

Mestrado em Sistemas Móveis
Seminário sobre Bluetooth
Relatório

Jorge Cardoso

7 de Fevereiro de 2007

Conteúdo

1	Introdução	3
1.1	Bluetooth	3
1.2	Tecnologias e <i>Standards</i> de Redes sem Fios	3
1.3	Redes de Sensores sem Fios	4
1.4	Estrutura deste Relatório	4
2	A Tecnologia Bluetooth	5
2.1	História	5
2.2	Arquitectura	6
2.3	Redes	8
2.4	Perfis	8
2.5	Descoberta de Dispositivos e Serviços	10
2.6	Bluetooth e os Sistemas Móveis	11
2.6.1	Sistemas de Posicionamento	11
2.6.2	Redes e Contextos Sociais	11
2.6.3	Arte	12
2.6.4	Segurança	12
3	Conclusão	13

Capítulo 1

Introdução

O objectivo deste relatório é descrever o seminário intitulado “Bluetooth” apresentado no âmbito do Mestrado em Sistemas Móveis da Universidade do Minho, em Novembro de 2006.

Para além da tecnologia Bluetooth, o seminário abordou os temas das Tecnologias e Standards de Redes sem Fios e das Redes de Sensores sem Fios. No entanto, este relatório foca apenas a tecnologia Bluetooth uma vez que foi também este o tema principal do seminário. Uma descrição breve dos vários temas do seminário é apresentada mais à frente neste capítulo.

Este relatório apresenta uma visão de mais alto nível do que a apresentada no seminário. Os detalhes de funcionamento do protocolo apresentados no seminário são deixados de lado em favor de uma descrição mais genérica e de uma abordagem mais direccionada ao arquitecto ou programador de software de aplicação.

As fontes utilizadas neste relatório foram, para além dos *slides* fornecidos pelo professor [1, 3, 2], diversos livros e outros documentos para os quais faço referências ao longo do relatório de forma a que o leitor mais interessado possa investigar mais aprofundadamente cada assunto.

1.1 Bluetooth

O Bluetooth é um protocolo de comunicação sem fios desenhado para interligar computadores e periféricos de forma ad-hoc e com um baixo custo. Estas características, aliadas à grande disseminação de dispositivos que implementam esta tecnologia, tornam o Bluetooth um protocolo incontornável no estudo e desenho de sistemas móveis.

1.2 Tecnologias e *Standards* de Redes sem Fios

Existem vários *standards* de redes de comunicação sem fios, todos eles com características diferentes – largura de banda, custo, alcance, etc. A utilização

de um ou de outro depende da aplicação que se pretende fazer da tecnologia pelo que é importante conhece-los e perceber as características de cada um. Isto é particularmente importante no caso dos sistemas móveis, uma vez que, tipicamente, se pretende desenvolver sistemas autónomos, que possam comunicar sem fios e com o menor custo possível.

1.3 Redes de Sensores sem Fios

As redes de sensores sem fios são um caso particular dos sistemas de redes sem fios principalmente devido às limitações do hardware utilizado na construção dos sensores. Normalmente, as aplicações nesta área implicam a utilização de um grande número de dispositivos e, por isso, é necessário construir sensores de baixo custo, com hardware simples e com baixo consumo energético. Isto implica que o sistema de comunicação seja também ele o mais simples possível. O protocolo IEEE 802.15.4/Zigbee [24] é um protocolo desenvolvido com estas aplicações em mente.

1.4 Estrutura deste Relatório

Este relatório está estruturado nos seguintes capítulos:

- O Capítulo 2 é o núcleo deste relatório. Descreve a tecnologia Bluetooth apresentando alguma da sua história; descreve a arquitectura do protocolo, o seu funcionamento, os perfis e também algumas aplicações de diversas áreas que utilizam o Bluetooth.
- o Capítulo 3 apresenta uma pequena conclusão do relatório.

Capítulo 2

A Tecnologia Bluetooth

O Bluetooth é um protocolo que descreve uma tecnologia de comunicação sem fios, de curto alcance, de baixo consumo e baixo custo. O objectivo do Bluetooth é substituir os cabos utilizados para interligar dispositivos como telemóveis, auriculares, PCs, PDAs, teclados, ratos, etc. A especificação Bluetooth [5] é mantida pelo Bluetooth SIG (*Bluetooth Special Interest Group*) – um grupo de empresas de várias áreas (telecomunicações, computação, indústria automóvel, música, automação industrial, etc), do qual fazem parte, entre outras, a Sony Ericsson, Intel, IBM, Toshiba, Microsoft, Nokia, 3COM e Motorola. Mais informação sobre o Bluetooth SIG pode ser encontrada em [7] e [6].

2.1 História

A ideia que levou ao surgimento do Bluetooth começou em 1994 quando os engenheiros da Ericsson começaram a pensar em utilizar tecnologia de comunicação rádio para interligar os telemóveis e os acessórios dos telemóveis.

A ideia amadureceu e a empresa começou a contactar outros fabricantes que pudessem estar interessados na tecnologia e, em 1998, as empresas Ericsson, IBM, Intel, Nokia e Toshiba, formaram o Bluetooth SIG.

O nome “Bluetooth” deriva do nome de um rei Dinamarquês do século X – Harald Blatand, ou Harold Bluetooth em Inglês – que foi fundamental na união dos povos do que é hoje a Noruega, Suécia e Dinamarca. A ideia para este nome surgiu numa discussão em que se tentava encontrar um nome de código para a tecnologia. O facto de o Bluetooth permitir a colaboração entre indústrias diferentes permitiu estabelecer um paralelo com o feito do rei Harald Blatand.

O leitor interessado pode aprofundar a história do aparecimento e desenvolvimento do Bluetooth em [17] e em [7].

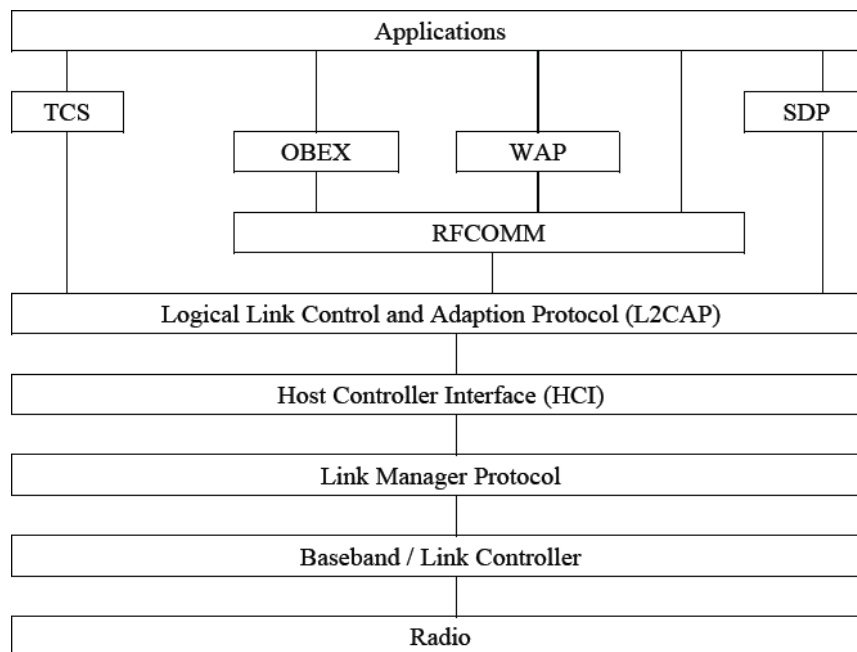


Figura 2.1: Pilha protocolar Bluetooth

2.2 Arquitectura

A especificação Bluetooth consiste numa pilha protocolar completa, que especifica não só o sistema de rádio mas também um conjunto de outros protocolos destinados a garantir que diferentes dispositivos, de diferentes fabricantes possam comunicar uns com os outros.

A pilha protocolar Bluetooth é apresentada na Figura 2.1¹.

A pilha é composta por várias camadas, umas tipicamente implementadas em hardware (camadas abaixo do HCI), outras em software (camadas acima do HCI). As camadas são as seguintes:

Radio Realiza a modulação e demodulação dos dados para transmissão e recepção através de rádio-frequência.

Baseband and Link Controller Especificação das operações de baixo nível (ao nível do bit e do pacote).

Link Manager Protocol Estabelecimento de ligações para outros dispositivos.

Host Controller Interface (HCI) Gere a comunicação entre o módulo Bluetooth e o dispositivo anfitrião.

¹Retirada de [15].

Logical Link Control and Adaptation Protocol Fornece serviços “connection-oriented” e “conectionless” às camadas superiores. Realiza multiplexagem de protocolos, segmentação e assemblagem de dados. O L2CAP suporta apenas ligações ACL (dados) e não SCO (áudio).

RFCOMM Fornece uma interface para emulação de porta série sobre rádio-frequência.

OBEX O OBEX (OBject EXchange) é um protocolo para transferência de objectos binários.

WAP Suporte para o protocolo WAP sobre Bluetooth que permite aceder a conteúdos residentes noutros dispositivos Bluetooth.

Telephony Control System (TCS) Permite controlar o dispositivo através de comandos AT.

Service Discovery Protocol (SDP) Protocolo utilizado para procurar outros dispositivos Bluetooth.

Applications As aplicações implementadas sobre Bluetooth.

O Bluetooth opera através de transmissões de rádio, o que significa que, ao contrário dos infravermelhos, não necessita de uma “linha de visão” entre os dispositivos para funcionar. Para diminuir o risco de interferência por parte de outros dispositivos, o Bluetooth utiliza a técnica “Frequency Hopping Spread Spectrum” (FHSS) que consistem em dividir a banda de frequências em diversos canais e “saltar” continuamente entre esses canais.

Cada dispositivo Bluetooth possui um identificador universal – UUID (Universally Unique Identifier) – atribuído durante o fabrico do módulo Bluetooth. Estes identificadores de 48 bits são equivalentes aos endereços MAC das placas de rede e servem, para além da identificação do dispositivo, para a sincronização do “frequency hopping” entre os dispositivos que pretendem comunicar entre si.

O hardware Bluetooth pode ser construído para emitir sinais de diferentes potências. A potência do sinal emitido define o alcance da comunicação. A especificação define três classes de potência. A Tabela 2.1 mostra a relação entre as classes de potência, a potência máxima e o alcance da comunicação.

Classe	Potência Máxima	Distância²
1	100mW	100 metros
2	2.5mW	20 metros
3	1 mW	10 metros

Tabela 2.1: Classes de potência Bluetooth

²Estes valores baseiam-se em [14].

2.3 Redes

Quando dispositivos Bluetooth necessitam de comunicar é necessário primeiro criar uma rede. Existem dois tipos de redes Bluetooth: Piconets e Scatternets.

Uma piconet é uma rede formada por um dispositivo *mestre* e por um, ou vários dispositivos *escravos*, até um máximo de sete. O mestre é o dispositivo que inicia a comunicação. A Figura 2.2³ mostra uma rede piconet com um mestre e quatro escravos.

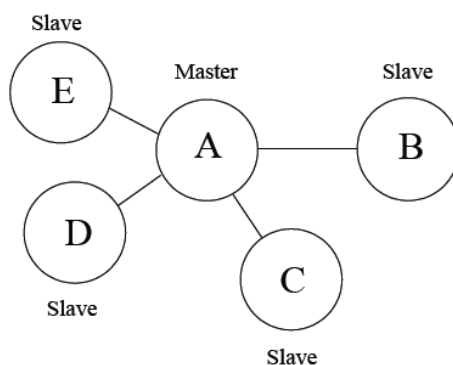


Figura 2.2: Uma rede piconet

Se o mesmo dispositivo for escravo em duas piconets, então estamos na presença de uma *scatternet*. A Figura 2.3⁴ mostra uma scatternet formada por sete dispositivos.

2.4 Perfis

O Bluetooth é um protocolo genérico que pode ser utilizado numa gama muito diversa de dispositivos, com funções muito diversas. Para além disso, implementar toda a especificação Bluetooth seria demasiado dispendioso, pelo que os dispositivos implementam, normalmente, apenas uma pequena parte. Para garantir que dois dispositivos conseguem comunicar entre si, por exemplo para garantir que podemos trocar ficheiros vCard entre um PDA e um telemóvel, ou que podemos usar o modem do telemóvel para aceder à Internet a partir do PDA, foram definidos perfis.

Um perfil é um conjunto de funcionalidades, que obviamente definem que parte da pilha protocolar Bluetooth o dispositivo deverá implementar. Alguns dos perfis definidos são descritos a seguir. Mais informação sobre os perfis Bluetooth pode ser encontrada em [11].

³Retirada de [15].

⁴Retirada de [15].

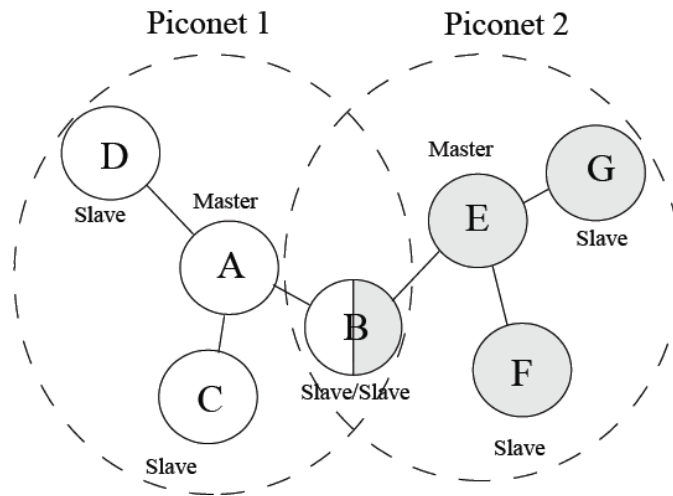


Figura 2.3: Uma rede scatternet

Generic Access Profile (GAP) Perfil que serve de base a todos os outros. Define os procedimentos básicos de descoberta e gestão de ligações.

Service Discovery Application Profile Define os procedimentos e funcionalidades para uma aplicação num dispositivo Bluetooth descobrir serviços e informação sobre os serviços registados noutros dispositivos.

Serial Port Profile (SPP) Define os requisitos para emulação de porta série sobre Bluetooth.

Cordless Telephony Profile Define os procedimentos necessários para a utilização de telemóveis para receber e efectuar chamadas através linhas terrestres, como se se tratasse de um telefone fixo.

Intercom Profile Define os requisitos para a utilização de telemóveis como intercomunicadores.

Headset Profile Usado para ligar auriculares Bluetooth a telemóveis.

Dial-Up Networking Profile Permite utilizar o modem de dispositivo Bluetooth para o acesso à Internet por outro dispositivo Bluetooth.

Fax Profile Define como um telemóvel ou modem podem ser utilizados por um PC para enviar e receber mensagens de fax.

Generic Object Exchange Profile Este perfil serve de base a todos os outros perfis que necessitem de utilizar o protocolo OBEX.

Object Push Profile Este perfil permite a troca de alguns tipos de ficheiros entre dispositivos, por exemplo vCards. O OBEX é utilizado para o envio de ficheiros.

File Transfer Profile Este perfil é mais genérico do que o anterior e permite transferir qualquer tipo de ficheiros ou pastas entre dispositivos.

Synchronization Profile Define os procedimentos necessários para a sincronização de dados entre dispositivos.

2.5 Descoberta de Dispositivos e Serviços

Antes de um dispositivo iniciar uma ligação a outro, é necessário conhecer o seu “endereço” e as suas capacidades. O Bluetooth define uma forma de encontrar dispositivos ao alcance do dispositivo que pretende comunicar e de inspeccionar os serviços (capacidades) desses dispositivos.

Este processo é designado por descoberta (“discovery”, ou “inquiry”). Existem dois tipos de descoberta: descoberta de dispositivos (“device discovery”) e descoberta de serviços (“service discovery”) disponibilizados por um dispositivo.

Para um dispositivo poder ser descoberto por outros é necessário que esteja em modo de descoberta (“inquiry scan”). Neste modo, outros dispositivos podem obter o endereço desse dispositivo. Normalmente todos os dispositivos permitem que o utilizar defina se pretende que o dispositivo seja descoberto, ou não.

Alguns dispositivos permitem definir um “timeout” para o modo de descoberta, findo o qual o dispositivo volta ao modo invisível (deixa de poder ser descoberto por outros dispositivos). O facto de um dispositivo estar invisível não significa que não possa aceitar ligações de outros dispositivos, apenas que o seu endereço deixa de ser anunciado. Se outro dispositivo já tiver conhecimento do endereço do dispositivo com o qual pretende estabelecer ligação, pode fazê-lo, mesmo que o outro dispositivo esteja invisível.

Diferentes dispositivos Bluetooth têm diferentes funcionalidades. Para um dispositivo determinar que pode estabelecer comunicação com outro é necessário saber se as funcionalidades são compatíveis entre os dois. Para isso é necessário realizar uma descoberta de serviços no dispositivo remoto. O resultado será um conjunto de identificadores de serviços disponíveis nesse dispositivo. Por exemplo, para um dispositivo poder transferir um ficheiro para outro dispositivo é necessário que ambos possuam o serviço OBEX File Transfer.

2.6 Bluetooth e os Sistemas Móveis – Exemplos de Aplicações

Apesar de o Bluetooth ter sido criado como um protocolo de comunicação, as suas características tornam-no atractivo para aplicações que o utilizam para além da sua função de comunicação.

Esta secção descreve algumas aplicações que tiram partido do Bluetooth em áreas tão diversas como localização, redes sociais e arte. Esta lista não pretende ser exaustiva, outras aplicações poderão ser encontradas seguindo as referências dos sítios web e artigos referidos neste relatório.

2.6.1 Sistemas de Posicionamento

Em [13], os autores avaliam a potencialidade do Bluetooth para a implementação de sistemas de posicionamento. Os autores implementaram dois modos diferentes de posicionamento: um modo directo, em que o dispositivo Bluetooth tem de ser programado para efectuar a tarefa de posicionamento e um modo indirecto, em que os dispositivos são passivos.

2.6.2 Redes e Contextos Sociais

A facto de o Bluetooth funcionar com base na descoberta de outros dispositivos fisicamente próximos permite explorar a presença e os padrões de presença dos utilizador em vários locais.

O sistema MobiTip [23], consiste numa aplicação móvel que permite aos utilizadores realizarem comentários e partilhá-los com outros utilizadores na proximidade ou registá-los em *hotspots* instalados em vários locais. MobiTip utiliza o Bluetooth para a detecção de proximidade e para a partilha de informação.

A Nokia disponibiliza ao público ([20]) desde 2005 a aplicação Nokia Sensor [22]. O Nokia Sensor consiste numa aplicação móvel que permite comunicar com utilizadores na proximidade, utilizando o Bluetooth para a detecção de utilizadores e para a comunicação. A aplicação permite partilhar preferências de utilizadores, mensagens instantâneas, ficheiros, etc.

Os autores de Wireless Rope [18, 19] procuram estudar o contexto social através da análise da proximidade pessoal. Para isso desenvolveram uma aplicação para telemóvel e para desktop que utiliza o Bluetooth para a detecção de proximidade.

A intenção dos autores de Jabberwocky [21, 4] é semelhante à dos de Wireless Rope. Uma aplicação para telemóvel regista os “encontros” com outros dispositivos Bluetooth e representa graficamente a relação de familiaridade entre as pessoas com base no histórico de encontros.

2.6.3 Arte

O facto de ser possível detectar dispositivos Bluetooth nas proximidades de um local pode levantar questões de privacidade das quais, provavelmente, os utilizadores dos dispositivos não estão cientes. Por outro lado, a presença dos utilizadores num dado local pode ser explorado artisticamente, de várias formas.

O projecto Loca [16, 10] é uma acção artística de vigilância através da detecção de dispositivos Bluetooth em pontos determinados de uma cidade. Através da análise do percurso das pessoas, os autores pretendem enviar mensagens em que fica claro para essas pessoas que os seus passos foram seguidos.

O projecto DiABlu [9] consiste numa ferramenta (disponível em [8]) com o objectivo de permitir a fácil utilização do conhecimento sobre dispositivos Bluetooth presentes na proximidade de um computador por parte da comunidade artística.

2.6.4 Segurança

As falhas de segurança do protocolo Bluetooth têm sido exploradas pelo grupo triffinite.org [12]. Este grupo desenvolve, como provas de conceito, aplicações que tiram partido das vulnerabilidades do protocolo. As aplicações vão desde injeção de áudio em auriculares Bluetooth, até ao descarregamento não autorizado de listas de contactos de telemóveis.

Capítulo 3

Conclusão

A tecnologia Bluetooth é mais do que apenas uma substituição dos fios para interligar dispositivos. As funcionalidades de descoberta de dispositivos tornam-na também num mecanismo de localização de pessoas e objectos. A ubiquidade da sua implementação faz com que seja também uma forma de permitir interacção entre pessoas e aplicações que normalmente não permitiriam interacção.

O Bluetooth pode ser, no entanto, também uma fonte de preocupações relativas à privacidade e à segurança dos dados. O facto de utilizar um meio aberto para as comunicações podem torná-las potencialmente inseguras. O desconhecimento ou a despreocupação por parte dos utilizadores tornam-na também num mecanismo para seguir pessoas, pondo em causa a sua privacidade.

Bibliografia

- [1] José Augusto Afonso. Bluetooth. Slides do Seminário do Mestrado em Sistemas Móveis, Universidade do Minho, November 2006.
- [2] José Augusto Afonso. Redes de Sensores sem Fios IEEE 802.15.4/Zigbee. Slides do Seminário do Mestrado em Sistemas Móveis, Universidade do Minho, November 2006.
- [3] José Augusto Afonso. Tecnologias e Standards de Redes sem Fios. Slides do Seminário do Mestrado em Sistemas Móveis, Universidade do Minho, November 2006.
- [4] Urban Atmospheres. Jabberwocky . Website, Visited January 2007. <http://www.urban-atmospheres.net/Jabberwocky/>.
- [5] Bluetooth SIG. Specification of the Bluetooth System version 1.2. Technical report, November 2003.
- [6] Bluetooth SIG. The Bluetooth Technology Web Site. Website, Visited December 2006. <http://www.bluetooth.com>.
- [7] Bluetooth SIG. The Official Bluetooth Membership Site. Website, Visited December 2006. <http://www.bluetooth.org>.
- [8] Jorge Cardoso. DiABlu Project. Website, Visited January 2007. <http://diablu.jorgecardoso.org>.
- [9] Jorge Cardoso and Nuno Rodrigues. Diablu: Digital arts' bluetooth. In *Proceedings of the Artech 2006 Conference*, Pontevedra, Spain, November 2006.
- [10] John Evans, Drew Hemment, Theo Humphies, and Mika Raento. Loca: Location oriented critical arts. Website. <http://leoalmanac.org/gallery/locative/loca/index.htm>.
- [11] Dean A. Gratton. *Bluetooth Profiles*. Prentice Hall PTR, 1st edition, 2002.

- [12] Trifinite Group. Trifinite.org. Website. http://trifinite.org/trifinite_org.html.
- [13] J. Hallberg, M. Nilsson, and K. Synnes. Positioning with bluetooth. In *Telecommunications, 2003. ICT 2003. 10th International Conference on*, volume 2, pages 954–958 vol.2, 2003.
- [14] B. Hopkins and R. Antony. *Bluetooth for Java*. Apress, 2003.
- [15] André N. Klingsheim. J2ME Bluetooth Programming. Master’s thesis, Department of Informatics, University of Bergen, June 2004.
- [16] Loca. Loca. Website, Visited January 2007. <http://www.loca-lab.org/>.
- [17] Michael Miller. *Discovering Bluetooth*. Sybex, 2001.
- [18] Tom Nicolai, Nils Behrens, and Eiko Yoneki. Wireless rope: Experiment in social proximity sensing with bluetooth. In *Fourth Annual IEEE International Conference on Pervasive Computing*, Pisa, Italy, 2006.
- [19] Tom Nicolai, Eiko Yoneki, Nils Behrens, and Holger Kenn. Exploring social context with the wireless rope. In *1st International Workshop on MOBILE and NETWORKING Technologies for social applications (MONET’06)*, Montpellier, France, 2006.
- [20] Nokia. Nokia Sensor. Website, Visited January 2007. <http://www.nokia.com/sensor>.
- [21] Eric Paulos and Elizabeth Goodman. The familiar stranger: anxiety, comfort, and play in public places. In *CHI ’04: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 223–230, New York, NY, USA, 2004. ACM Press.
- [22] Per Persson and Younghee Jung. Nokia sensor: from research to product. In *DUX ’05: Proceedings of the 2005 conference on Designing for User eXperience*, page 53, New York, NY, USA, 2005. AIGA: American Institute of Graphic Arts.
- [23] R. Svensson, M. Cster, and R. Hk. Mobitip: Using bluetooth as a mediator of social context, 2004.
- [24] Zigbee Alliance. Zigbee Alliance. Website, Visited January 2007. <http://www.zigbee.org/>.