Notas de Aula de Arquitetura e Organização de Computadores

Barramentos - Bluetooth

Tecnologia Bluetooth

Introdução

O **Bluetooth** é uma tecnologia que permite a comunicação simples, rápida, segura e barata entre computadores, S*martPhones*, telefones celulares, mouses, teclados, fones de ouvido, impressoras e outros dispositivos, usando ondas de rádio. Assim, é possível fazer com que dois ou mais dispositivos comecem a trocar informações com uma simples aproximação entre eles.

O que é Bluetooth

Bluetooth é um padrão global de comunicação sem fio e de baixo consumo de energia que permite a transmissão de dados entre dispositivos compatíveis com a tecnologia. Para isso, uma combinação de hardware e software é utilizada para permitir que essa comunicação ocorra entre os mais diferentes tipos de aparelhos. A transmissão é feita através de radiofrequência, permitindo que um dispositivo detecte o outro independente de suas posições, desde que estejam dentro do limite de proximidade. Deste modo, o alcance máximo do Bluetooth foi dividido em três classes:

- **Classe 1:** potência máxima de 100 mW alcance de até 100 metros;
- **Classe 2:** potência máxima de 2,5 mW alcance de até 10 metros;
- **Classe 3:** potência máxima de 1 mW alcance de até 1 metro.

Isso significa que um aparelho com Bluetooth classe 3 só conseguirá se comunicar com outro se a distância entre ambos for inferior a 1 metro, por exemplo. Neste caso, a distância pode parecer inutilizável, mas é suficiente para conectar um fone de ouvido a um telefone celular pendurado na cintura de uma pessoa.

A velocidade de transmissão de dados no Bluetooth é baixa: até a versão 1.2, a taxa pode alcançar, no máximo, 1 Mbps.

Na versão 2.0, esse valor passou para até 3 Mbps. Essas taxas são suficientes para conexão satisfatória entre a maioria dos dispositivos.

Na busca por velocidades maiores é constante, como prova a chegada da versão 3.0, capaz de atingir taxas de até 24 Mbps.

Surgimento do Bluetooth

A história do Bluetooth começa em meados de 1994. Na época, a empresa Ericsson começou a estudar a viabilidade de desenvolver uma tecnologia que permitisse a comunicação entre telefones celulares e acessórios utilizando sinais de rádio de baixo custo, ao invés dos tradicionais cabos. O estudo era feito com base em um projeto que investigava o uso de mecanismos de comunicação em redes de telefones celulares, que resultou em um sistema de rádio de curto alcance que recebeu o nome *MCLink*. A Ericsson percebeu que o MCLink poderia dar certo, já que o seu principal atrativo era uma implementação relativamente fácil e barata.

Em 1997, o projeto desperta interesse de outras empresas que, logo, passaram a fornecer apoio. Por conta disso, em 1998 foi criado o consórcio **Bluetooth SIG** (*Special Interest Group*), formado pelas empresas Ericsson, Intel, IBM, Toshiba e Nokia. Note que esse grupo é composto por dois "gigantes" das telecomunicações (Ericsson e Nokia), dois nomes de peso na fabricação de PCs (IBM e Toshiba) e a líder no desenvolvimento de chips e processadores (Intel).

O Bluetooth começou a virar realidade, inclusive pela adoção desse nome. A denominação *Bluetooth* é uma homenagem a um rei dinamarquês chamado *Harald Blåtand*, mais conhecido como *Harald Bluetooth (Haroldo Dente-Azul*). Um de seus grandes feitos foi a unificação da Dinamarca, e é em alusão a esse fato que o nome *Bluetooth* foi escolhido, como que para dizer que a tecnologia proporciona a unificação de variados dispositivos. O logotipo do Bluetooth é a junção de dois símbolos nórdicos que correspondem às iniciais de Harald.

Frequência e comunicação

O Bluetooth é uma tecnologia criada para funcionar no mundo todo, razão pela qual se fez necessária a adoção de uma frequência de rádio aberta, que seja padrão em qualquer lugar do planeta. A faixa ISM (Industrial, Scientific, Medical), que opera à frequência de 2,45 GHz, é a que me mais se aproxima dessa necessidade e é utilizada em vários países, com variações que vão de 2,4 GHz a 2,5 GHz.

Como a faixa ISM é aberta, isto é, pode ser utilizada por qualquer sistema de comunicação, é necessário garantir que o sinal do Bluetooth não sofra e não gere interferências. O esquema de comunicação FH-CDMA (Frequency Hopping - Code-Division Multiple Access), utilizado pelo Bluetooth, permite tal proteção, já que faz com que a frequência seja dividida em vários canais. O dispositivo que estabelece a conexão vai mudando de um canal para outro de maneira muito rápida. Esse esquema é chamado *salto de frequência* (frequency hopping). Isso faz com que a largura de banda da frequência seja muito pequena, diminuindo sensivelmente as chances de uma interferência. No Bluetooth, pode-se utilizar até 79 frequências (ou 23, dependendo do país) dentro da faixa ISM, cada uma espaçada da outra por 1 MHz.

Como um dispositivo se comunicando por Bluetooth pode tanto receber quanto transmitir dados (modo *full-duplex*), a transmissão é alternada entre slots para transmitir e slots para receber, um esquema denominado FH/TDD (Frequency Hopping/Time-Division Duplex). Esses *slots* são canais divididos em períodos de 625 µs (microssegundos). Cada salto de frequência deve ser ocupado por um *slot*, logo, em 1 segundo, tem-se 1600 saltos.

No que se refere ao enlace, isto é, à ligação entre o emissor e receptor, o Bluetooth faz uso, basicamente, de dois padrões: SCO (Synchronous Connection-Oriented) e ACL (Asynchronous Connection-Less). O primeiro estabelece um link sincronizado entre o dispositivo master e o dispositivo escravo, onde é feito uma reserva de *slots* para cada um. Assim, o SCO acaba sendo utilizado principalmente em aplicações de envio contínuo de dados, como voz. Por funcionar dessa forma, o SCO não permite a retransmissão de pacotes de dados perdidos. Quando ocorre perda em uma transmissão de áudio, por exemplo, o dispositivo receptor acaba reproduzindo som com ruído. A taxa de transmissão de dados no modo SCO é de 432 Kbps, sendo de 64 Kbps para voz.

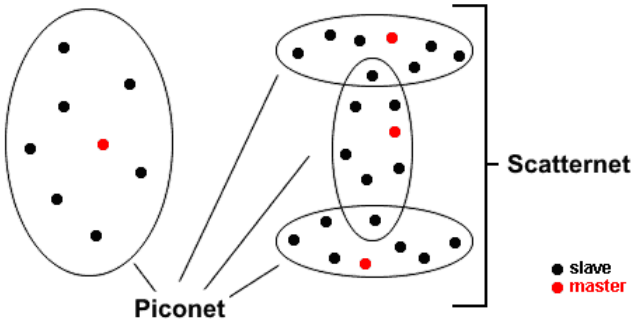
O padrão ACL, por sua vez, estabelece um link entre um dispositivo *master* e os dispositivos *slave* existentes em sua rede. Esse link é assíncrono, já que utiliza os *slots* previamente livres. Ao contrário do SCO, o ACL permite o re-envio de pacotes de dados perdidos, garantindo a integridade das informações trocadas entre os dispositivos. Assim, acaba sendo útil para aplicações que envolvam transferência de arquivos, por exemplo. A velocidade de transmissão de dados no modo ACL é de até 721 Kbps.

Redes Bluetooth

Quando dois ou mais dispositivos se comunicam através de uma conexão Bluetooth, eles formam uma rede denominada *piconet*. Nessa comunicação, o dispositivo que iniciou a conexão

assume o papel de *master* (mestre), enquanto que os demais dispositivos se tornam *slave* (escravos). Cabe ao *master* a tarefa de regular a transmissão de dados entre a rede e o sincronismo entre os dispositivos.

Cada piconet pode suportar até 8 dispositivos (um *master* e 7 *slave*), no entanto, é possível fazer com esse número seja maior através da sobreposição de piconets. Em poucas palavras, isso significa fazer com que uma piconet se comunique com outra dentro de um limite de alcance, esquema esse denominado *scatternet*. Um dispositivo *slave* pode fazer parte de varias piconets ao mesmo tempo, porém, um *master* só pode ocupar essa posição em uma única piconet.



Para que cada dispositivo saiba quais outros fazem parte de sua piconet, é necessário fazer uso de um esquema de identificação. Para isso, um dispositivo que deseja estabelecer uma conexão em uma piconet já existente pode emitir um sinal denominado *Inquiry*. Os dispositivos que recebem o sinal respondem com um pacote *FHS* (*Frequency Hopping Synchronization*) informando a sua identificação e os dados de sincronismo da piconet. Com base nessas informações, o dispositivo pode então emitir um sinal chamado *Page* para estabelecer uma conexão com outro dispositivo.

Como o Bluetooth é uma tecnologia que também oferece como vantagem economia de energia, um terceiro sinal denominado *Scan* é utilizado para fazer com que os dispositivos que estiverem ociosos entrem em *stand-by*, isto é, operem em um modo de descanso, poupando eletricidade. Todavia, dispositivos neste estado são obrigados a "acordar" periodicamente para checar se há outros aparelhos tentando estabelecer conexão.


Teclado e mouse Bluetooth da Logitech

Versões do Bluetooth

O Bluetooth é uma tecnologia em constante evolução, o que faz com que suas especificações mudem e novas versões surjam com o tempo. Até o momento do fechamento deste artigo no InfoWester, as versões disponíveis eram:

- **Bluetooth 1.0:** a versão 1.0 (e a versão 1.0B) representa as primeiras especificações do Bluetooth. Por ser a primeira, os fabricantes encontravam problemas que dificultavam a implementação e a interoperabilidade entre dispositivos com Bluetooth;
- **Bluetooth 1.1:** lançada em fevereiro de 2001, a versão 1.1 representa o estabelecimento do Bluetooth como um padrão IEEE 802.15. Nela, muitos problemas encontrados na versão 1.0B foram solucionados e o suporte ao sistema RSSI foi implementado;
- **Bluetooth 1.2:** lançada em novembro de 2003, a versão 1.2 tem como principais novidades conexões mais rápidas, melhor proteção contra interferências, suporte aperfeiçoado a scatternets e processamento de voz mais avançado;
- **Bluetooth 2.0:** lançada em novembro de 2004, a versão 2.0 trouxe importantes aperfeiçoamentos ao Bluetooth: diminuição do consumo de energia, aumento na

velocidade de transmissão de dados para 3 Mbps (2.1 Mbps efetivos), correção às falhas existentes na versão 1.2 e melhor comunicação entre os dispositivos;

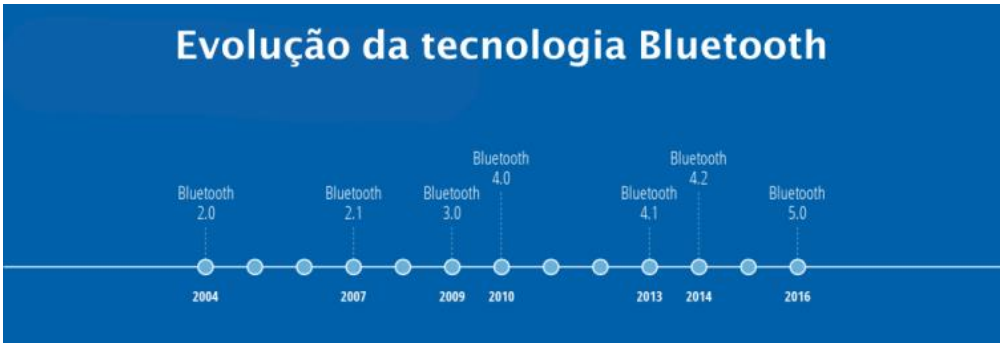
- **Bluetooth 2.1:** lançada em agosto de 2007, a versão 2.1 tem como principais destaques o acréscimo de mais informações nos sinais Inquiry (permitindo uma seleção melhorada dos dispositivos antes de estabelecer uma conexão), melhorias nos procedimentos de segurança (inclusive nos recursos de criptografia) e melhor gerenciamento do consumo de energia;
- **Bluetooth 3.0:** versão lançada em abril de 2009, tem como principal atrativo taxas altas de velocidade de transferência de dados. Dispositivos compatíveis podem atingir a marca de 24 Mbps de transferência. O "truque" para atingir taxas tão elevadas está na incorporação de transmissões 802.11 (saiba mais sobre isso neste artigo sobre Wi-Fi). Outra vantagem é o controle mais inteligente do gasto de energia exigido para as conexões. O Bluetooth 3.0 é compatível com as versões anteriores da tecnologia;
- **Bluetooth 4.0:** as especificações desta versão foram anunciadas em meados de dezembro de 2009 e o seu principal diferencial não é velocidade, mas sim economia de energia. Esse novo padrão é capaz de exigir muito menos eletricidade quando o dispositivo está ocioso, recurso especialmente interessante, por exemplo, para telefones celulares que consomem muita energia quando o Bluetooth permanece ativado, mas não em uso. A velocidade padrão de transferência de dados do Bluetooth 4.0 é de 1 Mbps.
- **Bluetooth 4.1**: Especificação que surgiu no final de 2013. O Bluetooth 4.1 é tido como uma revisão do Bluetooth 4.0, incorporando recursos que tornam a tecnologia ainda mais receptiva a dispositivos móveis, especialmente aqueles que se enquadram na chamada internet das coisas. Por conta disso, o Bluetooth 4.1 traz características que o tornam menos exigente em relação ao uso de recursos, como um modo de trabalho que mantém o módulo de Bluetooth quase inativo quando o dispositivo é afastado de uma conexão, voltando ao estado normal somente quando a conexão é reestabelecida (funcionalidade já existente, mas que foi aperfeiçoada).

  A velocidade máxima permanece em 24 Mb/s. Como o Bluetooth 4.1 consiste, basicamente, em melhorias feitas em protocolos e parâmetros, muitos dispositivos com Bluetooth 4.0 ganharam suporte ao Bluetooth 4.1 com uma atualização de software.
- **Bluetooth 4.2**: Apresentado no final de 2014, o Bluetooth 4.2 trouxe diferenciais importantes. Entre outros protocolos, a versão tem pleno suporte ao IPv6 para tornar a tecnologia ainda mais relevante para a internet das coisas: câmeras de segurança, lâmpadas inteligentes, termostatos e outros dispositivos domésticos podem usar a tecnologia de modo otimizado para comunicação no mesmo ambiente ou para acesso à internet.

  O Bluetooth 4.2 também usa criptografia do tipo FIPS (mais avançado) nas conexões e tem controle mais rigoroso da segurança, assegurando que apenas dispositivos devidamente autorizados se conectem a outros. A velocidade de transferência de dados permanece padronizada em 24 Mb/s, mas o Bluetooth 4.2 suporta tráfego de dados maior, ou seja, os dispositivos podem enviar e receber mais dados ao mesmo tempo.
- **Bluetooth 5.0**: O Bluetooth 5 foi apresentado oficialmente no final de 2016. Essa versão permite que dispositivos se comuniquem em distâncias de até 40 metros (relembrando, os padrões anteriores trabalham, em média, com até 10 metros, embora seja possível alcançar distâncias maiores neles). A velocidade passou de 24 Mb/s para 50 Mb/s.

  Outros recursos do Bluetooth 5 incluem o uso de técnicas que diminuem o risco de interferências em redes Wi-Fi ou LTE, suporte a mais dispositivos conectados ao mesmo tempo (novamente, para corresponder às necessidades da internet das coisas), funções para facilitar a geolocalização dos equipamentos conectados e mais controle sobre o consumo de energia.

- **Bluetooth LE** — ou Bluetooth Low Energy: Junto com o Bluetooth 4.0 surgiu uma variação da tecnologia chamada *Bluetooth Low Energy* ou, simplesmente, *Bluetooth LE* (também há a sigla BLE, mas ela é menos usada). Como o nome diz, trata-se de uma especificação que faz a tecnologia consumir uma quantidade muito pequena de energia elétrica — menos do que as versões "normais".
  Acessórios médicos portáteis, smartwatches e pulseiras inteligentes são exemplos de dispositivos que, por serem muito compactos, usam baterias de baixa capacidade. Assim, toda economia de energia é válida.
  O Bluetooth LE veio para atender justamente a essa necessidade. Para consumir menos energia, o Bluetooth LE utiliza várias técnicas. Uma delas é a redução na velocidade de transferência de dados, que normalmente não passa de 1 Mb/s: essa taxa costuma ser suficiente, pois o volume de dados é baixo.
  Um módulo Bluetooth LE também pode ficar a maior parte do tempo em "modo de descanso": como não há muitos dados a serem transmitidos, uma conexão de poucos milissegundos consegue dar conta de enviar ou receber todas as informações necessárias.
  Outra técnica é a redução do alcance da comunicação: o Bluetooth LE trabalha bem com distâncias de até 30 metros, mas o gasto de energia cai drasticamente se um dispositivo estiver bem perto do outro.



Evolução da tecnologia Bluetooth

O fato de haver várias versões não significa que um dispositivo com uma versão atual não funcione com outro com uma versão inferior, embora possa haver exceções. Todavia, se um dispositivo 2.0 for conectado a outro de versão 1.2, por exemplo, a velocidade da transmissão de dados será limitada à taxa suportada por este último.

Principais riscos que podem surgir ao usar Bluetooth

Os hackers costumam se concentrar no que é amplamente usado. O Bluetooth é, claro. Portanto, podemos encontrar muitos métodos que podem ser usados, as vulnerabilidades que podem surgir e, em última análise, os riscos que os usuários podem enfrentar.

Car Whisperer.

É um trecho de software que permite que hackers enviem mensagens de áudio e recebam áudio do estéreo com Bluetooth de um carro. Assim como uma brecha de segurança de um computador, essas vulnerabilidades são um resultado inevitável da inovação tecnológica, e os fabricantes de dispositivos estão lançando novas versões do software pré-gravado que solucionam os ***n*** problemas conforme eles vão surgindo.

BlueSmacking

Um dos problemas que podemos enfrentar ao usar um dispositivo com Bluetooth é o chamado **BlueSmacking**. Este é essencialmente um ataque de negação de serviço. Isso pode afetar muitos tipos de dispositivos que usam essa tecnologia.

O que o invasor faz é **enviar vários pedidos**. Isso é algo semelhante ao que poderia acontecer com um servidor web que recebe muitos pedidos e não pode cobrir tantos. Pode

acontecer que ele receba muito mais pacotes de dados do que pode suportar, ou que esses pacotes sejam maiores do que ele pode suportar.

Embora não seja o tipo de ataque mais perigoso, pode afetar drasticamente o funcionamento de um dispositivo a qualquer momento. Claro, normalmente isso pode ser consertado reiniciando-o e executando-o novamente normalmente.

BlueSnarfing

Através de um ataque **BlueSnarfing**, um hacker pode receber dados de nosso dispositivo, dados pessoais e, em última instância, qualquer informação que possa ser usada contra nós. Este é, sem dúvida, um método perigoso, pois compromete seriamente a nossa privacidade e segurança. Desta forma, um cibercriminoso poderia **enviar arquivos perigosos** via Bluetooth para não só infectar nosso dispositivo e causar mau funcionamento, mas também para obter dados pessoais.

Esses dados podem ser usados para realizar outros ataques, como um ataque de phishing, no qual você precisa saber algumas informações pessoais para ter sucesso.

Bluejacking

Outro ataque é o que é chamado de **bluejacking**. Consiste no envio de mensagens por outro dispositivo. Normalmente, trata-se de conteúdo publicitário, o que você pode chamar de "spam bluetooth". Por si só, isso não é perigoso, embora essas mensagens possam até ser usadas para lançar ataques de phishing.

O cibercriminoso pode tirar proveito do método BlueJacking para **enviar mensagem bluetooth** para a vítima e esta mensagem contém um link para um site malicioso. Por exemplo, pode ser uma página que afirma ser uma rede social ou o provedor de e-mail e a vítima, ao tentar fazer o *login*, envia esses dados para um servidor controlado pelo invasor.

BlueBugging

Continuando com os ataques *Blue*, outro é **BlueBugging**. Desta vez, é uma exploração que pode ser usada para estabelecer uma porta dos fundos em um computador que usa essa tecnologia para se comunicar. Por meio desse *backdoor*, você pode estabelecer comunicação, roubar dados e até mesmo enviar arquivos maliciosos.

Este é um dos métodos que eles podem usar para **espionar um usuário** via Bluetooth. Este é um problema significativo, porque hoje nossas informações pessoais são de grande valor na rede e os invasores podem encontrar uma maneira de tentar obter esses dados e comprometer nossa privacidade.

Rastreamento de localização

Temos cada vez mais dispositivos com conexão Bluetooth. Podemos pensar, por exemplo, em pulseiras ou relógios esportivos que usamos para registrar nossa atividade física. Em muitos casos, também registramos a rota que tomamos e, portanto, nossa posição.

Um invasor pode usar o Bluetooth com precisão para rastrear nossa localização. É um problema que pode ameaçar nossa privacidade, além de afetar a segurança pessoal. Eles lucram com as informações que os dispositivos coletam.

Fontes de pesquisa:

FutureLooks, TechRadar, PCPlus, bit-tech, TechTudo, TecMundo. Livros Didáticos.

informatique-mania.com/pt/securite/quels-sont-les-principaux-risques-de-securite-du-bluetooth/