Um estudo sobre o modelo *ZigBee* de rede sem fio IEEE 802.15.4

Carlos Pinto Alves[1,2], **José Barbosa da Silva Filho**[3,4]

[1]Programa de Pós-Graduação em Eng. Elétrica e de Telecom. (PPGEET) - UFF
Rua Passo da Pátria, 156, Bl D, Sl 502B, São Domingos, Niterói, RJ - Brasil

[2]Comando do 1º Distrito Naval - Marinha do Brasil
Praça Mauá, 65, Centro, Rio de Janeiro, RJ - Brasil

[3]Programa de Pós-Graduação em Informática (PPGI) - UFRJ
Av. Athos da Silveira Ramos, 149, Rio de Janeiro, RJ - Brasil

[4]Centro de Instrução Almirante Graça Aranha (CIAGA) - Marinha do Brasil
Av. Brasil, 9020, Olaria, Rio de Janeiro, RJ - Brasil

carlosparj@gmail.com, josebarbosa@ufrj.br

Abstract. *This paper aims to present the standard of low power and low transfer rate wireless communication and control technology for a mesh architecture also popularly known as ZigBee. There will be presented theoretical concepts that help you to understand the process of communication and control, its technical characteristics and its operational limits as well as its specifications. This article will allow you to know where to use this standard, what devices are used in the market, and to enable the creation and development of new ideas about applications, devices or services that can help solve so many difficulties that are present today in our social life.*

Resumo. *Este artigo tem como objetivo apresentar o padrão de tecnologia de comunicação e controle sem fio com pequena taxa de transferência, para uma arquitetura de malha com baixa potência também conhecido popularmente por ZigBee. São apresentados os conceitos teóricos que ajudam a entender o processo de comunicação e controle, suas características técnicas e seus limites operacionais como também suas especificações. Nesse sentido, esse artigo permitirá que você saiba onde usar esse padrão, quais dispositivos são usados no mercado, e possibilitar a criação e desenvolvimento de novas ideias a respeito de aplicativos, dispositivos ou serviços que possam ajudar a resolver tantas dificuldades que estão presentes hoje em nosso convívio social.*

1. Introdução

O presente artigo visa apresentar o modelo de arquitetura para dispositivos de baixa potência *ZigBee*, sobre o padrão IEEE 802.15.4 [1], suas características e exemplos de aplicações focando em cidades inteligentes. Este trabalho foi organizado em seções, sendo a seção 1, a introdução ao estudo. Nas seções 2 e 3 serão vistos as características do IEEE 802.15.4 e básicos conceitos necessários a compreensão da tecnologia. Nas seções 4, 5 e 6 serão abordadas as características e aplicações do *ZigBee* e por fim na seção 7 as conclusões.

[1]Padrão consolidado pelo Institute of Electrical and Electronics Engineers (IEEE) em 2003.

Concebido em 1998, o *ZigBee* teve sua origem da analogia entre o modo como as abelhas se locomovem e o funcionamento de uma rede malha. Abelhas voam em zigue zague e durante o vôo, trocam de informações com outras abelhas. Nessa época, em 1998, o padrão de rede *ZigBee* começou a fazer sentido, pois foi quando as tecnologias *WiFi* e *Bluetooth* não estavam sendo adequadas para determinadas aplicações [Farahani 2008].

O *ZigBee* é um conjunto de especificações designadas para a realização de comunicação de equipamentos eletrônicos (sensores e dispositivos), que possam operar sem fio. O padrão *ZigBee* foi designado para a operação de redes WPAN (*Wireless Personal Area Network*), com dispositivos que tenham um baixo consumo de energia, baixa complexidade, baixa latência e longa duração de bateria [Omojokun 2015].

Pelo fato de existir uma grande variedade de proprietários de dispositivos e cada um com suas características próprias de comunicação e controle, surgiu a necessidade de se criar uma aliança de empresas que tenham em comum o objetivo de padronizar um protocolo. Essa aliança hoje é conhecida como *ZigBee Alliance*, uma Aliança que conta com mais de 400 grandes empresas de diferentes segmentos do mercado de 20 países distintos. Por isso, a ideia de se criar um padrão único para garantir uma melhor confiabilidade, segurança e interoperabilidade entre os dispositivos e os equipamentos de controle, evitando o surgimento de padrões proprietários distintos que não consigam garantir a comunicação entre outros equipamentos.

2. O padrão 802.15.4

O padrão IEEE 802.15.4, define a camada física e MAC em redes sem fio de área pessoal de baixa capacidade, sob as quais alguns modelos de comunicação foram propostos. Como exemplos citamos o *WirelessHart*, *6LowPAN* e o *ZigBee*, este último objeto de nossa pesquisa [de Andrade Lorençato 2013, SANTOS 2014, ZigBee™ Alliance 2017].

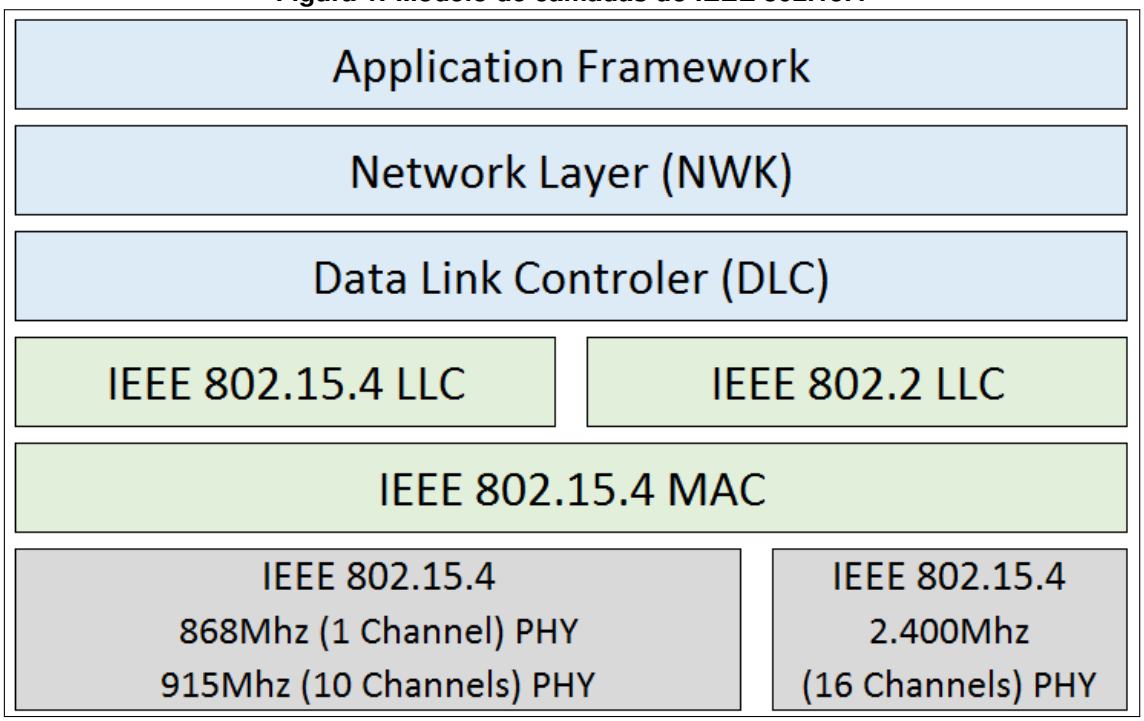
O modelo definido pelo IEEE 802.15.4, pode ser visto na figura 1 e define duas camadas físicas, as quais representam 3 faixas de frequência com licença livre que incluem 16 canais a 2.4 GHz, 10 canais a 915 MHz, e 1 canal a 868 MHz [Melo 2017].

As camadas físicas foram projetadas para acomodar as necessidades de interfaces de baixo custo, permitindo níveis elevados de integração. O uso da técnica de transmissão de Sequência Direta (DSS) permite que os equipamentos sejam "minimalistas", simples em sua especificação de hardware, possibilitando implementações de menor custo.

A camada MAC foi projetada para permitir topologias múltiplas de baixa complexidade. O MAC também permite que um dispositivo com funcionalidade reduzida (RFD) opere na rede sem a necessidade de grandes quantidades de memória disponíveis, podendo controlar também um grande número de dispositivos sem a necessidade de colocá-los "em espera", como ocorre em algumas tecnologias sem fio.

Já a camada de rede pode operar com grandes quantidades de nós de rede com latências relativamente baixas. E possibilita o crescimento da rede sem a necessidade de equipamentos de transmissão de potência mais elevada. Utiliza um algoritmo que permite implementações da pilha de protocolos visando balancear os custos das unidades em aplicações específicas, buscando produzir soluções com custo-desempenho para a aplicação.

Figura 1. Modelo de camadas do IEEE 802.15.4



Fonte: Autores, baseado em Tanenbaum 2011.

3. Tipos de dispositivos da rede

Dois tipos de dispositivos são definidos pelo padrão, o FFD (*Full Function Device*), que é um dispositivo com maior complexidade operando em toda a topologia e pode ter acesso a todos os outros dispositivos, e o RFD (*Reduced Function Device*) que é mais simples e se comunica apenas com os FFDs, na figura 2 podemos observar as três categorias de funções, que são:

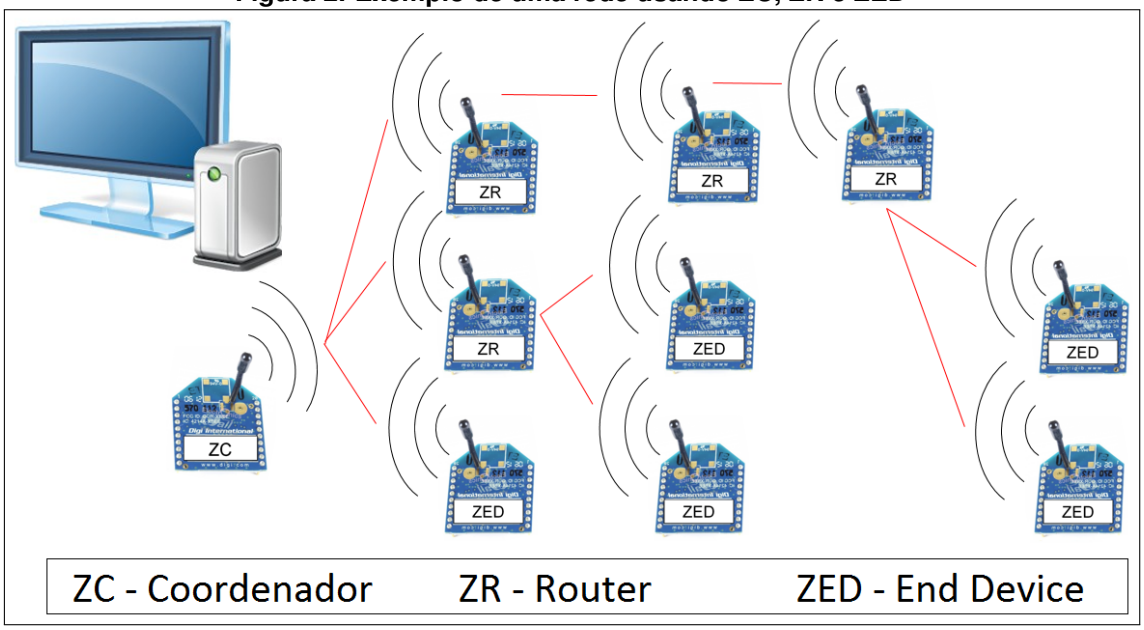
***Network Coordinator* ou Coordenador** – É o mais elaborado dos três, logo utiliza mais memória e processamento e está sempre mantendo o conhecimento da rede. Ele tem a função de formar a rede. Através dele, toda a rede recebe um canal e endereço para a comunicação, permitindo que os roteadores e os dispositivos finais interajam na rede. Para essa função é preciso utilizar um dispositivo FFD.

Roteador – O seu processamento computacional e sua memória adicional o tornam ideal para realizar funções de roteamento da rede. Ele cria nós, mantém a informação da rede e define a melhor rota para o pacote de dados. Pode também ser utilizados nas margens da rede conectando-as ao mundo real. Para essa função é preciso utilizar um dispositivo FFD.

***End Device* ou Dispositivo Final** – Não faz roteamento e possui funções limitadas. Por isso é usado nas margens das redes, como dispositivo final. Para se comunicar com outro *End Device*, ele precisa interagir com um nó roteador ou com um nó coordenador. Para essa função é preciso utilizar um dispositivo RFD [Omojokun 2015].

Na figura 3, é possível verificar que os dispositivos finais podem se comunicar com os coordenadores, com os roteadores, mas não com outros dispositivos finais (não

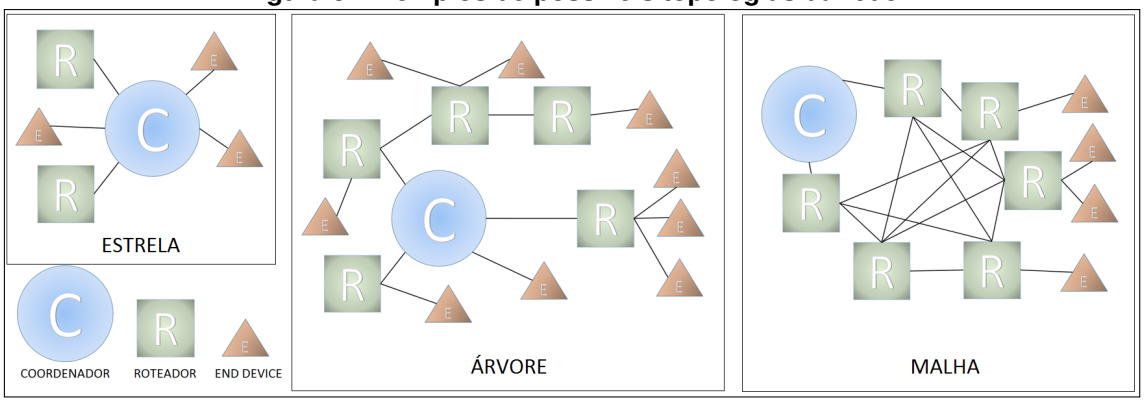
Figura 2. Exemplo de uma rede usando ZC, ZR e ZED



Fonte: Autores, baseado em Tanenbaum 2011.

diretamente). Já os roteadores podem se comunicar com os coordenadores e com outros roteadores, servindo de interface para os dispositivos finais. Esses três dispositivos podem formar diferentes redes. Cada Coordenador pode utilizar até 65535 nós [Melo 2017], o tempo de ativação de um nó na rede é de 30 ms e o tempo para ativar um nó adormecido na rede é de 15 ms.

Figura 3. Exemplos de possíveis topologias da rede

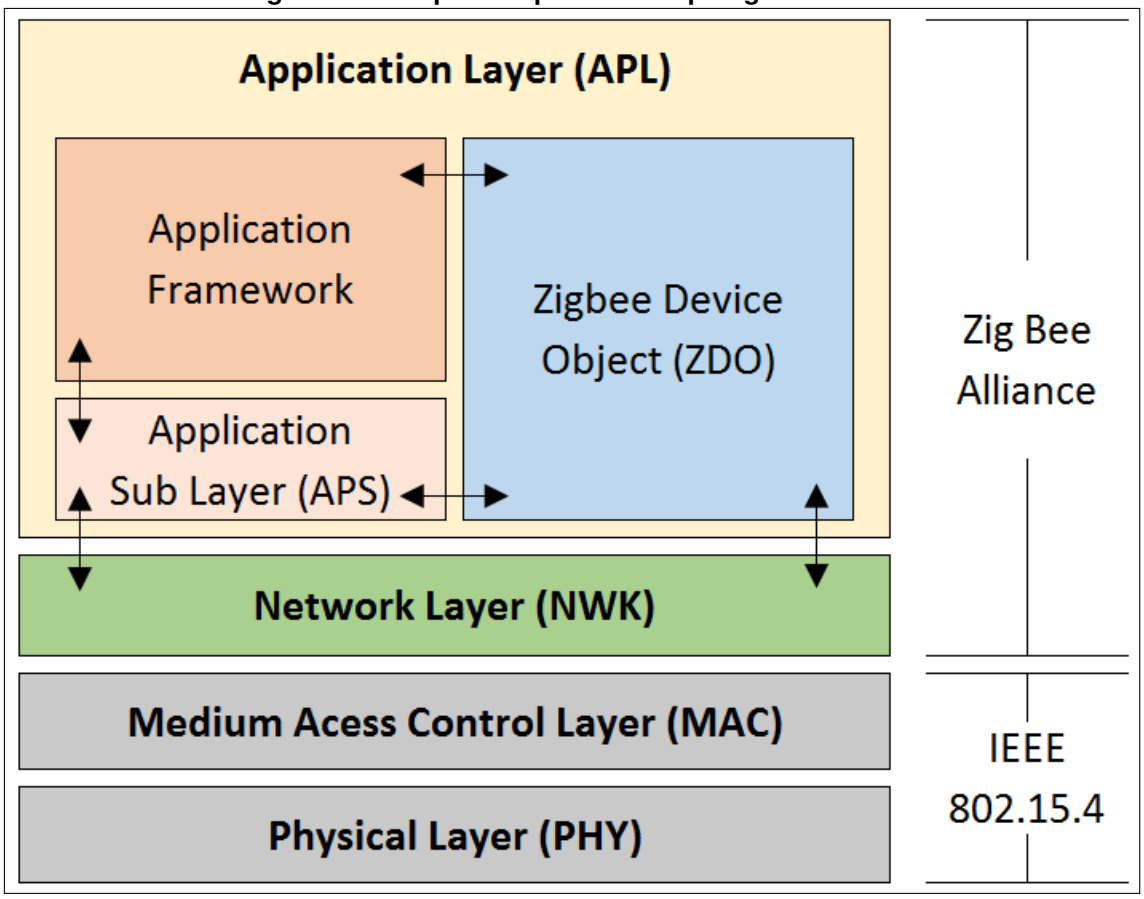


Fonte: Autores.

4. Camadas de Protocolos

Na figura 4, é possível verificar as camadas de protocolos e seus influentes [Kurose and Ross 2010]. No caso da aplicação, o usuário, em suporte e rede a *ZigBee* Alliance, e Mac e física, o IEEE.

Figura 4. Exemplos de possíveis topologias da rede



Fonte: Autores.

4.1. Aplicação:

Consiste em subsidiar as camadas APS (*Application Support Sublayer*), ZDO (*ZigBee Device Object*) e aplicação de objetos.

4.1.1. APS - *Application Support Sublayer*

Responsável pelo roteamento das mensagens aos diferentes pontos de aplicação de um nó e mantém as tabelas de descoberta (tabela de conexões compatíveis entre diferentes dispositivos finais). Provê duas interfaces: o APSME-SAP (APS Management *Entity Sevice Access Point*) e o APSDE-SAP (APS Data *Entity Service Access Point*). São usados para implementar segurança e utilizar a informação enviada da subcamada de aplicação (APS Layer) para os coordenadores *ZigBee Device Object*(ZDO).

4.1.2. ZDO - *ZigBee Device Object*

É responsável pela informação de disponibilidade dos dispositivos e provê a interface para descoberta de outros dispositivos na rede e seus serviços. Como suporte, utiliza o APSDE-SAP para APS Layer e o NLME-SAP para camada de Rede (*NWK Layer*). Ele

é implementado no dispositivo final justamente por conter as configurações necessárias à configuração dos demais dispositivos finais. Os outros dispositivos finais são numerados de 1 a 240. Tem seu próprio perfil, conhecido como o perfil do dispositivo de *ZigBee* (ZDP). É o ZDP que contém os serviços para a descoberta do dispositivo. O ZDO é então responsável pela gerência do dispositivo total e também por chaves e políticas da segurança. No ZDO é onde está definido o papel do dispositivo na rede, se ele atuará como coordenador, roteador ou dispositivo final. Além disso, há a definição do método de segurança usado na rede e o início das solicitações da tabela de conexões (*Bindings*).

4.2. Rede / Segurança

Responsável por iniciar e autenticar os endereços, utilizando duas interfaces: NLME-SAP (*Network Layer Management Entity Service Access Point*) e o NLDE-SAP (*Network Layer Data Entity Service Access Point*). Esses algoritmos permitem a implementação da pilha de protocolos visando balancear os custos das unidades em aplicações específicas, o consumo das baterias, buscando produzir soluções com o perfil específico de custo-desempenho para a aplicação. Envia e recebe dados das camadas de aplicação, aplica critérios de segurança e quando configurado com a característica de rede Mesh, permite a transmissão dos dados por diferentes caminhos.

4.3. MAC

A camada MAC foi projetada para permitir topologias múltiplas com baixa complexidade, onde o gerenciamento de energia, por exemplo, não requer modos de operação complexos. A camada MAC controla o acesso ao canal de rádio usando o mecanismo CSMA-CA (*Carrier Sense Multiple Access with Collision Avoidance*). Sua responsabilidade inclui transmitir quadros, sincronização e prover um mecanismo confiável de transmissão.

Quando um nó deseja fazer transmissão ele envia um sinal de aviso, por tempo suficiente para que todos os componentes da rede o recebam. Só então os dados são transmitidos. Se durante uma transmissão um sinal de aviso for detectado o emissor interrompe o envio da mensagem, reiniciando a tentativa de transmissão após um período aleatório. Existe um mecanismo para combater a degradações (dispersões, multipercursos, interferência) e para aperfeiçoar a transmissão de dados que pode ser com o uso do ARQ (*acknowledgement request*), onde um *acknowledge* (ACK) deve ser enviado quando ocorrer uma transmissão com sucesso. Se o ACK não é recebido, o pacote é retransmitido. Ou por meio do *Coordinator buffering*, onde o nó coordenador da rede armazena as mensagens para nós adormecidos até eles acordarem novamente [Melo 2017].

4.4. Tipos de endereçamento

A descoberta de um dispositivo é o processo onde um dispositivo *ZigBee* pode encontrar outros dispositivos *ZigBee* na rede, através de requisições que são distribuídas por *broadcast* ou unicast.

4.4.1. Endereço Unicast

Identifica apenas uma interface. Um pacote destinado a um endereço *unicast* é enviado diretamente para a interface associada ao endereço, ou seja, é ponto a ponto. Este modo

é o único que suporta retorno. Enquanto neste modo, os módulos receptores enviam em ACK (*acknowlegdement* - reconhecimento) do pacote de recepção RF para o transmissor. Se o módulo transmissor não receber o ACK, este retransmitirá o pacote por três vezes ou até receber o ACK. O módulo pode ser configurado para usar o endereço curto de 16 bits ou o endereço longo de 64 bits.

4.4.2. Endereço *broadcast*

Identifica um grupo de interfaces de nós diferentes. Um pacote destinado a um endereço *broadcast* é enviado para uma das interfaces identificadas pelo endereço. Especificamente, o pacote é enviado para a interface mais próxima de acordo com a medida de distância do protocolo de roteamento. Qualquer módulo dentro do alcance aceitará um pacote que contém um endereço *broadcast*. Quando configurado para operar no modo *broadcast*, os módulos receptores não enviam ACK's, e os módulos receptores não reenviam automaticamente os pacotes como no caso do modo *unicast*.

4.4.3. Solicitações de Endereço

Existem duas formas de um dispositivo solicitar a rede a fazer uma descoberta: solicitações de endereços IEEE e solicitações de endereços NWK. A solicitação IEEE é unicast e assume que o endereço NWK é conhecido. A requisição do endereço NWK é *broadcast* e contém o endereço IEEE como tamanho do quadro. Quando solicitado, o endereço IEEE dos dispositivos requisitados precisa ser devolvido (se o dispositivo for *ZigBee*) com o endereço do dispositivo e de todos seus dispositivos associados (se o dispositivo for um roteador ou um coordenador). Isso se refere à descoberta de dispositivo e é utilizado para encontrar os dispositivos *ZigBee* na rede. Adicionalmente à descoberta do dispositivo, a descoberta de serviços também é fornecida para determinar quais serviços foram oferecidos em cada dispositivo final ou definidos em um dispositivo pelo respectivo objeto da camada de aplicação. Tabelas de conexão são construídas e preenchidas conforme as solicitações e os resultados das conexões.

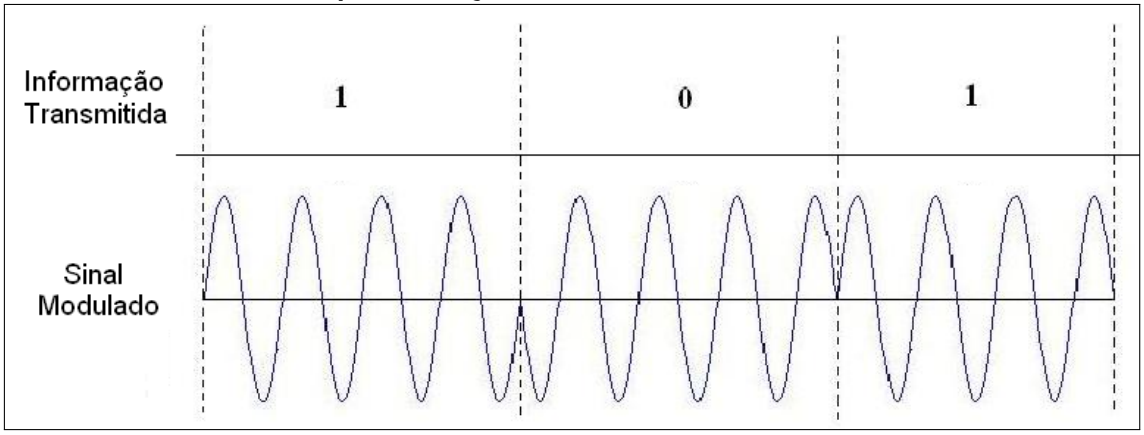
4.5. Física

Nesta camada são tratados os tipos de frequências de operação (868/915 MHz e 2.4 GHz). Foi projetada para acomodar as necessidades de interfaces de baixo custo, permitindo níveis elevados de integração. O uso da técnica de transmissão de Espalhamento Espectral de Sequência Direta (DSSS -*Direct Sequence Spread Spectrum*) permite que os equipamentos sejam muito simples, possibilitando implementações mais baratas. Para ajudar a reduzir degradações, essa camada usa o *Direct Sequence* com *Frequency Agility* (DS/FA) usa uma sequência especial de um "chip". Quanto maior a quantidade de chips por símbolos, maior a capacidade de rejeitar multicaminhos e interferência. O *Frequency Agility* consiste na habilidade de trocar de frequências para evitar interferência de alguma fonte de sinal.

4.5.1. Modulação

O protocolo de comunicação do padrão IEEE 802.15.4 foi desenvolvido para suportar comunicação digital de dados, com a meta de redução de consumo de energia e baixo custo. Para isso, utiliza uma transmissão *half-duplex*, de modo que o transmissor e o receptor não necessitam estarem ativos simultaneamente. Para as frequências de 868/915 MHz, é utilizado o BPSK (*Biphase or Binary Phase Shift Keying*), figura 5.

Figura 5. Modulação BPSK. Os bits relativos ao feixe em quadratura sofrem um deslocamento no tempo em relação aos bits do feixe em fase, de meio símbolo



Fonte: Autores, baseado em Viswanathan 2010.

Já para a frequência de 2.4 GHz, é utilizado o OQPSK (*Off-set Quadrature PSK*), figura 6. A frequência de 2.4GHz emprega uma forma de sinalização ortogonal multinível enviando quatro bits por símbolo, que habilita simultaneamente tanto altas taxas de transmissão quanto uma taxa de símbolo baixa. Estes dois esquemas de modulação também empregam uma distribuição de sequências para proporcionar os benefícios do serviço DSSS, que é uma das muitas técnicas para aumentar a largura de banda de um sinal transmitido, proporcionando um aumento da qualidade de comunicação [Nenoki 2013].

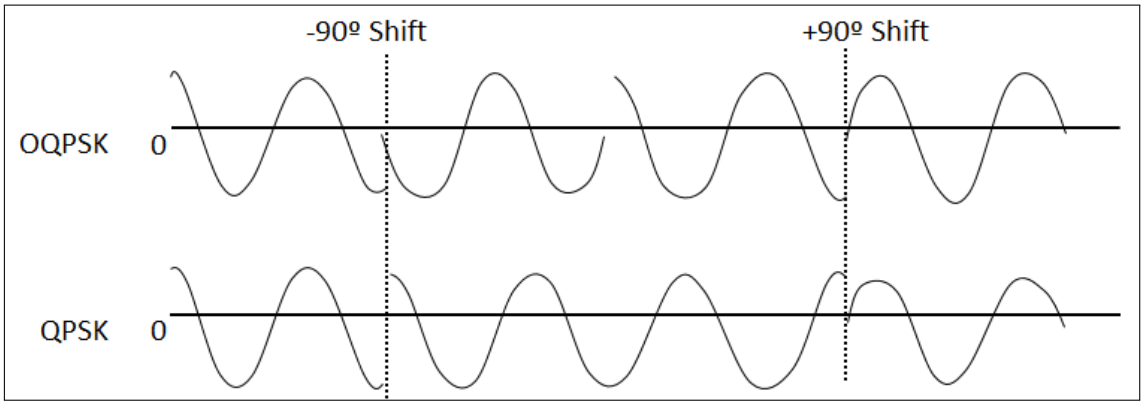
4.6. Sensibilidade do receptor e Potência de transmissão

Nas frequências 868/915 MHz a especificação de sensibilidade mínima é de –92 dBm, e em 2.4GHz a especificação de sensibilidade mínima é de -85 dBm. Assim, podem-se usar receptores simples, de baixo custo e com pouca amplificação de radiofrequência. Embora o Padrão IEEE 802.15.4 permita qualquer potência de saída legalmente aceita, ele necessita somente que o equipamento compatível seja capaz de transmitir –3 dBm, justamente dentro da capacidade de energia instantânea das baterias [Torres dos Santos 2017].

5. Segurança do padrão

O padrão *ZigBee* adotou a proposta de um algoritmo de segurança, baseado na simplificação do algoritmo de roteamento AODV (*Ad-hoc On-demand Distance Vector*) e esta proposta foi adotada como parte da especificação IEEE 802.15.4. O AES (*Advanced*

Figura 6. Modulação OQPSK



Fonte: Autores, baseado em Zou et al. 2013.

Encryption Standard) é utilizado na camada MAC como seu algoritmo de criptografia, descrevendo uma variedade de rotinas de segurança. Estas rotinas têm como objetivo prover a confidencialidade, a integridade e a autenticidade dos quadros da camada MAC. A camada MAC faz o processamento de segurança, mas são as camadas superiores que controlam o processo, ajustando as chaves de criptografia e determinando os níveis de segurança que deverão ser usados.

Quando a camada MAC transmite (ou recebe) um quadro, verifica o destino (a fonte do quadro), recupera a chave associada com esse destino, e usa então esta chave para processar o quadro de acordo com a rotina de segurança designada para a chave que está sendo usada. Cada chave é associada a uma única rotina de segurança e o cabeçalho do quadro MAC possui um bit que especifica se a segurança para o quadro está habilitada ou não. A segurança é implementada via listas de controle de acesso ACL (*Access Control List*) e cada receptor pode utilizar chaves e conjuntos de operação distintos.

5.1. Modo ACL

Segurança limitada para comunicação com outros dispositivos que podem aceitar ou rejeitar pacotes baseados nas informações e filtros contidos em uma ACL.

5.2. Modo Não Seguro

Não é requisitada a segurança dos componentes na rede *ZigBee*.

5.3. Modo Seguro

Qualquer serviço de segurança pode ser provido, definido pelo padrão. Os serviços de segurança são dependentes dos conjuntos de segurança implementados e em uso, criptografia de dados, criptografia simétrica, integridade de pacotes e código de Integridade de Mensagens MIC (*Message Integrity Code*).

O *ZigBee* pode assegurar mensagens transmitidas sobre um *single-hop* usando quadros de dados MAC seguros, mas para mensagens multi-hop, o *ZigBee* utiliza camadas superiores (como a camada de NWK) para segurança. A camada MAC faz a segurança de

processamento, mas as camadas superiores que montam as chaves e determinam os níveis de segurança para uso, controlando este processo.

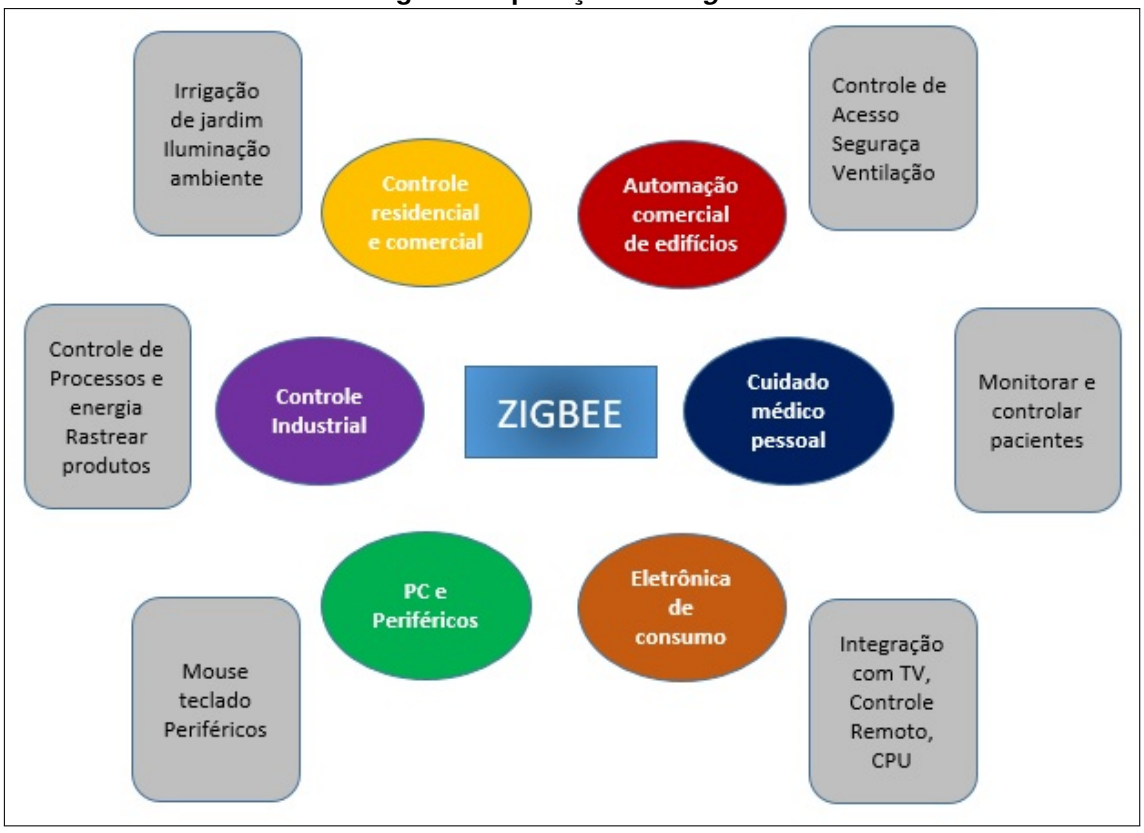
Quando é requerida a integridade na transmissão de um quadro, o cabeçalho MAC e dados do tamanho do quadro são usados em cálculos para criar um Código de Integridade de Mensagem (MIC) consistindo em 4, 8 ou 16 octetos. Se a confidencialidade é requerida, um quadro do tamanho do quadro MAC é adicionado ao quadro e a sequencia. Após a recepção de um quadro, se um MIC estiver presente, este é verificado e se o tamanho do quadro é codificado, com isso, ele é decifrado. Dispositivos enviados aumentarão a contagem de quadro com toda mensagem enviada e dispositivos receptores manterão o registro da última conta recebida de cada dispositivo enviado. Se uma mensagem com uma conta antiga é detectada, esta é sinalizada com um erro de segurança.

A camada de NWK também faz uso do AES (*Advanced Encryption Standard*), adicionalmente oferece capacidade de somente criptografia e somente integridade. Considerando que uma chave não é ligada estritamente a um único conjunto de segurança, uma aplicação tem a flexibilidade para especificar o conjunto de segurança atual para aplicar a cada quadro NWK, não apenas se segurança é habilitada ou desabilitada [Gascón 2009].

6. Aplicações

O padrão *ZigBee* pode ser empregado em diversas aplicações onde requer o uso de dispositivos sem fio, conforme descrito abaixo e também e exemplificado na figura 7: Sensor

Figura 7. Aplicações do *ZigBee*



Fonte: Autores.

de umidade, temperatura, velocidade do vento, direção do vento, pressão atmosférica.

Controle de iluminação, cancelas, aquecimento, velocidade em rodovias, ventilação, irrigação; alarmes, portas e portões, aplicações automotivas, entre outras.

Diferentes dispositivos e aplicações nas diversas áreas, como automação comercial (segurança, controle de acesso, ventilação), controle Residencial (iluminação; irrigação de jardim), controle industrial (gerenciamento de energia; controle de processos; rastreamento de equipamentos) como apresentado no trabalho da Silva et al. 2017, Eletrônica (TV, DVD) PC e Periféricos (teclado, joystick, mouse), cuidado médico pessoal (monitoramento de pacientes, corporal) e com muita presença, a IOT (*Internet Of Things* – Internet das Coisas), como no trabalho de Ferreira and Godoy 2016, monitoramento ambiental; gestão de infraestrutura, veículos aéreos não tripulados (VANT), produção industrial, controle de gastos, sistemas médicos e de cuidados com a saúde, automação residencial, como visto no trabalho de Osipov 2008, sistemas de transporte, cidades inteligentes, exemplificada pelo trabalho de Pinheiro 2006 e em redes veiculares VANETs, como visto nos trabalhos de Satyajeet et al. 2016 e Silva et al. 2017.

7. Considerações finais

O padrão *ZigBee* surge como uma solução para projetos sem fio destinados a controle de dispositivos e vem ganhando cada vez mais adeptos. De certa forma, essa aplicação ainda tem sua expressão voltada para o exterior. É esperado que essa tendência venha se difundir cada vez mais no mercado nacional.

A interoperabilidade entre diferentes produtos mantendo o mesmo padrão facilita o surgimento de novos fornecedores, mais investimentos e incentivos para esse tipo de aplicação. Uma vez introduzido no mercado, novos adeptos irão utilizar e desenvolver novas funcionalidades ou aplicações.

Há uma tendência muito forte para o surgimento de novas aplicações e serviços utilizando o padrão *ZigBee*, que serão desenvolvidas no campo da IOT, onde diversos dispositivos estarão conectados entre si em uma PAN (seja em estrela, árvore ou muito provável *mesh*). Esses dispositivos interconectados entre si, trocarão informações constantes e de forma automatizada, se tornarão uma facilidade para realizar tarefas simples ou complexas que hoje é executada de forma manual e individualizada.

Partindo desta premissa, vislumbra-se como continuidade do presente estudo a avaliação comparativa entre os custos de implantação e de manutenção das tecnologias que possuem por base o IEEE 802.15.4 (*WirelessHart*, *6LowPAN* e o próprio*ZigBee*).

Referências

[da Silva et al. 2017] da Silva, C. A. G., dos Santos, E. L., Ferrari, A. C. K., and dos Santos Filho, H. T. (2017). A study of the mesh topology in a zigbee network for home automation applications. *IEEE Latin America Transactions*, 15(5):935–942.

[de Andrade Lorençato 2013] de Andrade Lorençato, A. (2013). Analisador de redes wirelesshart. `http://hdl.handle.net/10183/96497`. Acessado em 08 de dezembro de 2019.

[Farahani 2008] Farahani, S. (2008). *ZigBee Wireless Networks and Transceivers*. Newnes, Newton, MA, USA.

[Ferreira and Godoy 2016] Ferreira, I. V. and Godoy, E. P. (2016). Integração de internet das coisas e zigbee no contexto de eficiência energética e automação predial. *XXI Congresso Brasileiro de Automática - CBA2016, UFES, Vitória - ES*.

[Gascón 2009] Gascón, D. (2009). Security in 802.15.4 and zigbee networks. http://www.libelium.com/security-802-15-4-zigbee/. Acessado em 08 de dezembro de 2019.

[Kurose and Ross 2010] Kurose, J. F. and Ross, K. W. (2010). *Redes de Computadores e a Internet: Uma abordagem top-down*. Pearson, São Paulo, trad. 5 ed. edition.

[Melo 2017] Melo, P. (2017). Padrão ieee 802.15.4 - a base para as especificações zigbee, wirelesshart e miwi. https://www.embarcados.com.br/padrao-ieee-802-15-4/. Acessado em 08 de dezembro de 2019.

[Nenoki 2013] Nenoki, E. (2013). Zigbee – estudo da tecnologia e aplicação no sistema elétrico de potência. http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/886/1/CT_COTEL_2012_2_01.pdf. Acessado em 08 de dezembro de 2019.

[Omojokun 2015] Omojokun, G. (2015). A Survey of ZigBee Wireless Sensor Network Technology: Topology, Applications and Challenges. *International Journal of Computer Applications*, 130(9):47–55.

[Osipov 2008] Osipov, M. (2008). Home automation with zigbee. In Balandin, S., Moltchanov, D., and Koucheryavy, Y., editors, *Next Generation Teletraffic and Wired/Wireless Advanced Networking*, pages 263–270, Berlin, Heidelberg. Springer Berlin Heidelberg.

[Pinheiro 2006] Pinheiro, J. M. S. (2006). Zigbee em home area network. https://www.projetoderedes.com.br/artigos/artigo_zigbee_em_home_area_network.php. Acessado em 08 de dezembro de 2019.

[SANTOS 2014] SANTOS, R. L. (2014). Internet das coisas e 6lowpan (monografia). http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3599/1/CT_GESER_V_2014_12.pdf. Acessado em 08 de dezembro de 2019.

[Satyajeet et al. 2016] Satyajeet, D., Deshmukh, A. R., and Dorle, S. S. (2016). Article: Heterogeneous approaches for cluster based routing protocol in vehicular ad hoc network (vanet). *International Journal of Computer Applications*, 134(12):1–8. Published by Foundation of Computer Science (FCS), NY, USA.

[Silva et al. 2017] Silva, L. A. G., Sousa, J. C., Sousa, D. F., and Vieira, P. A. (2017). Avaliação do padrão ieee 802.15.4 para redes veiculares com testes embasados na rfc 2544. *Anais Eletrônicos ENUCOMP 2017 - X Encontro Unificado de Computação*.

[Tanenbaum 2011] Tanenbaum, A. S. (2011). *Redes de Computadores*. Pearson, São Paulo, trad. 5 ed. edition.

[Torres dos Santos 2017] Torres dos Santos, S. (2017). Dissertação de mestrado em redes de sensores sem fio em monitora mento e controle. http://pee.ufrj.br/teses/textocompleto/2007062701.pdf. Acessado em 06 de julho de 2019.

[Viswanathan 2010] Viswanathan, M. (2010). Binary phase shift keying (bpsk) – modulation and demodulation. https://www.gaussianwaves.com/2010/04/

bpsk-modulation-and-demodulation-2/. Acessado em 08 de dezembro de 2019.

[ZigBee™ Alliance 2017] ZigBee™ Alliance (2017). Homepage do zigbee™ alliance. http://www.zigbee.org. Acessado em 13 de março de 2017.

[Zou et al. 2013] Zou, N., Huang, B., and Xu, Z. (2013). Shaped offset quadrature phase shift keying (soqpsk) modulation scheme and its application in optical wavelength-division multiplexed (dwdm) transmission. *Optical Fiber Technology*, 19(5):400 – 404.