Estudo do Protocolo de Comunicação Zigbee

João V. C. P. Dutra, Leonardo M. Franco, Pedro H. C. Macaiba, Evandro C. Vilas Boas
Laboratório de Cyber Segurança e Internet das Coisas (CS&I Lab.), Instituto Nacional de Telecomunicações - Inatel
joao.dutra@gec.inatel.br, leonardo.franco@ges.inatel.br, pedro.hugo@ges.inatel.br, evandro.cesar@inatel.br

***Abstract*—This work presents a study on the ZigBee communication protocol, carried out as a requirement for developing engineering projects with the company Pixel TI. Basic concepts, architectures, standards, aspects related to frequency bands and transmission rates, devices, network topologies, and communication are highlighted. Due to Pixel TI's confidentiality policies, project activities and results are omitted.**

***Index Terms*—IEEE 802.15.4, Internet of Things, communication protocol, ZigBee.**

***Resumo*—Esse trabalho apresenta um estudo sobre o protocolo de comunicação ZigBee, realizado como requisito para o desenvolvimento de projetos de engenharia com a empresa Pixel TI. Abordam-se os conceitos básicos, arquiteturas e padrões, aspectos relacionados às faixas de frequência, taxas de transmissão, dispositivos, topologias de rede e comunicação entre dispositivos. Devido às políticas de sigilo da Pixel TI, as atividades de projeto são omitidas desse documento.**

***Palavras chave*—IEEE 802.15.4, Internet das COisa, protocolo de comunicação, ZigBee.**

I. Introdução

A Internet das Coisas (IoT, *Internet of Things*) se refere a interconexão digital de dispositivos eletrônicos por meio da Internet ou uma rede de telecomunicações [1]. A conexão entre esses aparelhos permite o controle remoto de suas funções e/ou o sensoriamento de aspectos naturais e humanos. Logo, introduz-se a possibilidade de conexão de dispositivos eletrônicos e o uso de sensores em conjunto com atuadores. Dessa forma, pode-se controlar as funcionalidades desses dispositivos, sensorear e/ou atuar sobre determinada variável de um ambiente. A aplicação IoT se estende às mais diversas verticais do mercado como ambientes inteligentes (*Smart House*, *Smart Labs*, *Smart Offices*), cidades inteligentes (*Smart Cities*), fazendas inteligentes (*Smart Farm*) e Indústria 4.0 [2].

Esses diversos cenários de aplicações IoT requerem diferentes requisitos de comunicação, resultando na padronização de diferentes protocolos de comunicação. A implementação de uma aplicação ou rede IoT relaciona-se com a seleção adequada da tecnologia para atender requisitos como alcance, consumo de energia, largura da banda, qualidade de serviço, custo e ciclo de vida das baterias [2]. Cada requisito especifica diversas características que podem ser aplicadas para classificar os diferentes protocolos de comunicação IoT existentes. Por exemplo, pode-se empregar o alcance como métrica para classificação dos protocolos em tecnologias de conectividade sem fio de curto, médio e longo alcance.

Dentre os diversos protocolos de comunicação IoT, citam-se Bluetooth Low Energy, Zigbee, Z-Wave, 6LowPAN (IPv6 sobre Redes Pessoais Wireless de Baixa Potência), Identificação de Radiofrequência (*Radio Frequency Identification*, RFID), Comunicação *Near Field* e WiFi (*Wireless Fidelity*), que são padronizações de curto alcance. Já os protocolos SigFox, Lora, Random Phase Multiple Access e Weightless exemplificam protocolos de médio e longo alcance.

Fig. 1. Arquitetura de camada do protococo de comunicação ZigBee.

Nesse trabalho, apresenta-se um estudo sobre o protocolo de comunicação ZigBee realizado como requisito para o desenvolvimento de projetos de engenharia com a empresa Pixel TI. Abordam-se os conceitos básicos, arquiteturas e padrões, aspectos relacionados às faixas de frequência, taxas de transmissão, dispositivos, topologias de rede, comunicação entre dispositivos e estrutura de quadro básica. Devido às políticas de sigilo da Pixel TI, as atividades de projeto são omitidas. Estruturou-se o trabalho em cinco seções. Na Seção II, exploram-se os fundamentos relacionados ao protocolo ZigBee. Abordam-se aspectos relacionados aos tipos de dispositivos na Seção III. Na Seção IV, discorrem-se sobre as topologias de rede especificadas pelo padrão IEEE 802.15.4. Por fim, conclui-se o trabalho na Seção V.

II. Fundamentos em protocolo ZigBee

ZigBee é uma tecnologia de comunicação sem fio via rádio desenvolvida pela *ZigBee Alliance*, que emprega a especificação IEEE 802.15.4 em relação a camada física e de enlace para a formação de redes de curto alcance [3, 4]. Essa tecnologia apresenta como características curto alcance, baixo consumo de potência, baixa taxa de transmissão, especificação aberta e interoperabilidade. Aplica-se essa tecnologia para prover a comunicação de dispositivos energizados por baterias, aplicações residências como sistemas de segurança, sistemas de medida e leitura, controle de iluminação e aplicações industriais como gestão de ativos e rastreamento de pessoas [3, 4, 5].

A. Arquitetura de camadas ZigBee

O ZigBee baseia-se na arquitetura de camadas do modelo OSI (*Open System Interconnection*) para estruturação de suas camadas. Na Figura 1, especificam-se as quatro camadas que

TABELA I
CARACTERÍSTICAS DO PROTOCOLO ZIGBEE.

Frequência [MHz]	Número de canais	Modulação	Taxa de transmissão [kbps]	Técnica de espalhamento espectral
868 – 868,6	1	BPSK	20	DSSS binário
902 – 928	10	BPSK	40	DSSS binário
868 -868,6	1	ASK	250	PSSS - 20 bits
902 – 928	10	ASK	250	PSSS - 5 bits
868 -868,6	1	O-QPSK	100	Sequência de espalhamento ortogonal
902 – 928	10	O-QPSK	250	Sequência de espalhamento ortogonal
2400 – 2483,5	16	O-QPSK	250	Sequência de espalhamento ortogonal

compõem essa arquitetura, sendo as camadas de aplicação e rede definidas pelo padrão ZigBee e as camadas de enlace e física pelo padrão IEEE 802.15.4 [3, 6, 7]. A camada de aplicação é segmentada em subcamada de suporte de aplicação (ASP, *Application support Sub-layer*) e objetos de dispositivos Zigbee (ZDO, *ZigBee Device Objects*). A subcamada ASP provê a interface entre a camada de rede e a camada de aplicação através de um conjunto de serviços para uso dos dispositivos ZigBee, definidos pelos fabricantes. A subcamada ZDO está localizado entre a camada de aplicação e a subcamada de suporte de aplicação, sendo responsável por atender todos os requisitos comuns entre as aplicações operando no protocolo ZigBee.

A camada de rede é necessária para fornecer e garantir o funcionamento correto da camada MAC, além de prover uma interface de serviço adequada para a camada de aplicação com a camada de enlace. A camada de enlace fornece serviços de dados MAC (*Media Access Control*) e a interface para gerenciamento MAC. O serviço de dados MAC é responsável pela liberação da transmissão/recepção de dados do protocolo MAC. Na camada MAC está situado alguns mecanismos de segurança que podem ser utilizados para aumentar a confiabilidade dos dados transmitidos por dispositivos ZigBee, garantindo sua facilidade de manutenção e baixo consumo de energia e transmissão de dados. Por fim, a camada física é a mais próxima ao *hardware* e controla os transmissores dos dispositivos. Essa camada é responsável pela ativação e desativação dos transceptores, transmissão e recepção de dados, seleção do canal em que o transceptor irá operar e detecção de ocupação do canal.

B. Características do protocolo ZigBee

A rede ZigBee por meio do padrão IEEE 802.15.4 utiliza os padrões da camada física para relacionar suas frequências de operação. As bandas de transmissão são divididas em: 868 – 868,6 MHz (Europa), 902 - 928 MHz (América do norte) e 2400 – 2483,5 MHz (Padrão global) [3, 6]. A taxa de transmissão de dados (entre 20 a 250 kbps), o número de canais em cada banda, taxas de transmissão e técnicas de espalhamento espectral estão especificados na Tabela I [3, 4, 6].

O protocolo IEEE 802.15.4 apresenta algumas considerações em relação a operação de dispositivos entre as bandas de frequência e taxas de transmissão [3, 4, 6]. Dispositivos que operam na banda de 868 MHz devem suportar comunicações na banda de 915 MHz e vice-versa. Nas bandas de 868/915 MHz, define-se obrigatoriamente taxas de transmissão inferiores a 40kbps, sendo possível operar com taxas superiores a esse valor por meio de configuração opcionais (linha três à linha sies da Tabela I). Para a banda em 2,4 GHz, tem-se disponíveis 16 canais numerados de 11 até 26, com separação adjacente de 5 MHz. Para as bandas de 868 e 915 MHz, tem-se respectivamente 01 e 10 canais alocados que em conjunto com a modulação empregada provê diferentes taxas de transmissão.

C. Aspectos de comunicação

A comunicação ZigBee entre diversos dispositivos deve ser coordenada para que ocorra o acesso múltiplo ao meio. Nesse caso, pode-se implementar um acesso ao canal baseado em técnicas de contenção e livre de contenção [6]. Para acesso múltiplo ao meio por contenção, o IEEE 802.15.4 implementa a técnica de múltiplo acesso CSMA-CA (*Carrier Sensing Multiple Access with Colision Avoidance*). Um dispositivo que queira transmitir deve verificar se o canal está livre, caso positivo, o dispositivo aloca o canal. Dessa forma, evita-se a colisão por transmissão simultânea de estações vizinhas, que passam a reconhecer a ocupação do canal pelo dispositivo. Caso o canal esteja ocupado, o dispositivo que inicialmente queira transmitir aguarda por um tempo aleatório e repete o processo até obter direito ao uso do meio de transmissão.

Outra forma de prover o acesso múltiplo ao meio é utilizar técnicas de acesso ao canal livre de contenção. Nesse caso, cada dispositivo possui um *slot* dedicado eliminando o uso da técnica CSMA-CA. O dispositivo coordenador da rede utiliza mensagens de sincronismo para garantir o tempo de *slot*, denominadas de *guaranteed time slot* (GTS).

Quanto a comunicação entre dispositivos, pode-se identificar três tipos de troca de dados: dados enviados pelo dispositivo para o coordenador, dados enviados pelo coordenador para o dispositivo e dados transferidos entre dispositivos [3, 6]. No primeiro caso, o dispositivo sincroniza o relógio para envio dos dados em redes livre de contenção ou utiliza CSMA-CA em redes com contenção. O reconhecimento de recebimento de dados é opcional. Para dados enviados pelo coordenador para o dispositivo, o coordenador utiliza mensagem de sinalização (*beacon*) para indicar ao dispositivo que tem dados a serem enviados em redes livres de contenção. Já em redes com contenção de acesso múltiplo ao meio, o coordenador aguarda o dispositivo solicitar os dados para envio. Semelhante ao primeiro caso, o reconhecimento de entrega dos dados é opcional.

Outros aspectos relacionados a comunicação em rede ZigBee são mecanismos de verificação de erros, cujo padrão IEEE 802.15.4 utiliza 16 bits como *Frame Check Sequency*, baseado em códigos de redundância cíclica (CRC, *Cyclic Redundancy Check*) e especificado pela ITU [7]. Em relação

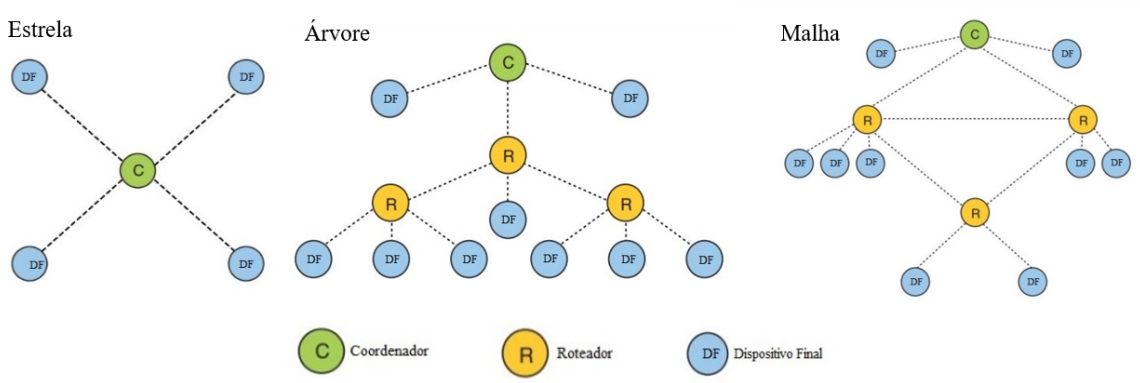

Fig. 2. Topologias de rede ZigBee: estrela, árvore e malha.

ao endereçamento, a camada de rede do protocolo ZigBee aloca 16 bits para endereçamento. Enquanto o protocolo IEEE 802.15.4 especifica 16 bits para comunicação em uma única rede e 64 bits para expansão de numero de dispositivos. Os endereços IEEE são mapeados em endereços de camada de Rede por uma *Lock-up Table*. As redes Zigbee incluem dois conceitos importantes definidos como *self-forming* que é a capacidade de estabelecer uma rede e *self-healing* relacionada a reorganização no roteamento de mensagens em caso de mudanças na rede [3].

III. Aspectos relacionados aos dispositivos

Os dispositivos ZigBee são basicamente formados por um microcontrolador, um transceptor e uma antena [5]. As especificações de programas embarcados em *hardware* especificam suas funções e, consequentemente, o tipo de dispositivo. Logo, tem-se dispositivos de função completa (FFD, *full-function devices*) e dispositivos de função reduzida (RFD, *reduced-function devices*). Os FFDs são aptos a executar todas as funcionalidades especificadas no IEEE 802.15.4, enquanto os RFDs limitados em funcionalidades se restringindo em integrar funções simples [3, 4, 7].

Em relação as funcionalidades dos dispositivos (FFD ou RFD) e ao seu posicionamento dentro de uma topologia de rede, pode-se classificar os dispositivos em coordenadores, roteadores, dispositivos finais, ZigBeed *Trust* e ZigBee *Gateway* [6, 7]. Dispositivos coordenadores são FFD e responsáveis por coordenar uma rede, sendo únicos e capazes de retransmitir pacotes de dados. Dentre as funções que executam, incluem-se a seleção do canal a ser utilizado pela rede, inicialização da rede, atribuição de endereços, exclusão e inclusão de dispositivos na rede, listagem de roteadores vizinhos e transmissão de pacotes de aplicação.

Os roteadores também são FFDs e utilizados para expansão de cobertura em topologias de rede do tipo árvore. Sua função é realizar o roteamento ótimo de mensagens pela rede até o destino. Ademais, implementam-se as função anteriormente listadas para um coordenador, exceto estabelecimento de rede. Os dispositivos finais resumem-se aos RFDs que se conectam tanto aso roteadores ou coordenador da rede. Os dispositivos definidos como ZigBeed *Trust* são responsáveis pelo gerenciamento e distribuição de chaves de segurança e autenticação para os dispositivos da rede. Já o ZigBee *Gateway* provê conexão externa para a rede Zigbee, sendo capaz de converter os protocolos de comunicação.

IV. Topologias de redes ZigBee

A tecnologia ZigBee permite a formação de redes por meio da camada de rede. O padrão IEEE 802.15.4 especifica topologias em estrela, malha e árvore, como visto na Figura 2 [3, 4, 6, 7]. Porém, aplicações práticas consideram uma mescla dessas topologias. A topologia estrela emprega um dispositivo como coordenador da rede e outros dispositivos como finais, que se conectam ao coordenador para comunicação direta. Uma desvantagem inerente dessa topologia, é a dependência da comunicação entre dispositivos em relação ao coordenador. Uma vez que todos os dados devem passar por esse dispositivo. Para uma comunicação volumosa de dados, o coordenador constitui um ponto de gargalo para os dispositivos periféricos.

A topologia em árvore introduz uma hierarquia na conexão, com a presença de roteadores para comunicação com todos os nós finais da rede. Dessa forma, experimenta-se uma expansão da rede em relação a topologia em estrela. Nessa topologia, os dispositivos finais se comunicam apenas com o roteador ou coordenador que está conectado, representando uma desvantagem para cenários onde dispositivos finais próximos queiram se comunicar. A topologia em malha também considera os mesmos dispositivos definidos para a topologia em árvore. Contudo, as conexões entre os dispositivos podem ser muti-ponto, resultando em roteamentos de mensagens por múltiplos nós e possibilitando as características de *self-healing*.

V. Conclusão

Esse trabalho apresentou um estudo sobre o protocolo de comunicação ZigBee, realizado como requisito para o desenvolvimento de projetos de engenharia com a empresa Pixel TI. Abordaram-se os conceitos básicos, arquiteturas e padrões, aspectos relacionados às faixas de frequência, taxas de transmissão, dispositivos, topologias de rede e comunicação entre dispositivos. Devido às políticas de sigilo da Pixel TI, as atividades de projeto foram omitidas nesse documento. Contudo, ressalta-se que o embasamento teórico desenvolvido em etapa inicial e registrado nesse trabalho foi importante para entender e manipular os *firmwares* envolvidos no projeto.

AGRADECIMENTOS

Os autores agradecem a empresa Pixel TI pelo apoio financeiro e conhecimento transmitido por parte de seus colaboradores na execução das atividades propostas, ao Instituto Nacional de Telecomunicações (Inatel) e ao Laboratório de Segurança Cibernética e Internet das Coisas (CS&I Lab.) por todo o suporte técnico oferecido.

REFERÊNCIAS

[1] Simone Cirani, Gianluigi Ferrari, Marco Picone e Luca Veltri. *Internet of things: architectures, protocols and standards*. John Wiley & Sons, 2018.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari e M. Ayyash. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications". Em: *IEEE Communications Surveys Tutorials* 17.4 (2015), pp. 2347–2376.

[3] C. Wang, T. Jiang e Q. Zhang. *ZigBee Network Protocols and Application*. SPRINGER, 2007.

[4] H. Labiod, H. afifi e C. de santis. *Wi-Fi Bluetooth ZigBee and Wi-Max*. CRC Press, 2012.

[5] D. S. Evangelista. *Integração de Redes de Sensores ZigBee para automação predial utilizando módulos Mahsbean*. Universidade de Brasília, Faculdade de Tecnologia,ENE, 2010.

[6] S. Farahani. *ZigBee Wireless Networks and Transceivers*. Newnes, 2008.

[7] Ata Elahi e Adam Gschwender. *Zigbee Wireless Sensor and Control Network*. Prentice Hall, 2009.