Tecnologia Bluetooth e Aspectos de Segurança

André Ricardo Abed Grégio
R.A. 079779
Instituto de Computação
Unicamp
abedgregio@gmail.com

RESUMO

Bluetooth é uma tecnologia definida por um padrão especificado pelo Bluetooth Special Interest Group (SIG), cujo objetivo é prover um meio de baixo custo, consumo de energia e baixa complexidade de configuração para interligar dispositivos eletrônicos diversos, tais quais telefones celulares, notebooks, desktops, câmeras digitais, impressoras, PDAs e periféricos em geral. Neste trabalho é apresentada a tecnologia para redes sem fio de curto alcance denominada Bluetooth, abordando aspectos de sua arquitetura, protocolos e segurança do sistema.

Termos Gerais

Padronização, segurança, projeto

Palavras-Chave

Bluetooth, redes wireless, segurança de sistemas de informação

1. INTRODUÇÃO

Desde o surgimento das redes de comunicação de dados utilizando computadores, nos idos dos anos 60, tem-se buscado novas soluções para aumentar a mobilidade e conectividade dos sistemas, de forma a prover um alto grau de independência aos usuários. Tal independência é alcançada com a evolução das tecnologias de interfaces de rede, como as wireless, aliado à facilidade do uso. Neste aspecto, o hardware possui papel importantíssimo, pois é necessário garantir a confiabilidade e integridade dos dados em trânsito, bem como a robustez do dispositivo.

No que diz respeito às tecnologias sem fios para sistemas computacionais, há vários protocolos disponíveis para tratar da comunicação em diversas áreas de alcance. Os dispositivos infra-vermelhos (IrDA) são utilizados para comunicações simples, pois a tecnologia possui alcance limitado, baixa transmissão de dados e nenhuma necessidade especial de configuração por parte do usuário. Redes utilizando IrDA também são conhecidas como PAN, ou Personal Area Networks. Para transmissões de dados de longo alcance, há as WLANs – Wireless Local Area Networks – que podem trafegar mais dados em menos tempo, mas que necessitam de uma configuração, mesmo que mínima, para que fiquem disponíveis para operação. Para suprir o *gap* entre as duas tecnologias citadas, isto é, para se ter uma solução intermediária em termos de configuração facilitada e alcance razoável, foi desenvolvida a tecnologia Bluetooth [3].

A tecnologia Bluetooth permite cobrir uma distância maior em termos de dispositivos conectados e formar pequenas redes, enquanto que não necessita de conhecimentos especializados a fim de configurar os dispositivos.

Neste trabalho serão descritos os pormenores da tecnologia Bluetooth, tais como protocolo e arquitetura, bem como aspectos relacionados à segurança deste tipo de comunicação.

Na seção 2, um breve histórico da tecnologia Bluetooth será apresentado. Na seção 3 será descrita a arquitetura Bluetooth. Na seção 4, é explicada a pilha de protocolos do Bluetooth, enquanto que na seção 5 serão abordadas algumas características relacionadas à segurança. As considerações finais encontram-se na seção 6.

2. BREVE HISTÓRICO

Com objetivo de eliminar os cabos das conexões entre dispositivos e desenvolver um padrão que atendesse à demanda de interconectar não só computadores, mas outros dispositivos de comunicação (ex.: celulares e PDAs) e acessórios (ex.: controles remotos, fones de ouvido, mouses) de maneira eficiente e de baixo custo, cinco companhias (Ericsson, IBM, Intel, Nokia e Toshiba) se uniram para formar um consórcio (SIG – Special Interest Group) [6]. O consórcio foi nomeado Bluetooth, em homenagem ao Rei Viking Harald "Bluetooth" Blaatand, que unificou Noruega e Dinamarca durante seu reinado (940-981) e cuja estratégia era baseada no diálogo [4].

3. ARQUITETURA BLUETOOTH

3.1 Características

De maneira similar à tecnologia Wi-Fi 802.11, Bluetooth também utiliza a faixa de freqüência de 2.4 GHz, estando sujeita aos mesmos problemas de interferência ocorridos nesta faixa de freqüência [1].

A definição do protocolo Bluetooth abrange tanto dados como voz, e é para ser utilizado por dispositivos diversos, que vão desde celulares e PDAs, até microfones e impressoras. É dividido em três classes, onde a variação se dá na potência máxima e na área de cobertura estimada [4]. A tabela 1 a seguir ilustra as classes em que os equipamentos podem ser divididos:

Tabela 1: Potência e área de cobertura por classe

Classe	Potência máxima (mW)	Potência máxima (Dbm)	Área de cobertura estimada
1	100	20	100 m
2	2.5	4	10 m
3	1	0	1 m

3.2 Arquitetura

Um sistema Bluetooth pode ser composto por oito dispositivos separados por uma distância de 10 metros entre si, sendo um nó mestre e até sete nós escravos ativos. Podem haver até 255 outros nós na rede, colocados em estado suspenso pelo nó mestre, a fim de economizar bateria. Um dispositivo suspenso tem por função apenas responder a sinais de ativação ou sinalização (*beacon*) enviados pelo mestre, o qual pode suspender dispositivos e ativar outros, desde que obedecendo ao limite de 8 nós ativos [1].

O conjunto dos dispositivos interconectados da maneira supracitada é chamado de *piconet* [2], pois forma uma pequena rede de comunicação entre eles. A Figura 1 mostra um exemplo de *piconet.*

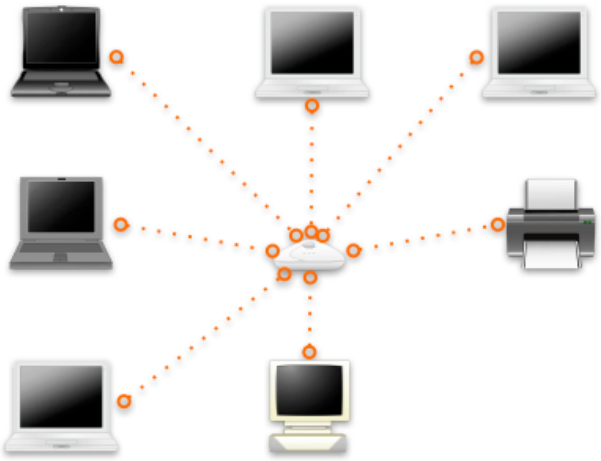

Figura 1: Vários nós escravos conectados a um mestre formando uma piconet

Caso um dos nós escravos seja configurado em modo *bridge* e permitir a interligação de uma ou mais *piconets*, forma-se uma *scatternet* [6]. Assim, a *scatternet* é a rede formada pela interconexão de diversas *piconets* presentes em um ambiente, como ilustrado na Figura 3.2.

A arquitetura mestre-escravo facilita a redução de custo e economia de bateria, uma vez que o mestre controla a comunicação entre os escravos, os quais apenas efetuam as ações que lhes são comandadas.

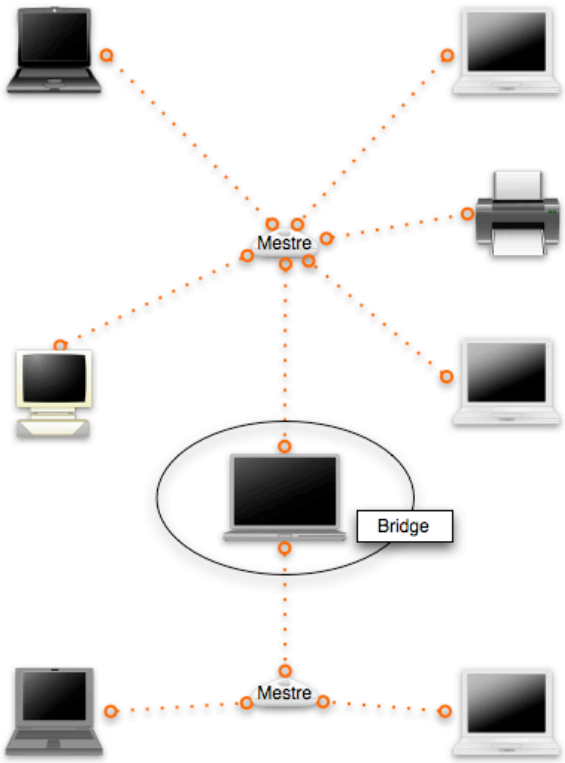

Figura 2: Uma scatternet formada por duas piconets

4. A PILHA DE PROTOCOLOS

O padrão Bluetooth é composto por diversos protocolos agrupados em camadas, conforme pode-se visualizar na Figura 3.

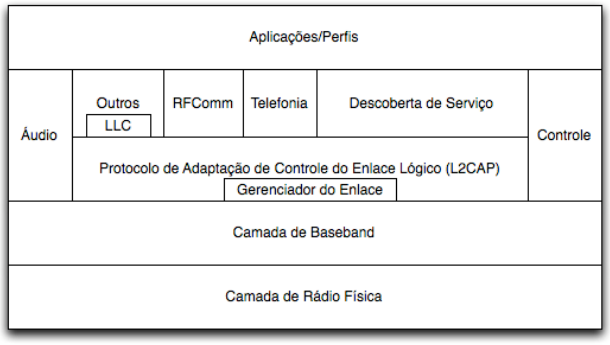

Figura 3: Arquitetura Bluetooth segundo padrão IEEE 802.15

A arquitetura básica dos protocolos que correspondem ao padrão Bluetooth é dividida em camada física de rádio; camada de *baseband*; uma camada (L2CAP) com alguns protocolos relacionados entre si e que, junto com a camada de *baseband*

corresponde à camada de enlace de dados; a camada de *middleware* e a camada de aplicações [1].

4.1 Camada de Rádio

A camada de rádio tem por função movimentar os bits entre nós mestre e escravo. Nesta camada ocorre a emissão dos sinais e alocação de canais, na qual o mestre estabelece a seqüência de salto entre os canais e todos os nós da piconet saltam ao mesmo tempo, através de FHSS (*Frequency Hopping Spread Spectrum*). A banda utilizada (ISM 2.4 GHZ) é dividida em 79 canais de 1 MHz e a taxa de dados é de aproximadamente 1 Mbps.

4.2 Camada de Baseband

A função da camada de *baseband* é transformar um fluxo de bits em frames, bem como definir alguns formatos importantes, como a divisão de *slots* de tempo para comunicação dos dispositivos mestre e escravos. Por padrão, um nó mestre de uma piconet define *slots* de 625 micro segundos, sendo que as transmissões do mestre são iniciadas nos *slots* pares e as dos escravos iniciam-se nos *slots* ímpares.

Para a transmissão dos frames, é estabelecido um link entre o mestre e o escravo, o qual pode ser assíncrono (ACL – *Asynchronous Connection-Less*) ou síncrono (SCO – *Synchronous Connection Oriented*).

Os links do tipo ACL são utilizados por dados enviados em intervalos irregulares e entregues seguindo a filosofia do melhor esforço, ou seja, não há garantias de que os dados cheguem íntegros ou que não haja necessidade de retransmissão devido à corrupção ou perda de pacotes.

Os links do tipo SCO são utilizados normalmente para dados que necessitam ser trafegados em tempo real e, portanto, possuem prazos críticos de tempo. Neste caso, é alocado um slot fixo para cada direção de tráfego e os frames não são retransmitidos em caso de perda.

4.3 Camada L2CAP

Nesta camada são tratados o gerenciamento de potência, autenticação e qualidade de serviço, correspondendo ao estabelecimento dos canais lógicos entre os dispositivos. Para encapsular os detalhes de transmissão enviados para camadas superiores, há o protocolo de adaptação de controle do enlace lógico (L2CAP – *Logical Link Control Adaptation Protocol*), que nomeia a camada. Suas três principais funções são:

- Receber pacotes das camadas superiores e dividí-los em frames para transmissão, a fim de que sejam remontados no destino, sendo que os pacotes devem respeitar o limite de 64 KB;
- Gerenciar a multiplexação e demultiplexação dos pacotes provenientes de origens distintas, determinando qual protocolo de camada superior irá tratá-los quando da remontagem destes;
- Gerenciar os requisitos de qualidade de serviço tanto durante o estabelecimento dos links como na operação normal.

4.4 Camada de Middleware

Na camada de *middleware* repousam protocolos relacionados com outros padrões – como *Wireless Application Protocol* (WAP), *Transmission Control Protocol* (TCP), *Internet Protocol* (IP) – e protocolos de terceiros ou de interesse, como o protocolo de descoberta de serviço, o qual possibilita que dispositivos obtenham informações sobre serviços disponíveis em outros dispositivos Bluetooth.

4.5 Camada de Aplicações e Perfis

Diferentemente de outros protocolos de rede, como por exemplo o 802.11, a especificação do Bluetooth elege aplicações específicas para ser suportadas e provê suas respectivas pilhas de protocolos. São 13 as aplicações definidas pelo Bluetooth SIG, e estas aplicações são denominadas **perfis**, os quais estão identificados e descritos na Tabela 2 a seguir.

Tabela 2: Perfis definidos pelo Bluetooth SIG como aplicações suportadas pelo protocolo

Nome	Descrição
Acesso genérico	Procedimentos para gerenciamento do enlace
Descoberta de serviço	Protocolos para descoberta de serviços oferecidos
Porta serial	Reposição para cabo de porta serial
Troca de objetos genérica	Define relacionamento cliente-servidor para movimentação de objeto
Acesso à LAN	Protocolo entre computador móvel e LAN fixa
Conexão discada	Permite a um laptop efetuar chamadas via telefone móvel
Fax	Permite a um aparelho móvel de fax conversar com um telefone móvel
Telefonia sem fio	Conecta um aparelho de telefone sem fio e sua estação-base local
Intercom	Walkie-talkie digital
Headset	Comunicação *hands-free*
Push de objetos	Provê troca simples de objetos
Transferência de arquivos	Provê transferência de arquivos geral
Sincronização	permite a um PDA sincronizar com outro computador

5. SEGURANÇA EM BLUETOOTH

As tecnologias wireless possuem problemas inerentes de segurança devido ao meio físico não ser auto-contido (como um cabo de rede) e a comunicação dar-se por intermédio de ondas eletromagnéticas as quais podem ser facilmente interceptadas.

Os riscos a que as comunicações Bluetooth estão submetidos podem ser divididos basicamente em [4]:

- Captura de tráfego (escuta);
- Negação de serviço;
- Forja de identidade;
- Configuração padrão e força bruta
- Acesso não autorizado;

Estes riscos, quando explorados ou combinados, causam problemas de violação de integridade, confidencialidade ou disponibilidade da *piconet* e dos dados dos dispositivos/usuários conectados a ela. A seguir, serão detalhados os riscos citados.

5.1 Captura de Tráfego

Uma vez que o meio de transmissão das comunicações envolvendo Bluetooth é o não guiado, a captura de tráfego torna-se uma tarefa simples. Basta se utilizar de uma ferramenta de análise de tráfego, mais conhecida pelo nome de *sniffer* e escutar o tráfego em fluxo.

Existem ferramentas para escuta de tráfego de rede tradicionais para uso em sistemas *unix-like* e plataforma Microsoft, como *tcpdump* e *Wireshark*, bem como ferramentas próprias para escuta em Bluetooth, como o *hcidump*.

A captura de tráfego pode fornecer informações sensíveis sobre a comunicação, tais quais as características deste tráfego, seqüências de comandos, senha (PIN) e arquivos (fotos, dados) transmitidos [5].

Nos dispositivos cabeados, a dificuldade da escuta está no acesso físico aos equipamentos. Nos dispositivos *wireless*, a dificuldade é centrada na distância entre o atacante e o alvo, sendo que nos equipamentos Bluetooth esta distância chega a cerca de 250 metros.

5.2 Negação de Serviço

Ataques de negação de serviço são comuns em redes de computadores e, se bem orquestrados, muito difíceis de serem evitados. Este tipo de ataque consiste na indisponibilização do uso do equipamento, fazendo-o deixar de comunicar-se com a rede ou com outros dispositivos temporariamente.

No caso da tecnologia Bluetooth, uma negação de serviço pode simplesmente consistir do envio de pacotes um pouco maiores ou do envio massivo de pacotes, fazendo com que o dispositivo alvo não consiga tratar o tráfego e comece a descartá-lo, bem como toda e qualquer conexão estabelecida ou tentativas de estabelecimento enquanto sob ataque.

Outra maneira de causar negação de serviço em Bluetooth é baseada na geração de ruído, ou *jamming*, seja através da identificação da seqüência de saltos na mesma ordem de freqüência dos dispositivos envolvidos, seja através do preenchimento de boa parte do espectro com tráfego de ruído.

5.3 Forja de Identidade

Para que um dispositivo Bluetooth estabeleça uma comunicação com outro e troque dados, é feita uma autenticação entre eles, na qual é combinada uma senha que pode ser memorizada nas partes envolvidas. Quando essa autenticação é feita, também é estabelecida uma relação de confiança entre os dispositivos, e a falsificação das credenciais de um dos dispositivos por um terceiro pode fazer com que este tenha acesso ao dispositivo alvo, fazendo-se passar pela parte autorizada.

Tanto a forja de identidade como a captura de tráfego podem levar ao roubo de informações, uma vez que na captura de tráfego, escuta-se a transmissão e é possível obter credenciais que possibilitem a forja de identidade.

5.4 Configuração Padrão e Força Bruta

Tratam-se de problemas de autenticação que permitem que um dispositivo seja acessado com suas próprias credenciais.

No caso da configuração padrão, o atacante tenta utilizar um PIN pré-determinado pelo fabricante para aquele tipo de equipamento, identificado através de uma varredura por dispositivos Bluetooth e suas características. Caso o dispositivo esteja configurado para aceitar conexões sem a solicitação de confirmação e o usuário não tiver trocado o seu PIN, o ataque será concretizado com sucesso.

No ataque de força bruta, o atacante tenta descobrir o PIN através do esgotamento de possibilidades, tentando todas as combinações possíveis dentro de um escopo específico.

5.5 Acesso Não Autorizado em Redes

Usuários mal intencionados podem configurar seus computadores pessoais ou mesmo concentradores Bluetooth para permitir acesso de dispositivos Bluetooth à rede cabeada ou *wi-fi* de uma organização. Com isso, um atacante sem acesso físico ou credenciais para acessar uma rede corporativa poderia se utilizar dessa ponte Bluetooth para efetuar o acesso e obter informações sensíveis. Este tipo de ataque é dificultado devido ao alcance limitado da tecnologia Bluetooth, mas é facilitado devido ao fato de que normalmente há pouca ou nenhuma monitoração de redes Bluetooth nas organizações em geral.

6. CONSIDERAÇÕES FINAIS

A tecnologia Bluetooth alcançou altos níveis de popularidade, uma vez que está presente em diversos dispositivos do dia-a-dia. Sua flexibilidade permite que seja utilizada em diversas atividades, como sincronismo de bases de dados em geral (agendas de telefone, fotos, músicas, entre outros), formação de redes ponto a ponto, possibilidade de acesso discado, integração de equipamentos em uma pequena rede (headset, impressora, celular, PC) e acesso à redes IP, por exemplo.

O Projeto Bluetooth alcançou seu objetivo de prover uma tecnologia versátil para comunicação e de baixo custo e consumo

de energia sem abrir mão da facilidade de utilização e configuração.

Enquanto que a arquitetura e protocolos do padrão Bluetooth são bem definidos e limitados em escopo, este tipo de rede padece das mesmas vulnerabilidades encontradas nas redes sem fio padrão 802.11, devido à inerência de problemas no meio não-guiado.

Espera-se que, com a cada vez mais crescente utilização de dispositivos Bluetooth, sejam desenvolvidas mais métodos de segurança e formas para monitoração das redes Bluetooth, visando a autenticação e auditoria do ambiente.

7. REFERÊNCIAS

[1] Tanenbaum, A. S. Computer Networks, 4th Edition. Prentice Hall, 2003. ISBN 0-13-066102-3.

[2] Kurose, J. F. and Ross, K. W. Computer Networking: A Top-Down Approach Featuring the Internet, 2nd Edition. Addison Wesley, 2003. ISBN 0-201-97699-4.

[3] Peikari, C. and Fogie, S. Wireless: Maximum Security. Sams, 2002. ISBN 0-672-32488-1

[4] Rufino, N. M. Segurança em Redes sem Fio. Novatec, 2005. ISBN 85-7522-070-5.

[5] Rufino, N. M. Bluetooth e o Gerenciamento de Riscos. 2005. In: 5a Reunião do Grupo de Trabalho em Segurança (GTS), São Paulo, 2005. Disponível em: ftp://ftp.registro.br/pub/gts/gts0105/05-gts-bluetooth.pdf (acessado em 02/07/2009).

[6] Bluetooth SIG. Specification of the Bluetooth System v. 1.2. 2003. Disponível em: http://www.bluetooth.com (acessado em 02/07/2009).