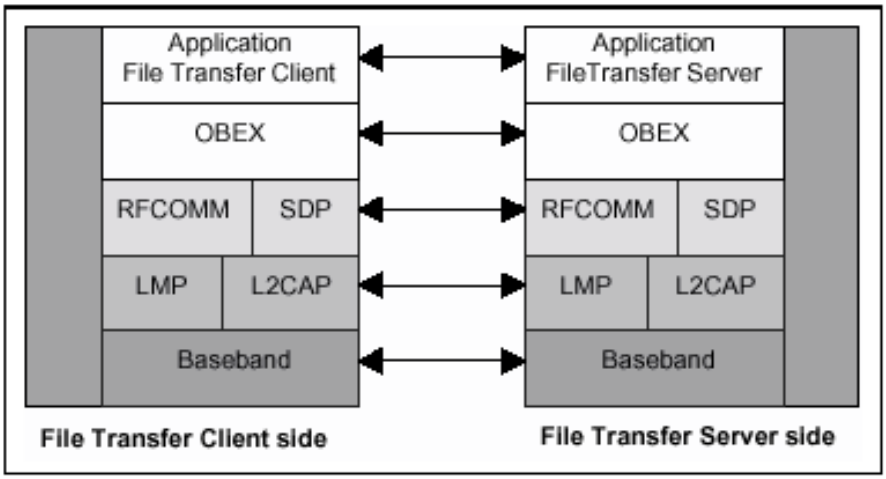

Fig. 10 – Modelo de protocolo do recurso de transferência de arquivos

Os protocolos banda base, LMP, L2CAP correspondem as camadas 1 e 2 do modelo OSI. O protocolo RFCOMM é o protocolo de adaptação para GSM. O SDP é o protocolo usado para descobrir serviços. O OBEX é o protocolo de adaptação para IrOBEX.

As seguintes 2 terminologias/funções são definidas neste recurso:

- Cliente – o dispositivo Cliente inicializa a operação de enviar e pegar objetos do Servidor.
- Servidor – o dispositivo Servidor é o dispositivo remoto alvo que fornece a funcionalidade de trocar objetos e capacidade de procurar diretórios.

Os cenários para este recurso são os seguintes:

- Uso de um dispositivo Bluetooth, por exemplo um notebook, para procurar arquivos armazenados em outro dispositivo Bluetooth. A procura envolve olhar objetos (arquivos e diretórios) e navegar na estrutura de diretórios de um outro dispositivo Bluetooth. Por exemplo, um PC procurando um arquivo de sistema em outro PC.

- Um segundo uso é transferir objetos (arquivos e diretórios) entre 2 dispositivos Bluetooth (Cliente para Servidor). Por exemplo, copiar arquivos de um PC para o outro. Servidores podem permitir arquivos e diretórios apenas como leitura, o que significaria uma restrição para enviar objetos.
- O terceiro uso de um dispositivo Bluetooth (Cliente) é pode manipular objetos (arquivos e diretórios) de um outro dispositivo Bluetooth (Servidor). Isto inclui apagar objetos e criar novos diretórios. Os Servidores podem restringir que arquivos/diretórios possam ser apagados ou criados, através da opção somente como leitura.

Seguem abaixo algumas restrições:

- Para o dispositivo que assume a função de Servidor, o usuário é responsável por deixá-lo no modo em que seja possível o seu descobrimento e conexão. Isto deve ocorre antes dos procedimentos de solicitação e estabelecimento da conexão, que são processadas pelo Cliente.
- O recurso apenas suporta a configuração ponto-a-ponto. Com isso, o Servidor pode oferecer serviço apenas para um Cliente por vez.

Princípio de Funcionamento

1. Antes que o Servidor possa ser utilizado pelo Cliente pela primeira vez; o procedimento de contato, incluindo o alinhamento, deve ser executado. Este procedimento deve ser suportado, porém seu uso depende dos recursos de aplicação. O procedimento de contato tipicamente envolve a troca dos códigos PIN e criação de chaves de conexão.

2. Em complemento, o procedimento de iniciação do OBEX deve ser executado antes do Cliente utilizar o Servidor pela primeira vez.

3. Segurança pode ser fornecida através de autenticação da conexão e criptografia de todos os dados do cliente,

4. O estabelecimento do canal e da conexão deve ser realizado de acordo com os procedimentos definidos no recurso de Acesso Genérico (GAP).

5. Não existe regra de mestre/escravo.

6. Este recurso não necessita modo de baixa potência para ser utilizado.

3.2.12. Recurso de Envio de Objeto

Este recurso define os requerimentos de protocolos e procedimentos que serão utilizados pela aplicação de Envio de Objeto. Este recurso faz uso do recurso de Troca de Objeto Genérico (GOEP) para definir os requerimentos de interoperabilidade dos protocolos necessários pela aplicação. Os dispositivos mais comuns utilizados nesta aplicação podem ser notebook, PDAs e telefones móveis.

O recurso de Envio de Objeto depende dos recursos de Troca de Objeto Genérico (GOEP), Porta Serial e Acesso Genérico, conforme figura 2.

A figura baixo apresenta os protocolos e entidades utilizadas.

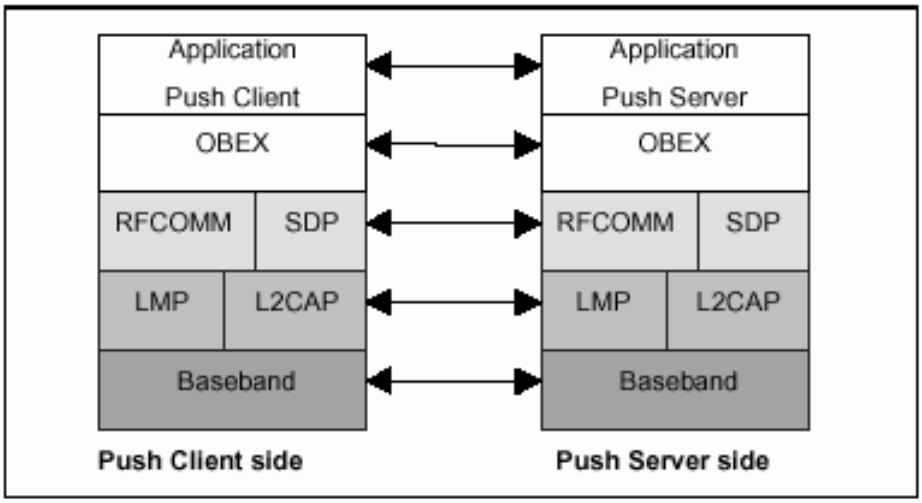

Fig. 11 – Modelo de protocolo de recurso de envio de objeto

Os protocolos Banda base, LMP, L2CAP correspondem as camadas 1 e 2 do modelo OSI. O protocolo RFCOMM é o protocolo de adaptação para GSM. O SDP é o protocolo usado para descobrir serviços. O OBEX é a protocolo de adaptação para IrOBEX.

As seguintes 2 terminologias/funções são definidas neste recurso:

- Servidor Push – este é o dispositivo que atua como servidor para a troca de objetos.
- Cliente Push – este é o dispositivo cliente que envia e pega objetos do Servidor Push.

Os cenários para este recurso são os seguintes:

- Uso de um dispositivo Bluetooth (Cliente Push), por exemplo um telefone móvel, para enviar um objeto para caixa de entrada de um outro dispositivo Bluetooth (Servidor Push). O objeto pode ser um cartão de negócios ou um agendamento.
- Uso de um dispositivo Bluetooth (Cliente Push), por exemplo um telefone móvel, para pegar um cartão de negócios de um outro dispositivo Bluetooth (Servidor Push).
- Uso de um dispositivo Bluetooth (Cliente Push), por exemplo um telefone móvel, para trocar cartões de negócios com um outro dispositivo Bluetooth (Servidor Push).

Seguem abaixo algumas restrições:

- Para o dispositivo que assume a função de Servidor, o usuário é responsável por deixá-lo no modo em que seja possível o seu descobrimento e conexão. Isto deve ocorrer antes dos procedimentos de solicitação e estabelecimento da conexão, que são processados pelo Cliente.
- O recurso apenas suporta a configuração ponto-a-ponto. Com isso, o Servidor pode oferecer serviço apenas para um Cliente por vez.

Princípio de Funcionamento

1. Antes que o Servidor possa se utilizado pelo Cliente pela primeira vez; o procedimento de contato, incluindo o alinhamento, deve ser executado. Este procedimento deve ser suportado, porém seu uso depende dos recursos de aplicação. O procedimento de contato tipicamente envolve a troca dos códigos PIN e criação de chaves de conexão.

2. Em complemento, o procedimento de iniciação do OBEX deve ser executado antes do Cliente utilizar o Servidor pela primeira vez.

3. Segurança pode ser fornecida através de autenticação da conexão e criptografia de todos os dados do cliente,

4. O estabelecimento do canal e da conexão deve ser realizado de acordo com os procedimentos definidos no recurso de Acesso Genérico (GAP).

5. Não existe regra de mestre/escravo.

6. Este recurso não necessita modo de baixa potência para ser utilizado.

Seguem abaixo alguns objetos que utilizam este recurso:

- Cartão de Negócios – usa o formato vCard 2.1
- Agenda Telefônica – usa o formato vCard 2.1
- Calendário – usa o formato vCalendar 1.0
- Mensagens – usa o formato vMessage
- Notas – usa o formato vNote

3.2.13. Recurso de Sincronização

Este recurso define os requerimentos para os protocolos e procedimentos que devem ser usados pelas aplicações que fornecem o modelo de usuário de sincronização. O modelo de usuário de sincronização utiliza o GOEP para definir condições de interoperabilidade para os protocolos necessários por aplicações. Típicos cenários previstos por este recurso incluem um computador instruindo um telefone celular ou um PDA a trocar dados de PIM, ou vice versa (um celular instruindo um computador a trocar dados de PIM), ou automaticamente iniciando sincronização quando dois dispositivos Bluetooth entram no raio de alcance.

As seguintes funções são definidas para este recurso:

- Servidor IrMC – Este é o dispositivo servidor IrMC que provê um servidor de troca de objeto. Tipicamente, este dispositivo é um telefone celular ou um PDA. Além das condições de interoperabilidade definidas neste recurso, o servidor IrMC deve atender aos requerimentos de compatibilidade para o servidor GOEP, se nada em contrário for definido.
- Cliente IrMC – Este é o dispositivo cliente IrMC, que contém um "sync engine" e executa as funções de "pull" e "push" de dados PIM do e para o servidor IrMC. Tipicamente, o dispositivo cliente IrMC é um PC. Como o cliente IrMC também deve permitir o recebimento do comando de inicialização para sincronização, ele deve operar temporariamente como servidor às vezes. Além das condições de interoperabilidade definidas neste recurso, o servidor IrMC também deve atender aos requerimentos de compatibilidade para o servidor e cliente do GOEP, se nada for definido em contrário.

Os cenários previstos por este recurso são:

- Uso de um servidor IrMC por um cliente IrMC para executar a operação de “pull” de dados PIM necessários para ser sincronizado do servidor IrMC, para sincronizar estes dados com os dados no cliente IrMC, e para executar a operação de “push” destes dados sincronizados de volta para o servidor IrMC;
- Uso de um cliente IrMC por um servidor IrMC para iniciar o cenário anterior enviando um comando de sincronização para o cliente IrMC;
- Sincronização automática iniciada pelo cliente IrMC.

3.3. Aplicativos Bluetooth

Neste capítulo são descritos alguns aplicativos Bluetooth. Para cada aplicativo existe um ou mais recursos correspondentes, definindo camadas de protocolos e funções a serem usadas.

3.3.1. Transferência de Arquivo

Este aplicativo oferece a capacidade para transferência de objeto_dado de um dispositivo Bluetooth para o outro. Arquivos, pastas inteiras, diretórios e formatos de mídias são suportados por este aplicativo. O aplicativo também oferece a possibilidade de navegação pelo conteúdo das pastas de um dispositivo remoto. Além disso, as operações de enviar e receber são cobertas por este aplicativo, por exemplo, troca de cartão de negócios usando o formato Vcard. Este aplicativo é baseado no GOEP.

3.3.2. Internet Bridge

Este aplicativo descreve como um telefone móvel ou modem sem fio pode fornece ao PC a capacidade de discagem na rede, sem a necessidade de uma conexão física com o PC. Esse cenário de rede requer duas camadas de protocolos, uma para comandos AT para controlar o telefone móvel e outra para transferência de dados.

3.3.3. Acesso de LAN

Este aplicativo é similar ao aplicativo Internet Bridge. A diferença é que o aplicativo Acesso de LAN não utiliza o protocolo para comandos AT. O aplicativo descreve como terminais de dados

usam pontos de acesso da LAN como conexão sem fio com a rede local. Quando conectados, os terminais de dados operam como se eles estivessem conectados na LAN através de discagem dial-up.

3.3.4. Sincronização

Este aplicativo fornece o meio para sincronização automática entre, por exemplo, um PC de mesa, um PC portátil, um telefone móvel e um notebook. A sincronização requer que informações de cartão de negócio, calendário e tarefas sejam transferidas e processadas pelos computadores, telefones celulares e PDA's, utilizando um protocolo e um formato comum.

3.3.5. Telefone 3 em 1

Este aplicativo descreve como um telefone pode se conectar a três provedores que oferecem serviços diferentes. O telefone pode atuar como um telefone sem fio, conectando-se a uma rede de telefonia pública, sendo cobrada a tarifa de uma ligação através da linha fixa. O telefone também pode se conectar diretamente com outros telefones atuando como "walkie-talkie", sendo que neste caso não existe tarifa. Finalmente, o telefone pode atuar como um telefone celular, conectando-se com a infra-estrutura celular.

3.3.6. Fone de Ouvido

Este aplicativo define como um fone de ouvido Bluetooth sem fio pode ser conectado para atuar como uma unidade remota com interface de entrada e saída de áudio. Esta unidade é provavelmente um telefone móvel ou um PC para entrada e saída de áudio. Este aplicativo requer duas camadas de protocolos, uma para comandos AT para controlar o telefone móvel e outra para transferência de dados, isto é, voz. Os comandos AT controlam o telefone levando em conta o instante de chamada e término das ligações.

3.4. Protocolos Bluetooth

3.4.1. Banda Base

Descrição Geral

O Bluetooth opera na banda não licenciada ISM em 2.4 GHz. Um transceptor de salto em freqüência é usado para combater interferências e desvanecimentos. Uma modulação Gaussiana FSK binária é usada para minimizar a complexidade do transceptor. A taxa de símbolos é de 1 Ms/s (1 milhão de símbolos por segundo). Um canal intervalado é usado com duração nominal do intervalo de tempo de 625 μs. Para transmissão full-duplex, utiliza-se TDD ("time division duplex"). Informação é trocada no canal através de pacotes. Cada pacote é transmitido em uma freqüência diferente da série de saltos em freqüência. Um pacote geralmente utiliza somente um intervalo de tempo, mas pode ser estendido para utilizar até cinco intervalos.

O protocolo de banda base do Bluetooth é uma combinação de comutação por circuitos com comutação por pacotes. Slots podem ser reservados para pacotes síncronos. O Bluetooth pode oferecer um canal de dados assíncrono, até três canais síncronos de voz simultâneos, ou um canal que oferece simultaneamente dados assíncronos e voz síncrona. Cada canal de voz oferece um canal síncrono de voz a 64 kbps em cada direção. O canal assíncrono pode oferecer uma taxa máxima de 723.2 kbps assimétrico (com até 57.6 kbps na direção de retorno), ou 433.9 kbps simétrico.

O sistema Bluetooth consiste em uma unidade de rádio, uma unidade de controle de conexão e uma unidade de suporte para gerência de conexão e funções de interface do terminal host (ver figura 12). Esta seção descreve o controlador de conexão Bluetooth, que executa os protocolos de banda base e outras rotinas de conexão de baixo nível.

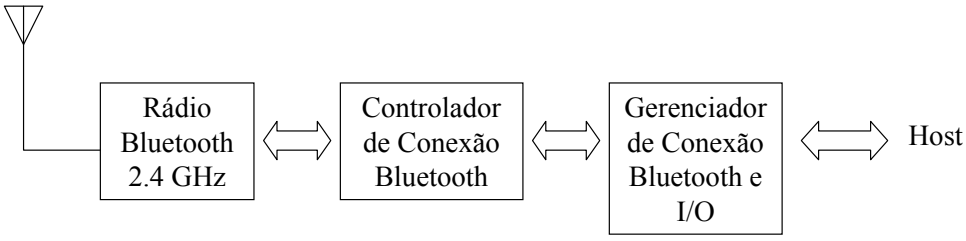

Fig. 12 – Blocos funcionais no sistema Bluetooth

O sistema Bluetooth provê conexões ponto-a-ponto (somente duas unidades envolvidas) ou conexões ponto-multiponto (ver figura 13). Na conexão ponto-multiponto, o canal é dividido entre várias unidades Bluetooth. Duas ou mais unidades dividindo o mesmo canal formam uma "piconet". Uma das unidades Bluetooth age como a mestre da piconet, enquanto todas as outras agem como escravas. Até sete escravos podem estar ativos em uma piconet. Além disso, várias outras unidades podem permanecer ligadas ao mestre em um estado denominado "parked". Os escravos que estão no estado parked não podem estar ativos no canal, mas permanecem sincronizados ao mestre. A unidade mestre controla o acesso ao canal tanto para escravos ativos como escravos no estado parked. Múltiplas piconets com áreas de cobertura sobrepostas formam uma "scatternet". Cada piconet pode ter somente um único mestre. Entretanto, escravos podem participar de diferentes piconets através de multiplexação TDM. Além disso, uma unidade mestre de uma piconet pode ser uma unidade escravo em outra piconet, como mostra a figura 13c. As piconets não podem ser sincronizadas em freqüência. Cada piconet tem seu próprio canal de salto em freqüência.

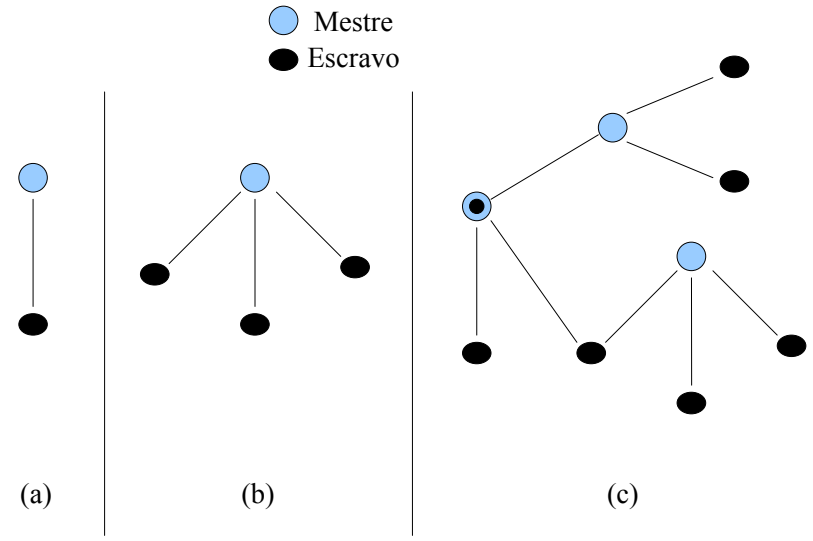

Fig. 13 – Modos de operação na Piconet

(a) operação com um único escravo

(b) operação multi-escravos e

(c) operação scatternet.

Canal Físico

O canal é representado por uma seqüência de saltos pseudo aleatória abrangendo os 79 ou 23 canais RF (ver seção 4.4). A seqüência de saltos é exclusiva para cada piconet e é determinada pelo endereço de dispositivo ("device address") Bluetooth da unidade mestre. A fase na seqüência de saltos é determinada pelo relógio Bluetooth da unidade mestre. O canal é dividido em intervalos de tempo onde cada intervalo corresponde a uma freqüência RF. Saltos consecutivos correspondem a diferentes freqüências. A taxa nominal de saltos é de 1600 saltos/s. Todas as unidades Bluetooth participantes da piconet se mantêm sincronizadas em tempo e em saltos ao canal.

Os intervalos de tempo do canal Bluetooth são numerados de acordo com o relógio Bluetooth da unidade mestre da piconet. A numeração vai de 0 até $2^{27} - 1$ e é cíclica, com um comprimento de ciclo de 2^{27}. Um esquema TDD é utilizado onde a unidade mestre e a unidade escravo transmitem alternadamente. A unidade mestre deve sempre iniciar sua transmissão em slots de numeração par, e uma unidade escravo somente deve iniciar uma transmissão em slots de numeração ímpar. O início da transmissão do pacote deve estar alinhado com o início do intervalo de tempo.

A freqüência de salto deve permanecer fixa durante a duração do pacote. Para um pacote simples (ocupando um único intervalo de tempo), a freqüência de salto é obtida do valor corrente do relógio Bluetooth. Para um pacote multi-slot (que ocupa mais de um intervalo de tempo), a freqüência de salto usada para o pacote inteiro é obtida do valor do relógio Bluetooth no primeiro intervalo de tempo do pacote. A freqüência de salto no primeiro intervalo de tempo após a transmissão de um pacote multi-slot é determinada pelo valor corrente do relógio Bluetooth.

Conexões Físicas

Dois tipos de conexão entre unidades mestre e unidades escravo foram definidos: Synchronous Connection Oriented, SCO, e Asynchronous Connectionless, ACL.

Conexão SCO

Uma conexão SCO é um enlace simétrico ponto-a-ponto entre a unidade mestre e uma única unidade escravo na piconet. O mestre mantém a conexão SCO utilizando slots reservados em intervalos regulares. Como a conexão SCO reserva slots, ela pode ser vista como uma conexão por comutação de circuitos entre a unidade mestre e a escravo. Conexões SCO tipicamente são

utilizadas para tráfego de voz. A unidade mestre pode oferecer até três conexões SCO para a mesma unidade escravo ou para diferentes unidades escravo. Uma unidade escravo pode realizar até 3 conexões SCO com o mesmo mestre, ou 2 conexões SCO se elas forem originadas de mestres diferentes. Pacotes SCO nunca são retransmitidos.

A unidade mestre envia pacotes SCO em intervalos regulares – chamados de intervalos SCO T_{SCO} (contado em intervalos de tempo) – para o escravo nos slots reservados de transmissão mestre-para-escravo. O escravo SCO pode sempre responder com um pacote SCO no slot escravo-para-mestre seguinte, a não ser que um escravo diferente tenha sido endereçado no slot mestre-para-escravo precedente.

A conexão SCO é estabelecida com o mestre enviando uma mensagem de set-up SCO através do protocolo LMP (descrito nas seções seguintes). Essa mensagem contem parâmetros de temporização como o intervalo T_{SCO} e o offset SCO (D_{SCO}) para especificar os slots reservados.

Conexão ACL

Nos slots não reservados para conexões SCO, a unidade mestre pode trocar pacotes com qualquer unidade escravo. A conexão ACL provê uma conexão comutada a pacotes entre a unidade mestre e todas as unidades escravo ativas na piconet. Tanto serviços assíncronos como isócronos são oferecidos. Somente uma conexão ACL pode existir entre um mestre e um escravo. Para a maioria dos pacotes ACL, a retransmissão é utilizada para assegurar a integridade dos dados.

Um escravo pode retornar um pacote ACL em um slot escravo-para-mestre se e somente se ele foi endereçado no slot mestre-para-escravo precedente. A unidade mestre controla a largura de faixa da conexão ACL e decide o quanto de largura de faixa uma unidade escravo pode usar na piconet.

Pacotes ACL não endereçados a um escravo em específico são considerados pacotes de difusão e são lidos por todos os escravos. Se não há informação para ser transmitida na conexão ACL e nenhuma sondagem (“polling”) é necessária, nenhuma transmissão deve ocorrer.

Formato Geral dos Pacotes Bluetooth

A ordenação de bits na definição de pacotes e mensagens da especificação de banda base do Bluetooth segue o formato “Little Endian”. Em outras palavras, as seguintes regras se aplicam:

- O bit menos significativo (LSB) corresponde a b_0;
- O LSB é o primeiro bit transmitido via interface aérea;
- Em ilustrações, o LSB é mostrado do lado esquerdo.

O formato geral dos pacotes Bluetooth é mostrado na figura 14. Cada pacote consiste de três entidades: o código de acesso, o cabeçalho e a carga útil. O código de acesso e o cabeçalho possuem tamanho fixo: 72 e 54 bits, respectivamente. A carga útil pode variar de 0 a um máximo de 2745 bits. Diferentes tipos de pacotes foram definidos. Pacotes podem consistir somente do código de acesso, do código de acesso e cabeçalho ou de todas as três entidades.

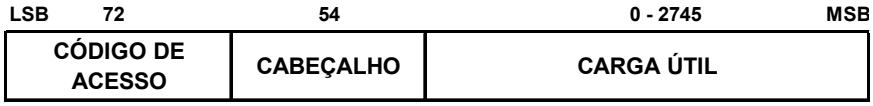

Fig. 14 – Formato padrão de pacote

Código de acesso

Cada pacote começa por um código de acesso. Se um cabeçalho de pacote se seguir ao código de acesso, o código tem 72 bits. Caso contrário, o código de acesso tem somente 68 bits de comprimento. O código de acesso é usado para sincronização, compensação de offset DC e identificação. O código de acesso identifica todos os pacotes trocados no canal da piconet: todos os pacotes enviados em uma mesma piconet possuem o mesmo código de acesso de canal.

O código de acesso também é usado em procedimentos de paging e consulta (“inquiry”). Neste caso, o próprio código de acesso é usado como mensagem de sinalização e nem o cabeçalho nem o campo de carga útil são usados.

São definidos três tipos diferentes de códigos de acesso:

- código de acesso ao canal (“channel access code” – CAC);
- código de acesso ao dispositivo (“device access code” – DAC);
- código de acesso de consulta (“inquiry access code” – IAC).

Os tipos de códigos de acesso são utilizados para uma unidade Bluetooth em diferentes modos de operação. O código de acesso ao canal identifica uma piconet. Este código é utilizado em todos os pacotes trocados em um canal de piconet. O código de acesso ao dispositivo é usado para

procedimentos especiais de sinalização, como por exemplo o paging e a resposta ao paging. Existem duas variações para o código de acesso de consulta. Um código geral de acesso de consulta ("general inquiry access code" – GIAC) é comum a todos os dispositivos. O GIAC pode ser usado para descobrir que outras unidades Bluetooth estão dentro do raio de alcance. O código dedicado de acesso de consulta ("dedicated inquiry access code" – DIAC) é comum a um grupo específico de unidades Bluetooth que possuem uma característica comum. O DIAC pode ser usado para descobrir quais dessas unidades Bluetooth com uma característica em comum estão dentro do raio de alcance.

Cabeçalho

O cabeçalho contem informações de controle de conexão e consiste de seis campos, como mostra a figura 7.

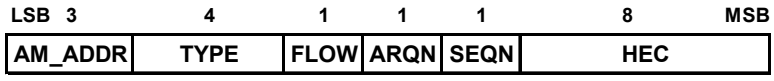

Fig. 15 – Formato do Cabeçalho

Os seis campos do cabeçalho totalizam 18 bits que recebem codificação FEC com taxa de 1/3, resultando em um cabeçalho de 54 bits. A função dos seis campos é explicada a seguir:

- ADM_ADDR: endereço de 3 bits usado para distinguir participantes ativos ("Active Members") em uma piconet;
- TYPE: código de 4 bits para distinguir os 16 diferentes tipos de pacotes; este código também informa o número de intervalos de tempo que o pacote irá ocupar.
- FLOW: 1 bit para controle de fluxo de pacotes em conexões ACL (FLOW = 0 indica que o buffer do receptor está cheio; FLOW = 1 indica que o buffer do receptor foi esvaziado);
- ARQN: 1 bit utilizado para indicar a fonte que houve sucesso na transferência de carga útil com CRC; ARQN = 1 (ACK) indica sucesso na transmissão; ARQN = 0 (NAK) indica o contrário;
- SEQN: 1 bit que provê um esquema de numeração seqüencial para ordenar a série de pacotes de dados; para cada novo pacote transmitido que contem dados com CRC, o bit SEQN é

invertido (com isso, pacotes retransmitidos erroneamente podem ser identificados e descartados);

- HEC: 8 bits de verificação da integridade do cabeçalho (“header error check”).

Carga Útil

Dois campos podem ser distinguidos na carga útil: o campo (síncrono) de voz e o campo (assíncrono) de dados. Pacotes ACL têm somente o campo de dados e pacotes SCO possuem somente o campo de voz – com exceção do pacote DV, um tipo de pacote SCO que possui os campos de voz e de dados.

O campo de voz tem um comprimento fixo, e não apresenta um cabeçalho de carga útil. O campo de dados consiste de três segmentos: um cabeçalho de carga útil, um corpo de carga útil e possivelmente um código CRC.

Tipos de Pacotes

Os pacotes utilizados em uma piconet estão relacionados à conexão física em que eles são utilizados. Até agora, dois tipos de conexões físicas estão definidas: a conexão SCO e a conexão ACL. Para cada uma dessas conexões, 12 tipos diferentes de pacotes podem ser definidos. Quatro pacotes de controle são comuns a todos os tipos de conexão: seu código TYPE é único, independente do tipo de conexão. Além deste quatro pacotes de controle, existe um pacote de identificação que também é comum a todos os tipos de conexão. Uma apresentação detalhada de cada tipo de pacote pode ser obtida em [1].

Correção de Erros

Existem três esquemas de correção de erros definidos para o Bluetooth:

- FEC com taxa de 1/3;
- FEC com taxa de 2/3
- Esquema ARQ para dados.

O propósito do esquema FEC na carga útil de dados é reduzir o número de retransmissões. Entretanto, em um ambiente que gere um número de erros razoavelmente pequeno, o FEC cria um overhead desnecessário que reduz a taxa líquida de transmissão. Em função disso, a

especificação do Bluetooth define alguns tipos de pacote que não fazem uso do FEC no campo de carga útil. O cabeçalho do pacote é sempre protegido com o FEC com taxa de 1/3, já que ele contem informações importantes de conexão e deve ser resistente a um número maior de erros.

Canais Lógicos

Cinco canais lógicos são definidos no sistema Bluetooth:

- canal de controle LC;
- canal de controle LM;
- canal de usuário UA;
- canal de usuário UI;
- canal de usuário US.

Os canais de controle LC e LM são usados nos níveis de controle de conexão e de gerência de conexão, respectivamente. Os canais de usuário UA, UI e US são usados para transportar informações de usuário assíncronas, isócronas e síncronas, respectivamente. O canal LC é levado no cabeçalho do pacote; todos os outros canais são levados no campo de carga útil do pacote. O canal US é levado apenas por conexões SCO; os canais UA e UI geralmente são levados por conexões ACL, mas também podem ser levados no pacote DV em uma conexão SCO. O canal LM pode ser levado tanto por conexões SCO como por conexões ACL.

Rotinas de Transmissão e Recepção

As rotinas de transmissão e de recepção são executadas separadamente para cada conexão ACL e SCO. As figuras 8 e 9 mostram os buffers ACL e SCO da forma como eles são usados nessas rotinas. Cada buffer consiste de dois registradores FIFO: um registrador “current” que pode ser acessado e lido pelo controlador de conexão Bluetooth para compor/ler os pacotes, e um registrado “next” que pode ser acessado pelo gerenciador de conexão do Bluetooth para carregar/descarregar novas informações. A posição das chaves S1 e S2 determinam qual registrador é “currrent” e qual registrador é “next”; as chaves são controladas pelo controlador de conexão Bluetooth. As chaves nunca podem estar conectadas ao mesmo registrador simultaneamente.

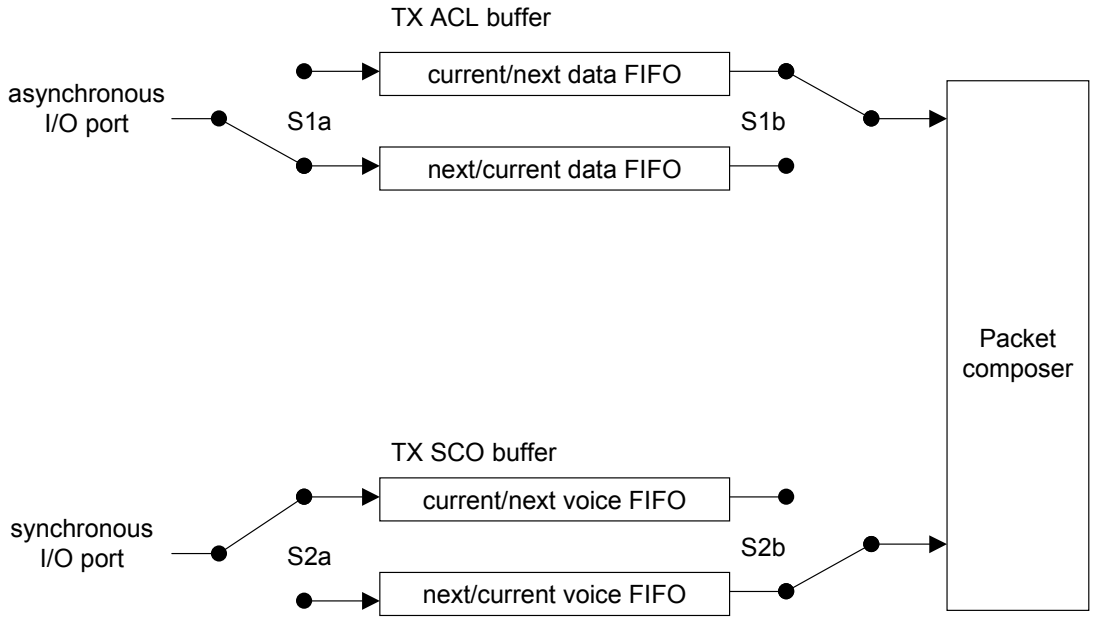

Fig. 16 – Diagrama funcional dos buffers de transmissão

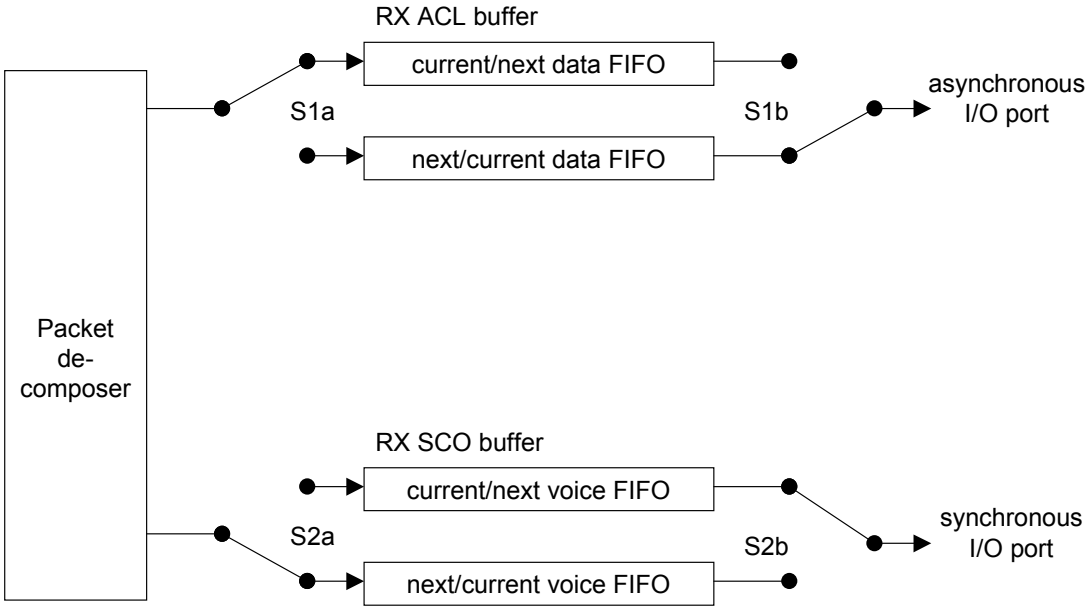

Fig. 17 – Diagrama funcional dos buffers de recepção

3.4.2. Interface de Controle do Host (HCI)

O HCI ("Host Controller Interface") provê uma interface de comando para o controlador de banda base e gerenciador de conexão, e acesso ao status de hardware e registradores de controle. Essencialmente, essa interface fornece um método uniforme de acessar as funcionalidades de banda base do Bluetooth. O HCI existe através de 3 seções: Host – camada de transporte – controlador de host. Cada uma dessas seções executa uma função diferente no sistema HCI.

Entidades Funcionais do HCI

O HCI é dividido, funcionalmente, em três partes:

- Firmware HCI – Localizado no controlador de host (o termo "controlador de host" significa o dispositivo Bluetooth habilitado para HCI). O firmware HCI executa os comandos HCI para o hardware do Bluetooth acessando comandos de banda base, comandos de gerenciador de conexão, registradores de status de hardware, registradores de controle, e registradores de evento.
- Driver HCI – Localizado no host (o termo "host" significa a unidade de software habilitada para HCI). O host recebe avisos assíncronos de eventos HCI – eventos HCI são usados para notificar o host da ocorrência de alguma coisa. Quando o host descobre a ocorrência de um evento, ele analisa o pacote de evento recebido para determinar qual evento ocorreu.
- Camada de transporte do controlador de host – O driver HCI e o Firmware HCI se comunicam através da camada de transporte do controlador de host, isto é, uma definição das várias camadas que podem existir entre o driver HCI no sistema do host e o firmware HCI no hardware Bluetooth. Essas camadas intermediárias (a camada de transporte do controlador de host) devem permitir a transmissão de dados sem um conhecimento detalhado dos dados que são transferidos. O host deve receber avisos assíncronos de eventos HCI independentemente da camada de transporte do controlador de host sendo usada.

Comandos HCI

O HCI provê um método uniforme de comando para acessar as funcionalidades do hardware Bluetooth. Os comandos de conexão HCI permitem que o host controle as conexões da camada de enlace para outros dispositivos Bluetooth. Estes comandos tipicamente requerem que o gerenciador de conexão troque comandos LMP com dispositivos Bluetooth remotos. Os "HCI

policy commands" são usados para afetar o comportamento dos gerenciadores de conexão local e remoto. Estes comandos fornecem ao host métodos para influenciar a forma como o gerenciador de conexão administra a piconet. Os "host controller and baseband commands", "informational commands" e "status commands" fornecem ao host acesso aos vários registradores no controlador de host.

3.4.3. Protocolo de Gerenciamento de Conexão (LMP)

O gerenciador de conexão ("Link Manager" – LM) executa set-up de conexão, autenticação, configuração de conexão e outros protocolos. Ele descobre outros gerenciadores de conexão e se comunica com eles através do protocolo de gerenciamento de conexão ("Link Manager Protocol"). Para exercer seu papel de provedor de serviços, o gerenciador de conexão utiliza os serviços do controlador de conexão ("Link Controller" – LC).

Mensagens LMP são transferidas no campo de carga útil em vez de no L2CAP, e são identificadas por um valor reservado no campo L_CH do cabeçalho do campo de carga útil. As mensagens são filtradas e interpretadas pelo gerenciador de conexão do dispositivo receptor e não são encaminhadas para camadas superiores.

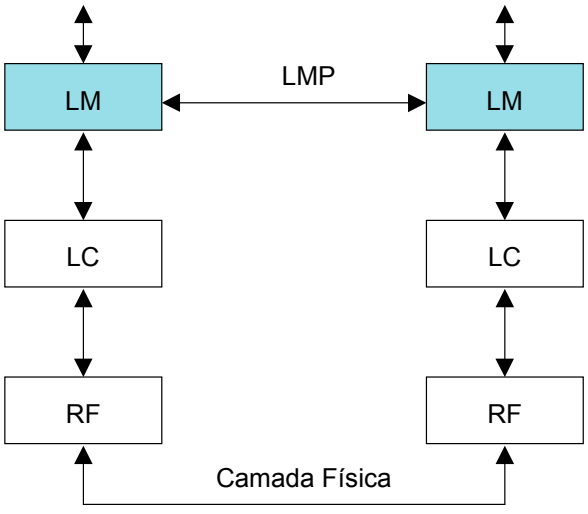

Fig. 18 – A posição do gerenciador de conexão no cenário global

Mensagens do gerenciador de conexão têm maior prioridade que dados de usuário. Isto significa que mensagens do gerenciador de conexão não sofrerão atraso provocado pelo tráfego L2CAP (elas podem sofrer atrasos, no entanto, provocados por muitas retransmissões de pacotes individuais de banda base).

O LMP consiste essencialmente de PDU's ("Protocol Data Units") que são enviados de um dispositivo ao outro em função do AM_ADDR no cabeçalho do pacote. PDU's do gerenciador de conexão são sempre enviados como pacotes simples (ocupando apenas um intervalo de tempo) – o cabeçalho do campo de carga útil possui, portanto, apenas 1 byte.

Cada PDU é mandatório ou opcional. O gerenciador de conexão (LM) não precisa ser capaz de transmitir uma PDU que é opcional. O LM precisa apenas reconhecer todas as PDU's opcionais recebidas e enviar, se requerido, uma resposta válida.

3.4.4. Controle Lógico de Conexão e Protocolo de Adaptação (L2CAP)

O L2CAP ("Logical Link Control and Adaptation Protocol") é localizado numa camada acima do protocolo banda base. O L2CAP fornece serviços de dados com conexão orientada e sem conexão para protocolos das camadas superiores com capacidade de multiplexação de protocolos, operações de segmentação e montagem. O L2CAP também permite que protocolos e aplicações de níveis superiores transmitam e recebam pacotes de dados acima de 64kbytes.

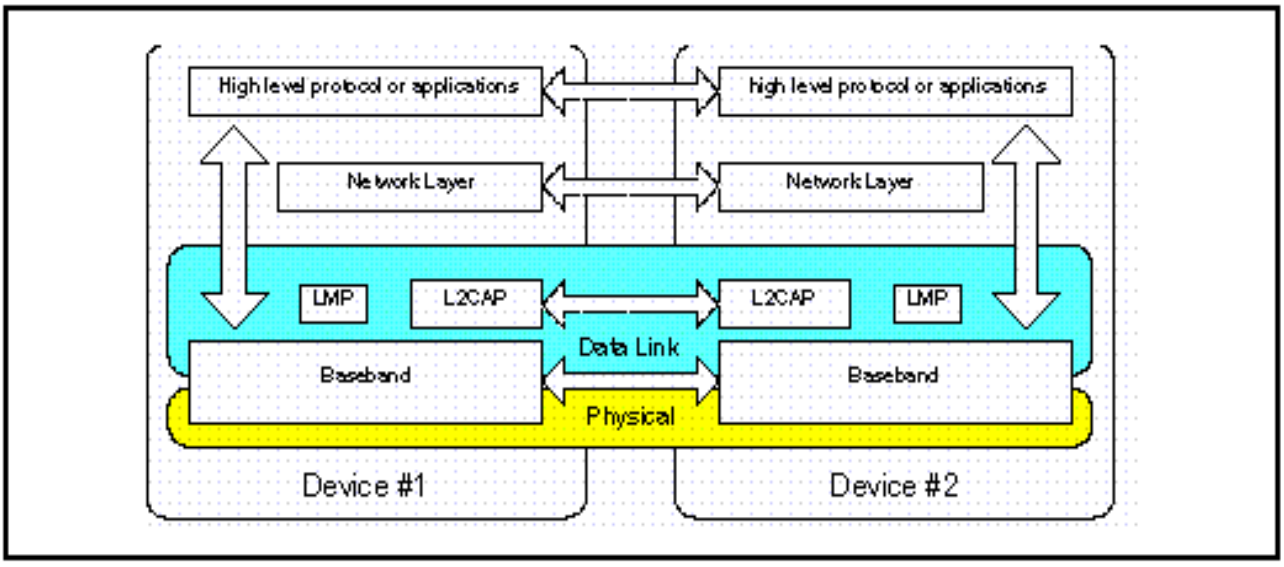

Fig. 19 – Camadas de protocolos com L2CAP

A especificação da banda base define 2 tipos de conexão: conexão síncrona orientada a conexão (SCO) e conexão assíncrona sem conexão (ACL). Conexões SCO suportam tráfego de voz em tempo real usando banda reservada. Conexões ACL suportam tráfego que exige melhor desempenho. A especificação do L2CAP é definida só para conexão ACL. O formato do cabeçalho do conteúdo ACL é mostrado abaixo. O tipo de pacote (campo no cabeçalho da banda base) distingue pacotes simples (que ocupam apenas um intervalo de tempo) de pacotes múltiplos (que ocupam mais do que um intervalo de tempo).

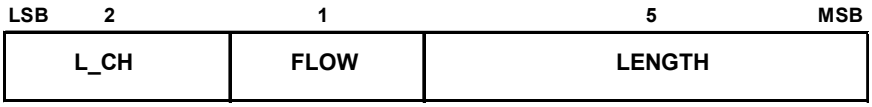

Fig. 20 – Cabeçalho do conteúdo ACL para pacotes simples

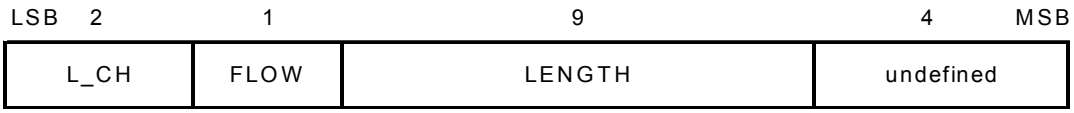

Fig. 21 – Cabeçalho do conteúdo ACL para pacotes múltiplos

O 2 bits lógicos do campo L_CH distinguem pacotes L2CAP de pacotes LMP, conforme tabela abaixo:

L_CH code	Logical Channel	Information
00	RESERVED	Reserved for future use
01	L2CAP	Continuation of L2CAP packet
10	L2CAP	Start of L2CAP packet
11	LMP	Link Manager Protocol

Tabela 2 – Canais lógicos (L_CH)

O bit “Flow” no cabeçalho é comandado pelo “Controlador de Conexão – LC”. Normalmente é setado em “1”, sendo que é setado em “0” quando nenhum tráfego de L2CAP será enviado sobre conexão ACL.

Condições funcionais

Requerimentos essenciais de protocolos para L2CAP incluem simplicidade e pouco overhead. A implementação do L2CAP tem que ser aplicável para dispositivos com recursos computacionais limitados. O L2CAP não pode consumir energia excessiva para não sacrificar energia para a interface de rádio Bluetooth. Requerimentos de memórias para a implementação de protocolo devem ser também mínimos.

A complexidade do protocolo deve ser aceitável para computadores pessoais, PDA’s, celulares, fones de ouvido sem fio, joysticks e dispositivos sem fio.

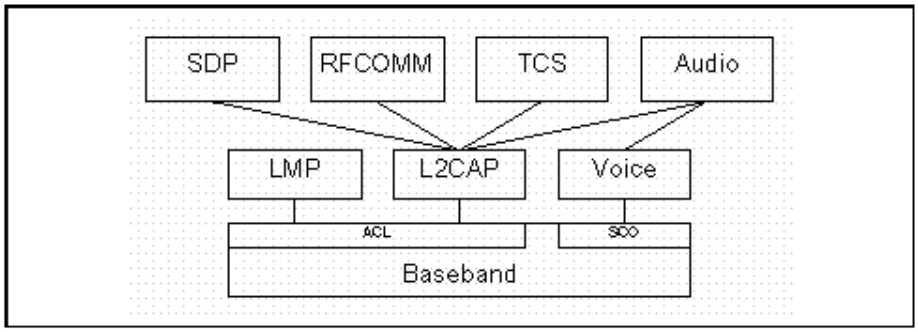

Fig. 22 – L2CAP na arquitetura de protocolos Bluetooth

As quatro principais tarefas do L2CAP são:

- Multiplexação de Protocolos

O L2CAP precisa permitir a multiplexação de protocolos, pois o protocolo banda base não provê nenhum tipo de campo de identificação de protocolo das camadas superiores. O L2CAP precisa ser capaz de distinguir os protocolos das camadas superiores.

- Segmentação e Montagem

Os pacotes de dados definidos pelo protocolo de banda base são limitados em tamanho. Com isso pacotes L2CAP grandes precisam ser segmentados em múltiplos pacotes pequenos banda

base para serem transmitidos pelo ar. Similarmente, os múltiplos pacotes banda base recebidos precisam ser remontados em um pacote L2CAP grande. A funcionalidade de segmentação e remontagem é necessária para suportar uso de pacotes grandes.

- Qualidade de serviço

O processo de estabelecimento de conexão L2CAP permite a troca de informações com relação a qualidade de serviços (QoS) esperada entre 2 unidades Bluetooth. Cada implementação L2CAP deve monitorar os recursos usados pelo protocolo e garantir que a QoS contratual está sendo honrada.

- Grupos

O protocolo de banda base permite a concepção da piconet utilizando a técnica de saltos em freqüência ("frequency hopping"). O grupo abstrato L2CAP permite implementações para o mapeamento eficiente dos grupos de protocolos na piconet. Sem o grupo abstração, os protocolos das camadas superiores necessitarão ser expostos para as funcionalidades do protocolo de banda base e controlador de conexão, com a finalidade de controlar os grupos eficientemente.

3.4.5. Protocolo de Descobrimento de Serviço (SDP)

O SDP ("Service Discovery Protocol") define como uma aplicação Bluetooth do cliente precisa atuar para descobrir serviços Bluetooth disponíveis e suas características. O protocolo define como um cliente pode procurar serviços baseados em atributos específicos sem saber dos serviços disponíveis.

Como a computação continua movendo para um modelo central de rede, procurar e usar os serviços que podem estar disponíveis na rede se tornam processos incrivelmente importantes. O SDP é otimizado para a natureza dinâmica das comunicações Bluetooth, focando principalmente no descobrimento dos serviços disponíveis de ou através de um dispositivo Bluetooth. O SDP não define o método de acesso aos serviços, sendo que os mesmo podem ser acessados de várias maneiras, dependendo do serviço.

O serviço é qualquer entidade que pode fornecer informação, executar uma ação ou controlar um recurso de uma outra entidade. O serviço pode ser implementado como software, hardware ou uma combinação de ambos. Toda informação sobre os serviços é mantida pelo servidor SDP, sendo que o protocolo SDP usa o modelo de requisição/resposta.

O mecanismo de descobrimento de serviços fornece o meio para aplicações do cliente descobrirem a existência de serviços fornecidos por aplicações do servidor, bem como o atributos desses serviços. Os atributos dos serviços incluem o tipo ou a classe de serviço oferecido e o mecanismo ou informação de protocolo requerido para utilizar o serviço. O SDP também fornece funcionalidade para detectar quando o serviço não está mais disponível.

SDP envolve comunicação entre servidor SDP e cliente SDP. O servidor mantém uma lista de serviços gravados que descreve as características dos serviços associados com o servidor. O cliente precisa buscar informações do serviço gravado mantido pelo servido SDP fazendo uma requisição SDP.

Se o cliente ou a aplicação associada com o cliente decide usar o serviço, será necessário abrir uma conexão separada com o fornecedor de serviço com a finalidade de utilizar o serviço. O SDP fornece o mecanismo para descobrir serviços e seus atributos, porém não fornece o mecanismo para utilizar seus serviços.

Existe no máximo um servidor SDP por dispositivo Bluetooth. O dispositivo pode funcionar tanto como servidor SDP como cliente SDP. Se múltiplas aplicações no dispositivo fornecem serviços, o servidor SDP pode atuar em benefício dos demais servidores para lidar com requisições de informações sobre os serviços que pode fornecer. Similarmente, múltiplas aplicações de clientes devem utilizar o cliente SDP para questionar servidores em benefício das aplicações do cliente.

O grupo de servidores SDP que estão disponíveis para o cliente SDP pode mudar dinamicamente, baseado na proximidade entre os servidores e o cliente. Quando o servidor se torna disponível, o cliente em potencial deverá ser notificado por um meio que não seja SDP, com isso o cliente pode usar o SDP para questionar o servidor sobre os serviços. Da mesma forma, quando um servidor sai da proximidade ou se torna indisponível por alguma razão, não há nenhuma notificação através do SDP. Contudo, o cliente precisa usar o SDP para questionar o servidor e deduzir que o servidor não está mais disponível se demorar para responder a requisição.

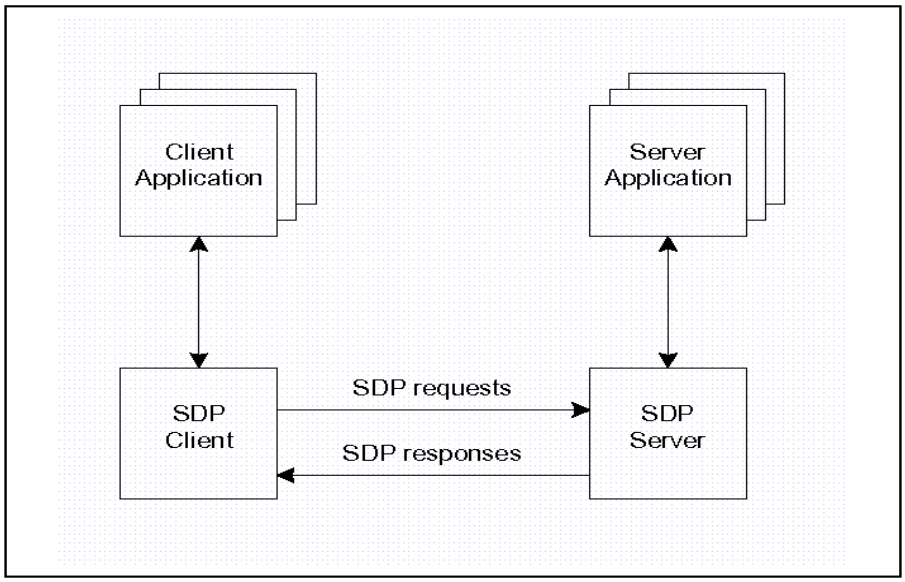

Fig. 23 – Interação cliente-servidor SDP

3.4.6. Protocolo de Substituição do Cabo (RFCOMM)

O protocolo RFCOMM ("Cable Replacement Protocol ") emula porta seriais sobre o protocolo L2CAP. Ele é um protocolo de transporte simples, com recursos adicionais para emular os 9 circuitos das portas seriais do RS-232 (EIA/TIA-232-E). O RFCOMM permite até 60 conexões simultâneas entre dois dispositivos Bluetooth. A quantidade de conexões que pode ser estabelecida simultaneamente por um dispositivo Bluetooth depende do tipo de implementação.

Considerando os propósitos do protocolo RFCOMM, um caminho de comunicação completo envolve duas aplicações sendo executadas em diferentes dispositivos com um segmento de comunicação entre eles (figura 24).

Fig. 24 – Segmento de comunicação RFCOMM

O objetivo do RFCOMM é permitir o uso de aplicações que utilizam as portas seriais dos dispositivos em que residem. Na configuração simples, o segmento de comunicação é uma

conexão Bluetooth entre um dispositivo Bluetooth e outro. Quando o segmento de comunicação é uma outra rede, a tecnologia Bluetooth é usada no caminho entre o dispositivo Bluetooth e um dispositivo de conexão de rede, como um modem. As figuras 25 e 26 ilustram estes dois casos.

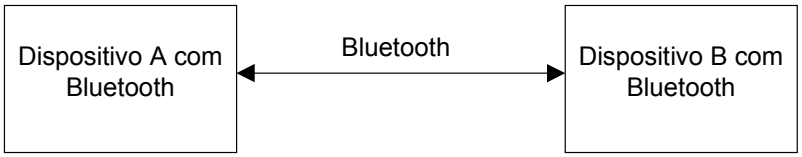

Fig. 25 – Conexão direta RFCOMM

Fig. 26 – RFCOMM usado com dispositivos sem Bluetooth

3.4.7. Protocolo de Controle de Telefonia (TCS Binary)

Este protocolo ("Telephony Control Protocol") define a sinalização de controle da chamada para o estabelecimento de chamadas de voz e dados entre os dispositivos Bluetooth.

O TCS é baseado no Anexo D da recomendação ITU-T Q.931, sendo que o texto não diferencia o usuário da rede, mas somente entre o originador da chamada (Outgoing side) e o receptor da chamada (Incoming side). Esforços foram feitos apenas com a finalidade de aplicar mudanças necessárias para aplicações Bluetooth e aplicações futuras, tentando ser mais abrangente possível.

O TCS contém as seguintes funções:

- Controle de Chamada (CC) – sinalização para estabelecer e liberar a chamada de voz e dados entre dispositivos Bluetooth.
- Gerenciamento de grupo (GM) – sinalização para facilitar o controle do grupo de dispositivos Bluetooth.
- Sem conexão (CL) – fornece uma maneira de trocar informações de sinalização não relacionadas com a chamada em si.

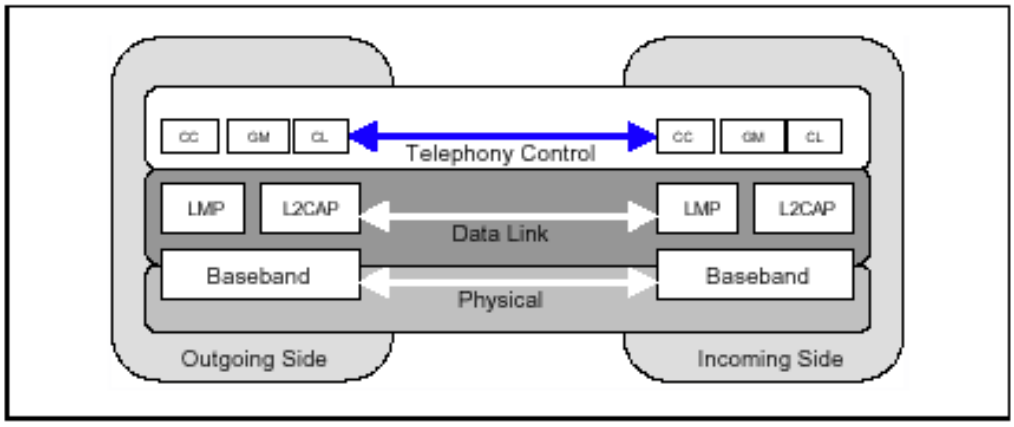

Fig. 27 – TCS na pilha Bluetooth

Operação Entre Dispositivos

O TCS utiliza sinalização ponto-a-ponto e pode usar sinalização ponto-multiponto. A sinalização ponto-a-ponto é utilizada quando se conhece o outro lado no qual se deseja que a chamada seja estabelecida, enquanto que a sinalização ponto-multiponto é usada quando se tem mais de um ponto disponível para o estabelecimento da chamada.

A sinalização ponto-a-ponto é mapeada através da conexão orientada do canal L2CAP, enquanto que a sinalização ponto-multiponto é mapeada através do canal L2CAP sem conexão, como informação broadcast.

A figura abaixo ilustra a sinalização ponto-a-ponto para estabelecer chamadas de voz ou dados. Primeiro o outro dispositivo é notificado através da requisição de chamada no canal de sinalização (A). Depois o canal de sinalização é utilizado para o estabelecimento do canal de voz ou dados (B).

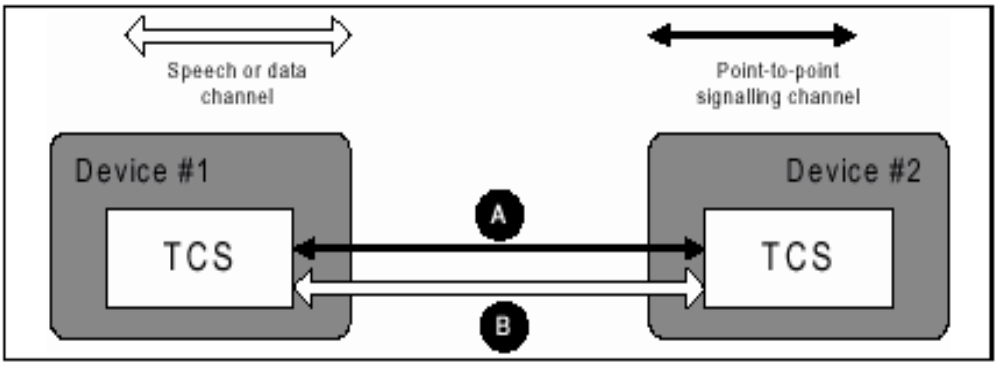

Fig. 28 – Sinalização ponto-a-ponto em uma configuração simples

A figura seguinte ilustra como a sinalização ponto-multiponto e ponto-a-ponto é utilizada para o estabelecimento da chamada de voz ou dados numa configuração multiponto. Primeiro todos os dispositivos são notificados através da requisição da chamada no canal de sinalização ponto-multiponto (A). Depois um dos dispositivos responde a chamada no canal ponto-a-ponto (B). Este canal de sinalização é então utilizado para o estabelecimento do canal de voz ou dados (C).

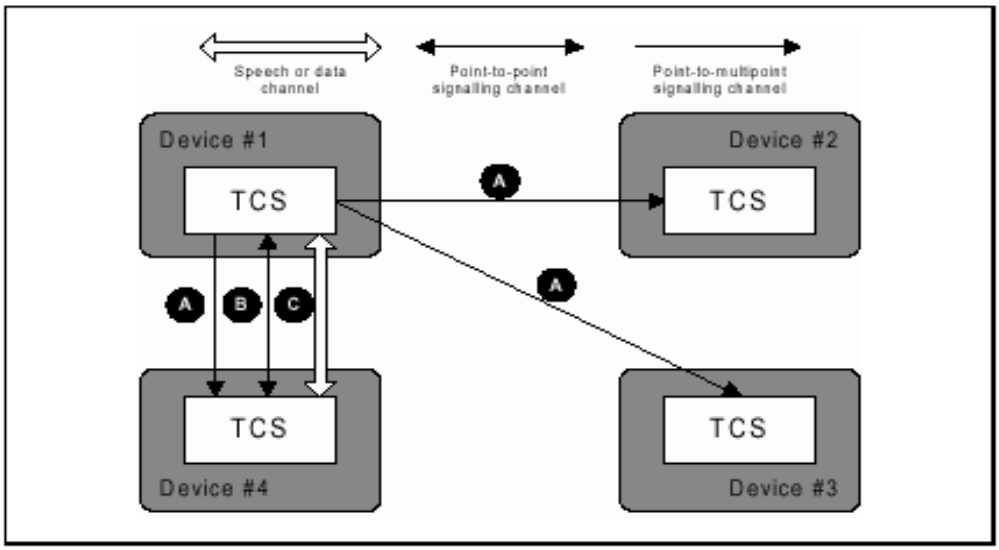

Fig. 29 – Sinalização em uma configuração multiponto

Operação entre Camadas

A implementação TCS deve seguir a arquitetura geral descrita abaixo, sendo que por simplicidade não foram desenhadas as chamadas de dados.

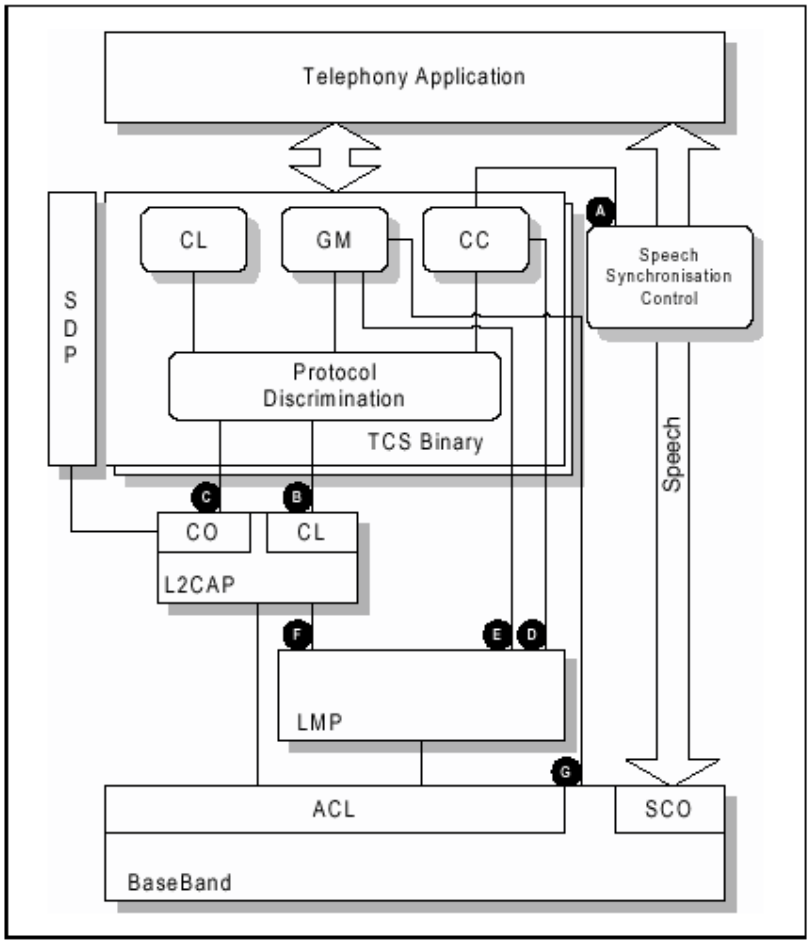

Fig. 30 – Arquitetura TCS

A estrutura interna do TCS contém as entidades funcionais Controle de Chamada, Gerenciamento de Grupo e Sem Conexão, completados com o Discriminador de Protocolo que roteia o tráfego para a entidade funcional apropriada.

Para lidar com mais chamadas simultaneamente, múltiplos processos de TCS deverão existir no mesmo tempo. A discriminação entre múltiplos processos podem ser baseados no canal identificador do L2CAP.

O TCS conecta através de interface com outras entidades para fornecer serviços de telefonia para a aplicação. As interfaces são identificados na figura acima e as informações são trocadas pelas interfaces com os seguintes propósitos:

(A) O Controlador de Chamadas fornece informação para o Controlador de Sincronização de Voz sobre quando conectar ou desconectar o canal de voz. Essa informação é baseada nas mensagens de controle de chamada (ex.: connect acknowledge ou disconnect).

(B) Para enviar uma mensagem de setup usando a sinalização ponto-multiponto, ela deverá ser entregue na interface com L2CAP para transmissão no canal sem conexão. Da mesma forma o L2CAP utiliza esta interface para informar ao TCS do recebimento de uma mensagem de setup no canal sem conexão. O canal sem conexão do L2CAP utiliza a função de broadcast da piconet.

(C) Sempre que a mensagem TCS precisa ser enviada usando a sinalização ponto-a-ponto, ela deverá ser entregue na interface com L2CAP para transmissão no canal com conexão orientada.

Durante o estabelecimento do canal L2CAP, será indicada a qualidade de serviço específica que será utilizada para a conexão. Em particular, L2CAP informará LMP quando do uso dos modos de baixa potência (F).

(D) A entidade Controlador de Chamada controla diretamente o LMP, com a finalidade de estabelecimento e liberação das conexões SCO.

(E) (G) A entidade de Gerenciamento de Grupo controla diretamente o LMP e a banda base durante a inicialização dos processos para controlar por exemplo perguntas, paging e conexão.

3.4.8. Controle de Telefonia

Vários comandos AT são suportados para transmissão de sinais de controle para "Controle de Telefonia". Eles usam a emulação de porta serial, RFCOMM, para transmissão.

PROTOCOLOS ADOTADOS

Esta seção descreve alguns protocolos que foram definidos para serem adotados pela pilha de protocolos Bluetooth.

3.4.9. PPP

O protocolo ponto-a-ponto (PPP) na tecnologia Bluetooth é designado para rodar sobre RFCOMM para efetuar conexões ponto-a-ponto. O PPP é um protocolo orientado a pacote e precisa com isso converter pacotes de dados em dados seriais.

3.4.10. TCP/UDP/IP

Os padrões TCP/UDP/IP são definidos para operar em unidades Bluetooth, permitindo que elas possam se comunicar com outras unidades conectadas, por exemplo, à Internet. Portanto a unidade Bluetooth pode atuar como uma bridge para a Internet. A configuração do protocolo TCP/UDP/IP é utilizado para todos os cenários da aplicação Internet Bridge na versão Bluetooth 1.0 e para OBEX em versões futuras. A configuração UDP/IP/PPP está disponível como transporte para aplicações WAP.

3.4.11. Protocolo IrOBEX

O IrOBEX é um protocolo de sessão definido pelo IrDA. Esse protocolo também é utilizado pela tecnologia Bluetooth, permitindo que aplicativos utilizem tanto a tecnologia de rádio Bluetooth com a tecnologia de infravermelho IrDA. Entretanto, embora o IrDA e o Bluetooth tenham sido desenvolvidos para comunicações sem fio de curto alcance, eles apresentam algumas diferenças fundamentais em seus protocolos de camadas baixas.

No Bluetooth, o IrOBEX é mapeado sobre os protocolos de camadas baixas adotados pela tecnologia (o RFCOMM é utilizado como a principal camada de transporte para OBEX).

A figura 31 mostra parte da hierarquia da arquitetura Bluetooth e indica a posição do protocolo OBEX e dos aplicativos que o utilizam.

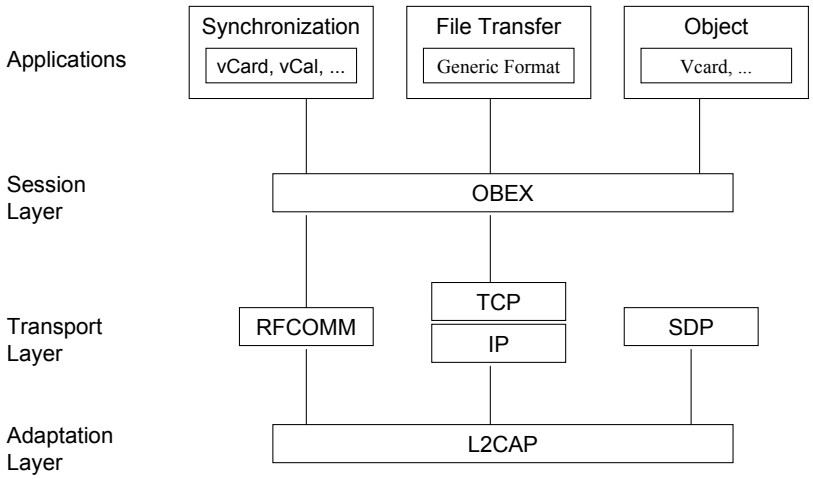

Fig. 31 – Parte da hierarquia de protocolos do Bluetooth

Formatos dos Conteúdos

Os formatos para transmissão de informações vCards e vCalendar também são definidos pela especificação Bluetooth. Os formatos não determinam mecanismos de transporte, mas o formato em que cartões eletrônicos de negócio, calendário pessoal e informações de planejamento são transportados (vCard e vCalendar são transferidos pelo OBEX).

3.4.12. Protocolo de Aplicação sem Fio (WAP)

Muitas características dos dispositivos Bluetooth são comuns para com o WAP ("Wireless Application Protocol"). Em alguns casos, o mesmo dispositivo pode ser habilitado para os 2 tipos de comunicações. Iremos descrever como o Bluetooth através do PPP pode ser utilizado para o transporte de comunicação dos protocolos e aplicações WAP. O Bluetooth fornece o meio físico e o controle da conexão para comunicações entre o cliente e servidor WAP.

Visão Geral dos Serviços WAP

O Protocolo de Aplicação Sem Fio (WAP) é designado para prover acesso a Internet para os dispositivos. Largura de banda limitada, memória, energia de processamento e capacidade do display são todos os fatores que impulsionaram o desenvolvimento do WAP. Embora alguns dispositivos apresentem os obstáculos descritos acima, o WAP ainda pode prover um benefício substancial para esses dispositivos.

O ambiente típico WAP consiste de 3 tipos de dispositivos: o cliente WAP, o proxy/gateway WAP e o servidor WAP. Em alguns casos, o proxy/gateway WAP pode também incluir a função de servidor.

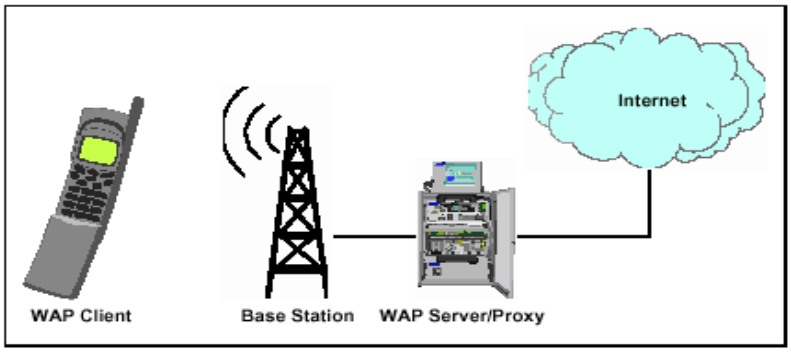

Fig. 32 – Ambiente Típico WAP

- Cliente WAP

O dispositivo Cliente WAP é usualmente encontrado nas mãos do usuário final. Este dispositivo pode ser tão poderoso como um computador portátil ou tão compacto como um telefone móvel.

O Cliente WAP é tipicamente conectado ao Proxy/Gateway WAP através da rede sem fio. Esta rede pode ser baseada em qualquer tecnologia disponível.

- Proxy/Gateway WAP

O Proxy/Gateway WAP atua como uma interface entre a rede sem fio e a Internet.

- Servidor WAP

O Servidor WAP executa uma função similar à de um servidor de Internet. Na realidade, o Servidor WAP é sempre um servidor HTTP. O servidor é um local de armazenagem para informações que os usuários podem acessar. Este conteúdo pode ser texto, gráfico e também script que pode permite ao dispositivo cliente executar processos com suporte do servidor.

O Uso do WAP em Ambiente Bluetooth

A presença de capacidade de comunicação nos dispositivos está distante de ter chegado ao fim por si só. O usuário final geralmente não está interessado na tecnologia e sim no que a tecnologia pode permitir que eles façam.

A telecomunicação tradicional tem como comunicação de voz a única aplicação de tecnologia e desta forma tem tido sucesso no mercado. Como os serviços de comunicação de dados tem se tornado largamente disponíveis, há um aumento de pressão para o fornecimento de serviços que aproveitam as vantagens dessa capacidade.

O Forum WAP foi formado para criar um padrão, no qual os serviços de dados com valor agregado podem ser desenvolvidos, garantindo alguns passos para interoperabilidade.

A qualidade única do Bluetooth para o propósito de entregar serviço com valor agregado é o limite de distância de comunicação. A seguir alguns exemplos de como o modelo cliente/servidor WAP pode ser aplicado no Bluetooth:

- Cenário 1 – Mala com laptop

Fig. 33 – Cenário 1 – Mala com Laptop

Esta cenário permite a comunicação entre o telefone móvel e o laptop, sem a intervenção do usuário, para fazer o update de e-mail. O usuário pode rever as mensagens recebidas pelo aparelho telefônico sem remover o laptop que está dentro da mala.

- Cenário 2 – Mensagens proibidas

Fig. 34 – Cenário 2 – Mensagens proibidas

Este cenário é similar ao anterior. O usuário pode escrever mensagens em um ambiente onde não é possível/permitido fazer uma conexão dial-up. Posteriormente, o laptop verifica o telefone móvel para ver se é possível enviar as mensagens pendentes. Se a comunicação estiver presente os e-mails serão transmitidos.

- Cenário 3 – Quiosque Inteligente

Este cenário permite ao usuário conectar seu laptop ou telefone móvel para se comunicar com um quiosque em um local público. O quiosque pode prover informações para o dispositivo que é específico do local em que o usuário se encontra. Por exemplo, informações de vôos e portões de embarque nos aeroportos, localização de lojas num shopping, horários de trens, etc.

WAP dentro da Piconet Bluetooth

De várias maneiras, Bluetooth pode ser usado como os outros tipos de redes sem fio, com respeito ao WAP. O Bluetooth pode ser utilizado para prover um meio de transportar dados entre o cliente e o servidor WAP.

- Iniciação da comunicação pelo cliente

Quando o cliente WAP está ativamente procurando por dispositivos Bluetooth disponíveis, ele pode descobrir a presença de um servidor WAP usando o SDP.

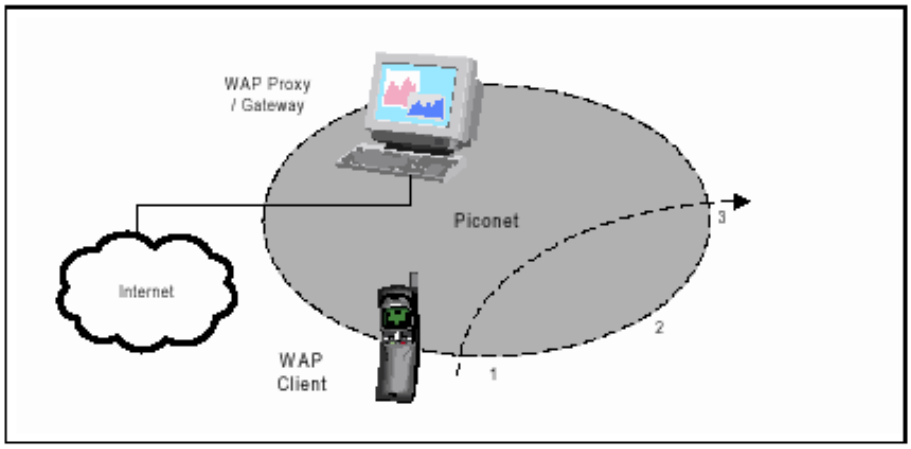

Fig. 35 – Servidor WAP / Proxy na Piconet

Na figura acima, o estágio (1) representa o dispositivo Cliente WAP se movendo dentro do alcance da piconet do Proxy/Gateway WAP. Quando o cliente detecta a presença do Proxy/Gateway WAP, ele pode automaticamente ou através da requisição do cliente se conectar ao servidor.

No estágio (2), o dispositivo está comunicando com o Proxy/Gateway WAP, sendo que normalmente é possível utilizar todo e qualquer serviço WAP de dado disponível.

No estágio (3), o dispositivo está saindo da piconet. Quando o dispositivo detecta que a comunicação com o Proxy/Gateway WAP se perdeu, ele pode opcionalmente decidir retomar a comunicação usando as informações obtidas pelo SDP. Por exemplo, se o usuário desejar continuar recebendo informações quando o mesmo estiver fora da piconet, o servidor Bluetooth

pode prover um endereço de internet para o usuário. Portanto, quando a comunicação Bluetooth não for mais possível, o dispositivo pode utilizar o celular para retomar a sessão cliente-servidor.

- Iniciação da comunicação pelo servidor

Um método alternativo de iniciação da comunicação entre o cliente e servidor é o servidor checar periodicamente os dispositivos cliente disponíveis. Quando o servidor descobre um cliente, que possui a capacidade de cliente WAP, o servidor pode opcionalmente conectar e entregar dados para o cliente, sendo que o cliente tem a opção de ignorar os dados recebidos.

A seguir especificamos a pilha de protocolos, que é utilizada para transportar WAP através do Bluetooth, usando PPP.

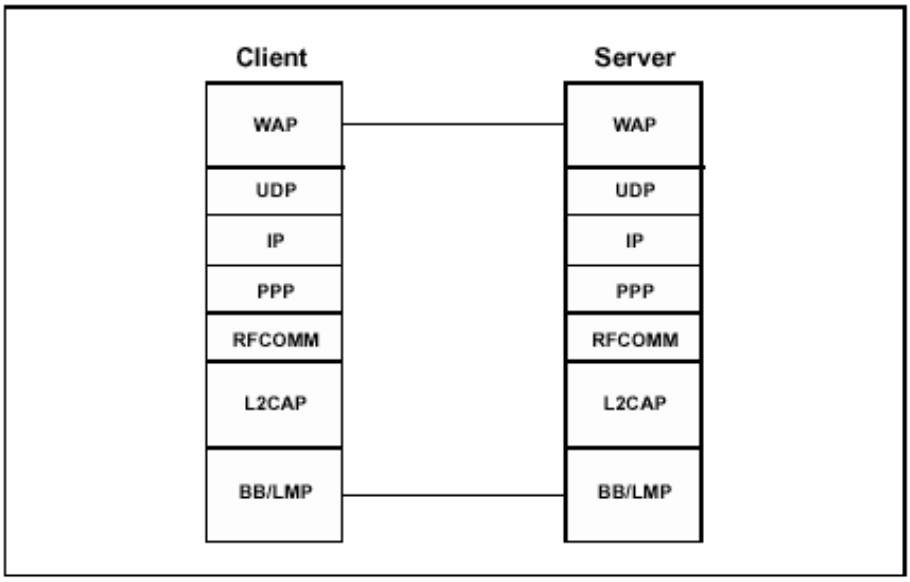

Fig. 36 – Protocolo de Suporte WAP

Para os propósitos de interoperabilidade, o Cliente WAP terá a função de terminal de dados, enquanto que o Servidor ou Proxy WAP terão a função de ponto de acesso da LAN.

A Banda base, o LMP e o L2CAP são as camadas 1 e 2 do modelo OSI. O RFCOMM é o adaptador Bluetooth, enquanto que o SDP será o protocolo de procura de serviços.

4. A INTERFACE AÉREA DO BLUETOOTH

Esta seção descreve a interface aérea do Bluetooth. Ela é a continuação da seção 2.3 (Uma Introdução da Interface Aérea do Bluetooth).

4.1. A Técnica de Salto em Freqüência

Utiliza-se a técnica de salto em freqüência ("frequency hopping" – FH) com espalhamento espectral ("spread-spectrum"), para evitar interferências. Esta técnica é bem adequada para projetos de rádio de baixo consumo e baixo custo e é utilizada em alguns produtos de LAN sem fio. A principal vantagem do Bluetooth é a alta taxa de saltos de freqüência, 1600 saltos por segundo, em vez de apenas alguns saltos por segundo. O menor comprimento do pacote na tecnologia Bluetooth é outra vantagem.

A banda de freqüência em sistemas FH é dividida em um número de canais de salto ("hop channels"). Cada um destes canais é apenas uma fração da banda total de freqüência. No Bluetooth, um canal é utilizado em 625 μs (um "slot") seguido por um salto – que ocorre em uma ordem pseudo-aleatória – para outro canal para a realização de outra transmissão de 625 μs. Este procedimento é repetido constantemente. Desta forma, os saltos espalham o tráfego do Bluetooth sobre toda a banda ISM e o sistema obtém uma boa proteção contra interferências. Se uma das transmissões recebe a interferência de, digamos, um forno de microondas, a probabilidade de interferência sobre o próximo canal de salto é muito baixa. Algoritmos de correção de erro são utilizados para corrigir as falhas causadas por transmissões bloqueadas por interferências.

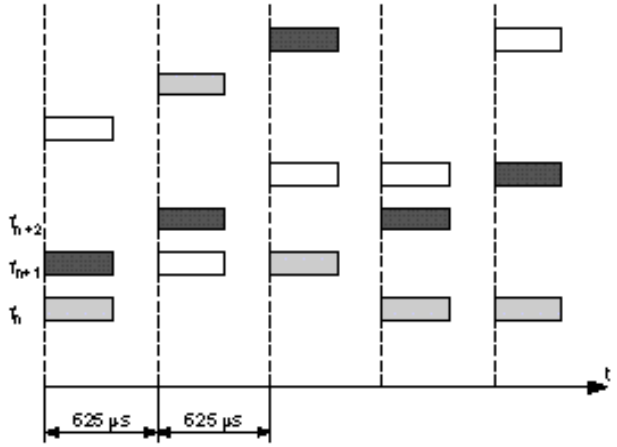

Fig. 37 – Frequency hop por divisão de tempo

4.2. Modulação/Transmissão e Definição de Pacotes

Uma modulação Gaussiana FSK binária é usada para minimizar a complexidade do transmissor em unidades Bluetooth. O sistema é full-duplex, e utiliza TDD, com slots subsequentes sendo usados para a transmissão do mestre e de escravos.

Um pacote tipicamente utiliza um único slot, mas as especificações do Bluetooth também definem um método multi-slot. Pacotes multi-slot podem ter três ou cinco slots. Pacotes são sempre enviados em um único canal de salto. Isto significa que quando pacotes multi-slot são transmitidos não ocorrem saltos até que todo o pacote seja transmitido. Isto é ilustrado na figura 38. O canal utilizando o pacote branco inicia a seqüência ilustrada com um pacote multi-slot de 3 slots. Observe que o canal de hopping que se segue à transmissão do pacote multi-slot é o mesmo (compare com a figura 37) que seria utilizado se não houvesse ocorrido a transmissão do pacote multi-slot.

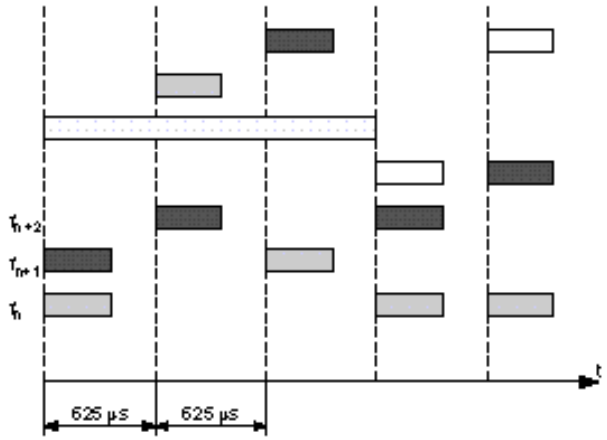

Fig. 38 – Pacote Multi-slot

4.3. Rede

Quando unidades Bluetooth estão se comunicando, uma unidade é Mestre e todas as outras unidades se comportam como Escravo. O relógio do sistema da unidade Mestre e a identidade do Mestre são partes centrais à técnica de frequency hopping. . Na unidade Escravo, um offset pode ser adicionado a seu relógio de sistema para criar uma cópia do relógio da unidade Mestre. Desta forma, todas as unidades Bluetooth conectadas mantêm relógios sincronizados e a identidade da unidade Mestre, que identifica a conexão. Saltos de freqüência sincronizados com a unidade Mestre podem então ser obtidos como descrito na figura 39. Setenta e nove freqüências de

portadoras foram definidas para a tecnologia Bluetooth (na França e Espanha, somente 23 freqüências de portadoras foram definidas, já que a faixa ISM é mais estreita nestes países).

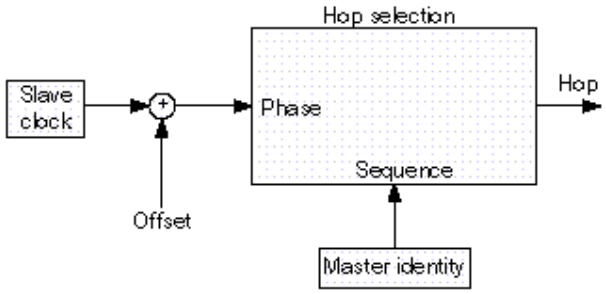

Fig. 39 – Seleção de salto

Os pacotes Bluetooth têm um formato fixo. Um código de acesso de 72 bits é a primeira informação contida no pacote. O código de acesso é baseado na identidade do Mestre e no relógio de sistema do Mestre, isto é, ele provê as informações necessárias para sincronização. Este código é único para o canal e usado por todos os pacotes transmitidos em um canal específico. Um cabeçalho de 54 bits se segue ao código de acesso. Este cabeçalho contém informações de correção de erros, retransmissão e controle de fluxo. As informações de correção de erros podem ser usadas para corrigir falhas na carga útil e no próprio cabeçalho. Finalmente, o pacote apresenta o campo de carga útil, com qualquer coisa entre zero e 2745 bits, ou seja, até 340 bytes.

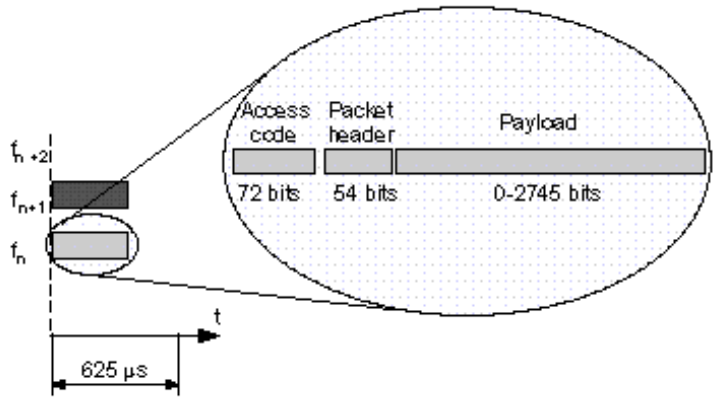

Fig. 40 – Formato do pacote Bluetooth

4.4. Parâmetros de Rádio

O transceptor Bluetooth opera na banda ISM de 2,4GHz. Esta especificação define os requerimentos necessários para ele operar nesta banda. Os requerimentos são definidos por 2 motivos:

- Fornecer compatibilidade entre os rádios dentro de um sistema.
- Definir qualidade do sistema.

Disposição de Bandas e Canais de Freqüências

Na maioria dos países a faixa de freqüência é de 2400-2483.5MHz, porém alguns países tem limitação nesta faixa de freqüência. Com a finalidade de cumprir esta limitação regional, algoritmos especiais de salto em freqüência foram especificados para estes países. Notar que produtos que implementarem esta redução de banda de freqüência não poderão trabalhar com produtos implementando a banda toda, com isso estes produtos serão considerados como versões locais.

Geography	Regulatory Range	RF Channels
USA, Europe and most other countries[1)]	2.400-2.4835 GHz	f=2402+k MHz, k=0,…,78

Tabela 3 – Banda de freqüência

Nota: A faixa de freqüência para a França é de 2,4465-2,4835GHz e os correspondentes canais de RF são de acordo com: f = 2454 + k [MHZ], k = 0,...,22

O espaçamento de canal é de 1MHz. Para atender a regulamentação, são utilizadas bandas de guarda superiores e inferiores.

Geography	Lower Guard Band	Upper Guard Band
USA, Europe and most other countries	2 MHz	3.5 MHz

Tabela 4 – Banda de guarda

Características de Transmissão

- Classes de Potências

Os equipamentos são classificados dentro 3 classes de potências:

Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1)]	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<=4 dBm to Pmax Optional: Pmin[2)] to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin[2)] to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin[2)] to Pmax

Tabela 5 – Classes de Potências

Nota 1 – Potência de saída mínima na configuração potência máxima.

Nota 2 – Limite da potência mínima Pmin< -30dBm é sugerido , mas não mandatório e pode ser escolhido de acordo com a necessidade do cliente

O controlador de potência é requerido para equipamentos da classe 1. Este controlador é usado para limitar potências de transmissão acima de 0dBm. Os equipamentos com controlador de potência otimizam a potência de saída através de comandos LMP, sendo que isto é realizado medindo-se o RSSI e o retorno de informação se a potência deve ser aumentada ou diminuída.

Notar que classe de potência 1 não pode ser utilizada para enviar pacotes de um dispositivo para o outro, se o lado que recebe não suporta as mensagens necessárias para o controle de potência do lado que está transmitindo. Lembrar também que se o dispositivo classe 1 estiver perguntando ou trocando mensagens muito próximo de um outro dispositivo, a potência de entrada pode ser muito alta em relação ao nível máximo utilizado. Isto pode causar falha na resposta do dispositivo que recebe. Nestes casos o transmissor deve obedecer as regras da classe 2 ou 3.

- Características de Modulação

A modulação é GFSK (Gaussian Frequency Shift Keying) com um BT=0,5. O bit ”1” é representado pelo desvio de freqüência positiva e o bit “0” é representado pelo desvio de freqüência negativa.

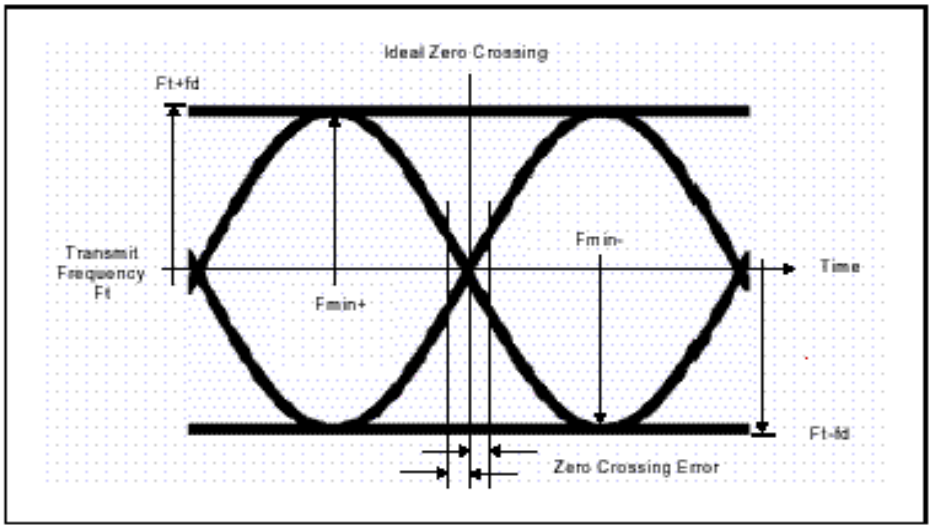

Fig. 41 – Modulação de transmissão

O erro de “zero crossing” é a diferença do tempo entre o período do símbolo ideal e o tempo de cruzamento medido, isto não pode ser menor que 1/9 do período do símbolo.

- Emissões de espúrios

A emissão de espúrios, dentro e fora da banda, é medida com o transmissor saltando numa única freqüência. Isto significa que o sintetizador deverá trocar de freqüência entre o receptor e transmissor, mas retornando para a mesma freqüência de transmissão.

- Emissão de espúrios dentro da banda

Dentro da banda ISM, o transmissor deve passar por uma máscara de espectro, mostrado na tabela 6. Em complemento ao requerimento FCC, a potência do canal adjacente sobre o canal adjacente, com diferença do número de canal de 2 ou mais, é definido. A potência de transmissão deve ser medida com uma largura de banda de 100KHz. O transmissor é transmitido no canal M e a potência no canal adjacente é medida no canal N.

Frequency offset	Transmit Power
± 500 kHz	-20 dBc
|M-N| = 2	-20 dBm
|M-N| ≥ 3	-40 dBm

Tabela 6 – Máscara de espectro de transmissão

- Emissão de espúrios fora da banda

A potência de transmissão deve ser medida com uma largura de banda de 100KHz.

Frequency Band	Operation mode	Idle mode
30 MHz - 1 GHz	-36 dBm	-57 dBm
1 GHz – 12.75 GHz	-30 dBm	-47 dBm
1.8 GHz – 1.9 GHz	-47 dBm	-47 dBm
5.15 GHz – 5.3 GHz	-47 dBm	-47 dBm

Tabela 7 – Requerimentos da emissão de espúrios fora da banda

Características de Recepção

Para medir a performance do erro de bit, o equipamento deve ter a facilidade de "loop back", isto é, o equipamento manda de volta a informação decodificada.

- Nível de sensibilidade

O nível de sensibilidade é definido como o nível de entrada para que o BER seja de 0,1%. O requerimento para o receptor Bluetooth é um nível de sensibilidade de –70dBm ou melhor.

- Performance de Interferência

A performance de interferência de co-canal e canal adjacente são medidos com um sinal desejado de 10dB sobre o nível de sensibilidade referente. Nas outras frequências o sinal

desejado deverá ser de 3dB sobre nível de sensibilidade. O BER deve ser ≤ 0,1%. A relação sinal interferência é mostrada na tabela 8.

Requirement	Ratio
Co-Channel interference, $C/I_{co\text{-}channel}$	11 dB[1)]
Adjacent (1 MHz) interference, C/I_{1MHz}	0 dB[1]
Adjacent (2 MHz) interference, C/I_{2MHz}	-30 dB
Adjacent (≥3 MHz) interference, $C/I_{\geq 3MHz}$	-40 dB
Image frequency interference[2) 3)], C/I_{image}	-9 dB[1]
Adjacent (1 MHz) interference to in-band image frequency, $C/I_{image\pm 1MHz}$	-20 dB[1]

Tabela 8 – Performance de interferência

- Nível Máximo Utilizado

O nível de entrada máximo utilizado com o qual o receptor pode operar deve ser melhor que –20dBm.

- Indicador do Sinal Recebido (RSSI)

O transceptor que pretende ter um controlador de potência, deve ser capaz de medir o sinal recebido e determinar se o transmissor do outro lado deve aumentar ou diminuir a potência, sendo que esta é a função do RSSI.

4.5. Tipos de Conexão

A unidade mestre pode formar, na mesma piconet, diferentes pares Mestre-Escravo utilizando tipos de conexão diferentes. O tipo de conexão pode ser alterado durante uma sessão.

Pacotes de dados são protegidos por um esquema de Automatic Retransmission Query, ARQ. Este esquema indica que uma verificação de erros é realizada para cada pacote recebido. Se um erro é detectado, a unidade destino indica esta detecção no pacote de retorno; de maneira que

pacotes perdidos ou com erro causam um atraso de somente 1 slot. Desta forma, somente pacotes com erro ou perdidos são restransmitidos.

Como a retransmissão não é adequada para transmissão de voz – dada sua vulnerabilidade a atrasos – um esquema de codificação de voz é utilizado. Este esquema é altamente resistente a erros de bit. Os erros que não podem ser corrigidos resultam em ruído de fundo para o ouvinte.

4.6. Piconet e Scatternet

Quaisquer dois dispositivos Bluetooth que estejam dentro do raio de alcance um do outro podem estabelecer a chamada conexão "ad hoc" ("como e quando necessário"). Quando tal conexão é estabelecida, uma piconet é criada. Sempre há uma unidade Mestre na piconet e todas as outras unidades agem como Escravo. Até oito unidades ativas podem formar uma piconet, que é definida pelo canal que estas unidades compartilham. A quantidade de dispositivos em uma piconet é, na verdade, ilimitada, mesmo que só possam existir oito unidades ativas em um dado momento. Qualquer unidade pode ser Mestre, já que elas possuem hardware ou software idênticos. A unidade que estabelece a piconet se torna a unidade Mestre. Os papéis em uma piconet podem se alterar, mas nunca pode haver mais de uma unidade Mestre.

A unidade Mestre controla todo o tráfego em uma piconet. Ela aloca capacidade para conexões SCO e gerencia esquemas de "polling" para conexões ACL. Unidades Escravo só podem enviar no slot "Escravo-para-Mestre" depois de terem sido endereçadas no slot "Mestre-para-Escravo" precedente. Se não houverem informações a serem transmitidas do Mestre para o Escravo, um pacote contendo somente o código de acesso e cabeçalho é enviado. Ou seja, todas as unidades Escravo são endereçadas em uma ordem específica, e seguindo um esquema de polling, e só podem transmitir após serem endereçadas. Este método elimina a possibilidade de colisão de pacotes transmitidos por unidades Escravo.

4.6.1. Estabelecendo Conexões de Rede

Antes de se juntar a uma piconet, uma unidade Bluetooth está no modo standby. Neste modo, a unidade não conectada "acorda" periodicamente e verifica por mensagens a cada 1,28 segundos. Mensagens de paging são transmitidas em 32 dos 79 (ou em 16 dos 23 na França e Espanha) portadoras, que são definidas como "wake-up carriers" (a identidade da unidade determina qual das portadoras ela é). Uma conexão é feita por uma mensagem de "page" se o endereço já é

conhecido, ou por uma mensagem de “inquiry” seguida por uma mensagem de “page” se o endereço é desconhecido.

A seqüência de wake-up é transmitida pela unidade Mestre nas 32 “wake-up carriers”. Inicialmente, as primeiras 16 portadoras são usadas. Se não houver resposta, o restante das portadoras é usada. O relógio de sistema da unidade Escravo determina a fase na seqüência wake-up. A unidade Escravo escuta por 18 slots na portadora wake-up e compara o sinal de entrada com o código de acesso derivado de sua própria identidade. Se as informações coincidirem, a unidade inicia um procedimento de setup de conexão e passa ao modo Connected. A unidade Mestre deve conhecer a identidade da unidade Escravo e seu relógio de sistema. Isto é necessário para calcular o código de acesso e a seqüência de wake-up e para prever a fase desta seqüência. Para se manter atualizada com os relógios de sistemas das unidades Escravo, um procedimento de paging é definido para a unidade Mestre. Ele define como identidades são transmitidas entre unidades Mestre e Escravo e como os relógios de sistema atuais dos escravos são distribuídos à unidade Mestre.

Um sinal de inquiry é transmitido inicialmente para conectar unidades com endereços desconhecidos. O sinal é usado para informar a identidade da unidade Escravo à unidade Mestre. A unidade de paging nas portadoras de inquiry wake-up envia o código de acesso de inquiry. Unidades recebendo esta mensagem respondem com suas identidades e relógios de sistema. A mensagem de inquiry é utilizada, tipicamente, para localizar dispositivos Bluetooth, incluindo impressoras compartilhadas, aparelhos de fax e dispositivos similares com endereços desconhecidos.

- Modos de Economia de Energia

Três diferentes modos de economia de energia foram definidos: Hold, Sniff e Park. Eles podem ser usados se não há nenhuma transmissão de dados sendo feita na piconet. Uma unidade Escravo tanto pode exigir ser colocada no modo Hold como ser colocada neste modo pela unidade Mestre. No modo Hold, somente um timer interno está rodando. A transmissão de dados é reiniciada instantaneamente quando unidades fazem a transmissão fora do modo Hold. O modo é usado para a conexão de várias piconets ou para gerenciar um dispositivo de baixo consumo como um sensor de temperatura. No modo Sniff, um dispositivo Escravo “ouve” a piconet a uma taxa reduzida, reduzindo portanto o seu duty cycle. No modo Park, a unidade se mantém sincronizada à piconet mas não participa do tráfego.

4.6.2. Scatternet

Para otimizar o uso do espectro disponível, várias piconets podem existir na mesma área. Isto é chamado de scatternet. Dentro de uma scatternet, todas as unidades compartilham a mesma faixa de freqüências, mas cada piconet utiliza diferentes seqüências de salto e transmite em diferentes canais de salto ("hop channels") de 1 MHz. Desta forma, uma maneira de otimizar a capacidade de transmissão de dados é manter as piconets pequenas (isto é, com poucas unidades). Todas as piconets compartilham a banda de 80 MHz, onde cada piconet usa 1 MHz. Desta forma, enquanto as piconets escolherem diferentes seqüências de salto, não há compartilhamento de canais de salto de 1 MHz.

Consequentemente, se um usuário móvel quer conectar uma quantidade de unidades Bluetooth a seu telefone móvel, a melhor maneira de obter altas taxas de transmissão é formar a maior quantidade de piconets possível dentro de uma scatternet. Cada conexão está utilizando a máxima capacidade da piconet (723 kbps). As leis da probabilidade indicam que o número de colisões resultando em retransmissões é tão baixo que até 8 piconets são possíveis em uma scatternet.

4.7. Segurança no Bluetooth

O uso da tecnologia Bluetooth como alternativa ao uso de cabos exige recursos de segurança na solução sem fio contra "eavesdropping" e falsificação de mensagens transmitidas. Desta forma, recursos de autenticação e criptografia foram acrescentados à tecnologia do Bluetooth. Autenticação é utilizada para prevenir acessos indesejáveis a informações e para prevenir a falsificação de mensagens do originador. Criptografia é usada para impedir "eavesdropping". Estas duas técnicas combinadas ao salto em freqüência e ao limitado alcance de transmissão das unidades Bluetooth, normalmente 10 m, dão à tecnologia grande proteção contra "eavesdropping".

Como as exigências de segurança dependem do tipo de aplicação desejada, três níveis de segurança foram definidos no conceito Bluetooth:

1. Non-secure – este modo não utiliza os recursos de autenticação e criptografia.
2. Service-level security – procedimentos de segurança não são inicializados até o estabelecimento do canal L2CAP.

3. Link-level security – procedimentos de segurança são iniciados antes que o setup no nível LMP seja completado.

4.7.1. Segurança em Nível de Serviço

Neste modo, sugere-se a introdução de um Gerenciador de segurança que controle o acesso a serviços e unidades. Este modo de segurança permite que se definam níveis de confiabilidade para serviços e unidades utilizados. O acesso é restringido de acordo com os níveis de confiabilidade definidos.

4.7.2. Segurança em Nível de Conexão

Este modo é baseado no conceito de chaves de conexão. Estas chaves são números aleatórios secretos de 128 bits armazenados individualmente para cada par de dispositivos em uma conexão Bluetooth. Cada vez que duas unidades Bluetooth se comunicam, a chave de enlace é usada para autenticação e criptografia.

5. POR QUÊ BLUETOOTH – ASPECTOS MERCADOLÓGICOS

5.1. Técnicas concorrentes

Existem vários concorrentes da tecnologia do Bluetooth. Entretanto, não há uma tecnologia única que claramente possa concorrer em todos os segmentos de mercado em que o Bluetooth pode operar.

5.1.1. IrDA

O principal concorrente no mercado de substituição de cabos é o IrDA. IrDA é uma padrão de interface via luz infravermelha que permite conexões sem fios entre, por exemplo, telefones celulares e PDA's. A técnica está bastante difundida no mercado, mas apresenta alguns problemas porque alguns fabricantes de IrDA desenvolveram aplicativos incompatíveis com as implementações padrão. A capacidade máxima de carga útil alcançada pela tecnologia IrDA é superior à alcançada pelo Bluetooth. As duas maiores desvantagens da tecnologia IrDA são que ela é limitada a conexões ponto a ponto (somente dois dispositivos em uma conexão) e exige visada direta (já que é baseada em luz infravermelha).

5.1.2. Implementações baseadas no IEEE 802.11

Os principais concorrentes no mercado de LAN's sem fio são as implementações baseadas no padrão IEEE 802.11. Algumas destas implementações também utilizam tecnologia de frequency hopping. As principais diferenças entre o Bluetooth e estas implementações são as seguintes:

- Implementações baseadas no IEEE 802.11 têm maior capacidade de transmissão;
- Sistemas baseados no IEEE 802.11 permitem maior número de usuários simultâneos;
- tamanho do hardware do Bluetooth é consideravelmente menor;
- preço da unidade Bluetooth é de 10 a 20 vezes menor que o de uma unidade IEEE 802.11;
- A quantidade de saltos em freqüência é consideravelmente maior no Bluetooth do que em implementações IEEE 802.11.

5.1.3. Rádio de Banda Ultra Larga (UWB)

A tecnologia de rádio UWB é nova. O conceito é similar ao radar. Pulsos de curta duração são transmitidos em uma faixa de freqüência larga. A informação é modulada pela duração e freqüência do pulso. A tecnologia ainda não foi completamente aperfeiçoada, mas poderá representar uma ameaça ao Bluetooth, já que é superior tanto em capacidade como em consumo. Protótipos UWB indicam carga útil de até 1.25 Mbps com um alcance de 70 metros e somente 0.5 mW de consumo de potência.

5.1.4. Home RF

Home RF é uma técnica desenvolvida por um consórcio composto por, entre outras, Microsoft, Intel, HP, Motorola e Compaq. A técnica foi desenvolvida a partir do conceito DECT e opera na banda de 2.4 GHz (a mesma do Bluetooth). A intenção foi a de desenvolver uma solução para o mercado residencial. As semelhanças desta solução com o Bluetooth são muitas, e incluem preço por unidade, alcance, potência de transmissão etc.. As principais diferenças são que o Home RF permite até 127 unidades por rede e suporta somente 50 saltos de freqüência por segundo. No Bluetooth, estes números são 8 e 1600, respectivamente.

5.2. Pontos fortes do Bluetooth

O conceito do Bluetooth apresenta vários benefícios quando comparado a outras técnicas. As principais vantagens são:

- As pequenas dimensões do hardware;
- baixo custo dos componentes Bluetooth;
- baixo consumo de potência para conexões Bluetooth.

As vantagens permitem introduzir suporte ao Bluetooth em vários tipos de dispositivos a um baixo custo. A variedade de produtos oferecidos (telefones móveis, PDA's, computadores, notebooks, acessórios etc.) pelas empresas que fazem parte do Bluetooth SIG e seu amplo suporte à tecnologia criam uma posição de mercado única.

A capacidade fornecida pelo Bluetooth – cerca de 723 kbps – pode ser usada para substituição de cabos e para várias outras aplicações, tais como voz, LAN etc.. A figura 42 ilustra em que áreas a tecnologia Bluetooth pode ser utilizada. A definição de aplicativos de usuário específicos e

correspondentes recursos (profiles) combinados aos quatro recursos gerais irão certamente levar a uma situação de mercado onde aplicativos de usuário utilizarão os modelos de usuários já definidos e seus profiles. Além disso, é provável que novos aplicativos utilizem os profiles padrões e, portanto, evitem problemas de interoperabilidade entre diferentes fabricantes.

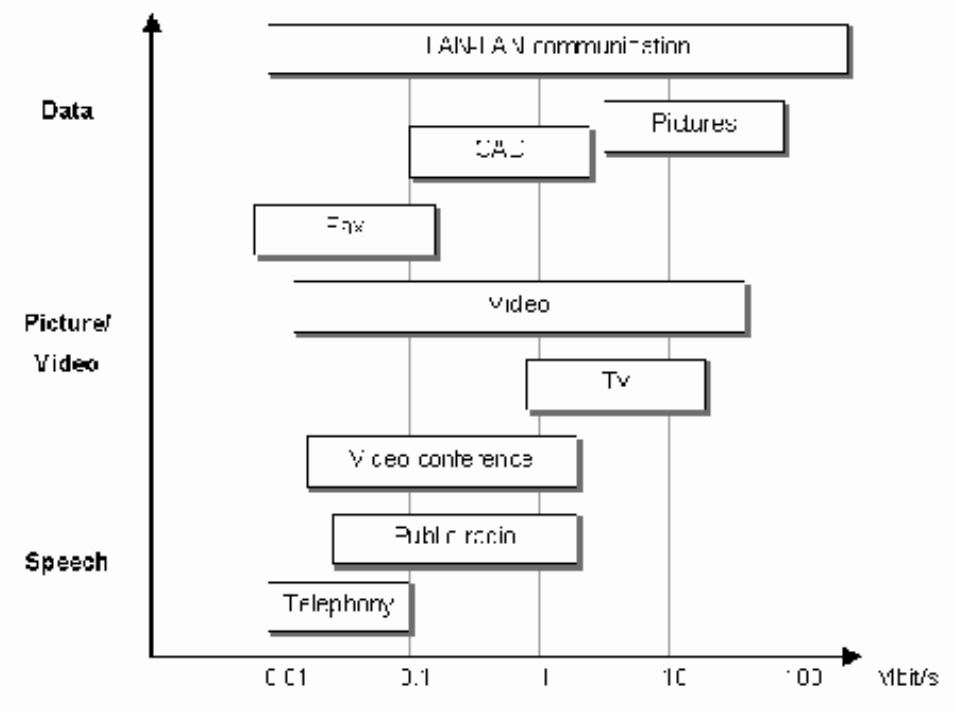

Fig. 42 – Requisitos para transmissão de dados

Referências Bibliográficas

[01] – Bluetooth SIG. Specification of the Bluetooth System – Specification Volume 1 – Core, Version 1.1, February 22, 2001, 1084 p.

[02] – Bluetooth SIG. Specification of the Bluetooth System – Specification Volume 2 – Profiles, Version 1.1, February 22, 2001, 452 p.

[03] – http://www.bluetooth.com.