UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS ARARANGUÁ

João Carlos Cichaczewski

ANÁLISE DA INTERFERÊNCIA MÚTUA ENTRE REDES IEEE 802.11 E IEEE 802.15.4

Araranguá, dezembro de 2013.

João Carlos Cichaczewski

ANÁLISE DA INTERFERÊNCIA MÚTUA ENTRE REDES IEEE 802.11 E IEEE 802.15.4

Trabalho de Conclusão de Curso submetido à Universidade Federal de Santa Catarina, como parte dos requisitos necessários para a obtenção do Grau de Bacharel em Tecnologias da Informação e Comunicação.
Orientador: Prof. Dr. Ricardo Moraes

Araranguá, dezembro de 2013.

João Carlos Cichaczewski

ANÁLISE DA INTERFERÊNCIA MÚTUA ENTRE REDES IEEE 802.11 E IEEE 802.15.4

Este Trabalho de Conclusão de Curso foi julgado aprovado para a obtenção do Título de Bacharel em Tecnologias da Informação e Comunicação, e aprovado em sua forma final pelo Curso de Graduação em Tecnologias da Informação e Comunicação.

Araranguá, dezembro de 2013.

Prof. Vilson Gruber, Dr.
Coordenador do Curso

Banca Examinadora:

Prof. Ricardo Moraes, Dr.
Orientador
Universidade Federal de Santa Catarina

Prof.ª Dr.ª Analucia Schiaffino Morales
Universidade Federal de Santa Catarina

Prof. Dr. Gustavo Medeiros de Araújo
Universidade Federal de Santa Catarina

Este trabalho é dedicado à toda minha classe social e aos meus queridos pais, Ivete e Argemiro.

AGRADECIMENTOS

"Um homem de valor nunca é ingrato."
Goethe

A conclusão do presente trabalho é um momento especial e fruto do envolvimento de muitas pessoas durante todo o processo de sua confecção. Por diferentes que sejam as razões, existem muitas pessoas a serem agradecidas, principalmente:

À Ricardo Moraes, professor da Universidade Federal de Santa Catarina - pelo exercício exemplar da sua função de orientador, e por acreditar no meu crescimento pessoal e profissional. Pela disponibilidade e acessibilidade dispensadas durante todo este processo que não teria sido possível sem seu auxílio e dedicação.

À Luis Seeman, Guilherme Damásio e Eduardo Arnold, colegas da UFSC e de projeto de pesquisa - pelo atenção dispensada na inúmeras vezes que necessitei.

À todos os meus familiares, amigos e colegas da UFSC que me apoiaram de uma maneira ou de outra no decorrer deste trabalho.

"A característica fundamental da guerrilha é a mobilidade."
(Che Guevara)

RESUMO

Atualmente, tem-se registrado um aumento constante na utilização de redes sem fio para controle e automação de processos nos mais variados ambientes. Nesses processos, as padronizações IEEE 802.11 e IEEE 802.15.4 figuram entre as redes de maior utilização. Porém, estes padrões de rede podem utilizar a mesma faixa de frequência para transmitir seus dados, ou seja, a faixa ISM de 2,400GHz à 2,480GHz. Essa banda é dividida em 11 canais no IEEE 802.11 e em 15 canais no IEEE 802.15.4, existindo sobreposição de canais em muitas situações. Entre os efeitos das interferências geradas pela transmissão em canais sobrepostos está o aumento no número de colisões e em seguida a perda de pacotes. Esses efeitos são altamente impactantes nas taxas de transferência das tecnologias supracitadas. Sendo assim, este Trabalho de Conclusão de Curso tem por objetivo avaliar experimentalmente a interferência mútua quando da operação simultânea de dispositivos IEEE 802.11 e IEEE 802.15.4 que compartilham um determinado ambiente. Primeiramente é realizada uma revisão bibliográfica com o objetivo de fundamentar o estudo das redes sem fio e ao aprofundamento de questões próprias da padronização IEEE 802. Na sequência, apresentam-se os cenários montados e os resultados obtidos, onde contatou-se que ocorre interferência mútua nos casos de transmissão em canais sobrepostos, diminuindo as taxas de transmissão e aumentando o número de mensagens perdidas, efeito que não é registrado quando os dispositivos operam em canais livres de sobreposição.

Palavras-chave: IEEE 802.11, IEEE 802.15.4, WiFi, ZigBee, Interferência, Sobreposição de canais.

ABSTRACT

Currently, there has been a constant increase in the use of wireless networks for control and automation processes in diverse environments. In this process, the IEEE 802.11 and IEEE 802.15.4 standardization remain between the most used networks. However, these standards can use the same frequency band to transmit their data, i.e., the ISM band 2.400 GHz to 2.480 GHz. This frequency band is divided in 11 channels in IEEE 802.11 and IEEE 802.15.4 in 15 channels, with overlapped channels in many situations. Among the effects of interference generated by overlapping transmission channels is the increase in the number of collisions and followed by packet loss. These effects are highly impactful in the transfer rates of the above mentioned technologies. The main objective this work is to evaluate the mutual interference of IEEE 802.11 and IEEE 802.15.4 networks, when they are sharing the same communication area, through an experimental assessment. Firstly, a bibliographic review that shows how wireless networks works is done, followed by a description of IEEE 802 standard. Afterwards, the scenarios are described and it is showed the experimental results, that demonstrates the mutual interference occurring in cases of overlapping transmission channels, decreasing transmission rates and increasing the number of lost messages, an effect that is not registered when devices operate on free channels overlapping.

Keywords: IEEE 802.11, IEEE 802.15.4, WiFi, ZigBee, Interference, Overlapping.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ACK - Acknowledgement
AIFS - Arbitration Interframe Space
AP - Access Point
APDU - Application Protocol Data Unit
ARPANet - Advanced Research Projects Agency Network
BSS - Basic Service Set
C11 - Canal 11
C12 - Canal 12
C13 - Canal 14
C15 - Canal 15
C16 - Canal 16
C17 - Canal 17
C18 - Canal 18
C19 - Canal 19
C20 - Canal 20
CAP - Controlled Access Phase
CCA - Clear Channel Assessment
CFP - Contention Free Period
CH - Cluster Head
CID - Cluster Identification
CSA - Channel Switch Announcement
CSMA - Carrier Sense Multiple Access
CSMA/CA - Carrier Sense Multiple Access / Collision Avoidance
CSMA/CD - Carrier Sense Multiple Access / Collision Detection
CTS - Clear To Send
DCF - Distributed Coordination Function
DIFS - Distributed Interframe Space
DNS - Domain Name System
DoD - Departamento de Defesa dos Estados Unidos
DS - Distribution System
ED - Energy Detection
EDCA - Enhanced Distributed Channel Access
EIFS - Extended Interframe Space
ESS - Extended Service Set
FDD - Full Function Device
FDMA - Frequency Division Multiple Access
FSO - Free Space Optic
FTP - File Transfer Protocol
GHz - Gigahertz

HCCA - HCF Controlled Channel Access
HCF - Hybrid Coordination Function
HT - High Throughput
HTTP - Hypertext Transfer Protocol
IEEE - Institute of Electrical and Electronics Engineers
IFS - Interframe Space
IP - Internet Protocol
ISM - Industrial, Scientific and Medical
ISO - International Organization for Standardization
LAN - Local Area Network
LLC - Logical Link Control
LQI - Link Quality Indication
LR - Low-Rate
MAC - Medium Access Control
MAN - Metropolitan Area Network
MCF - Mesh Coordination Function
MHz - Megahertz
min - Minuto
OSI - Open Systems Interconnections
PAN - Personal Area Network
PC - Point Coordinator
PCF - Point Coordinator Function
PIFS - Point Interframe Space
PHY - Physical
pkt - Pacote
PPDU - Presentation Protocol Data Unit
PSMP - Power Save Multi-Poll
QoS - Quality Of Service
RD - Reserve Direction
RFD - Reduced Function Device
RIFS - Reduced Interframe Space
RM/OSI - Reference Model OSI
RSSF - Rede de Sensores Sem Fio
RTS - Request To Send
SIFS - Short Interframe Space
SMPT - Simple Mail Transfer Protocol
SPDU - Session Protocol Data Unit
SS - Spread Spectrum
TCC - Trabalho de Conclusão de Curso
TCP - Transmission Control Protocol
TDMA - Time Division Multiple access

TIM - Traffic Indication Map
TPDU - Transport Protocol Data Unit
TR - Tempo Real
TXOP - Transmission Opportunity
UDP- User Datagram Protocol
WLAN- Wireless Local Area Networks
WMAN - Wireless Metropolitan Area Networks
WPAN - Wireless Personal Area Networks
WWAN - Wireless Wide Area Networks
WWW- World Wide Web

SUMÁRIO

1 - INTRODUÇÃO

Atualmente, as redes sem fio são amplamente utilizadas em diversos domínios de aplicação, que variam de simples usos domésticos a complexos sistemas de automação industrial. A motivação para a utilização desta tecnologia está relacionada a questões como baixo custo e facilidade de instalação e manutenção. Atualmente, as redes padronizadas como IEEE 802.11(802.11, 2012), conhecidas como redes WiFi, são o padrão de *facto* em conectividade para redes locais sem fio em ambientes domésticos e de escritório.

Devido à implantação bem sucedida das redes sem fio nos ambientes supracitados, há um grande interesse de uso destas redes em outros domínios de aplicação. As redes de sensores sem fio (RSSF) são um exemplo desses novos domínios, onde a comunicação entre os nós é feita através de uma rede *ad hoc* ou infraestruturada sem fio, e há diversos nodos transmitindo valores do sensoriamento. A ideia é tirar proveito de dispositivos tão pequenos e (espera-se) baratos que possam ser usados em larga escala.

Neste sentido, em 2004 o padrão IEEE 802.15.4 (802.15.4A, 2007) padronizou a primeira versão de uma tecnologia de transmissão sem fio de curto alcance, de baixas taxas de transmissão e, principalmente, com baixo consumo de energia. Essa tecnologia, que ficou conhecida comercialmente como ZigBee, incorpora diversas vantagens e é comumente empregada em projetos de monitoramento e sensoriamento remoto (ANDRIGHETTO, 2008).

Uma característica comum nos dois modelos apresentados é a transmissão dos dados utilizando a faixa de frequência de 2,4GHz à 2,4835GHz, além da tendência em transmitir utilizando o canal de frequência *default* (GARCÍA; ALONSO, 2009; SHUAIB et al., 2005). Logo, em situações reais, atuais e futuras, é muito provável a ocorrência de sobrecarga do canal, podendo ocorrer colisões e atrasos na transmissão, além da consequente perda de dados (MATHEW, 2009), pois, como estas redes operam em um ambiente de comunicação aberto, será comum a existência de várias redes operando na mesma área de cobertura. Outra característica em comum nessas tecnologias é a utilização do protocolo CSMA/CA (*Carrier Sense Multiple Access with Collosion Avoidance*) (MORAES, R.; PORTUGAL; et al., 2010) como mecanismo de controle de acesso ao meio físico.

Atualmente, um número significativo de trabalhos de pesquisa está sendo efetuado no desenvolvimento de redes sem fios de alto desempenho. Então, é provável que num futuro próximo, a ampla

disponibilidade de soluções de redes sem fios deverá gerar um padrão de *facto* para comunicação sem fios na Automação, onde os protocolos IEEE 802.11 e IEEE 802.15.4 são os principais candidatos. A utilização de uma infraestrutura de redes sem fio para a Automação ainda apresenta grandes desafios. Os requisitos das aplicações nesta área são muito específicos. Para além do tráfego genérico, similar àquele encontrado em ambientes de escritório/domésticos, existe tráfego com requisitos de tempo real (TR). Este tráfego está tipicamente associado a aplicações de controle, para as quais os dados devem ser periodicamente transferidos entre sensores e controladores de acordo com metas temporais. Ademais, o meio de comunicação em ambientes sem fio é essencialmente aberto. Isso quer dizer que nestes ambientes, um conjunto de estações externas pode formar, por exemplo, uma rede *ad hoc* e transmitir na mesma faixa de frequência que as estações de tempo real , perturbando o tráfego de TR, que poderá não ser capaz de cumprir as suas especificações temporais. Assim, as abordagens utilizadas em redes cabeadas, baseadas no conhecimento de todo o tráfego da rede, não são mais adequadas. Como consequência, atualmente existem diversas questões em aberto, no domínio das comunicações para a Automação (MORAES, R.; PORTUGAL; et al., 2010).

O presente Trabalho de Conclusão de Curso (TCC) pretende colaborar com os estudos referentes à questão das interferências em redes de sensores sem fio, geradas por sinais transmitidos por outras redes sem fio que, em um meio compartilhado, estejam a operar na mesma faixa de frequência.

1.1 PROBLEMÁTICA E JUSTIFICATIVA

Especialmente em áreas com grande densidade demográfica, há sempre um significativo número de dispositivos sem fio em operação. Atualmente, as principais interfaces de redes sem fio são organizadas de acordo com os padrões IEEE 802.11, IEEE 802.15.1 e IEEE 802.15.4. Apesar destes padrões serem utilizados com diferentes propósitos, conforme especificado anteriormente, há uma característica comum entre eles, que é a transmissão utilizando a mesma frequência de transmissão, ou seja, a frequência de ~2.4GHz - 2,483GHz, que equivalem a uma faixa de transmissão de ~83,5MHz. Esta faixa é reservada ao uso sem licença, da chamada Banda ISM (*Industrial, Scientific, Medical*) (TANENBAUM; WETHERALL, 2011). Considerando a coexistência de diversos dispositivos na mesma área de alcance, as transmissões realizadas por um dispositivo podem interferir

nas transmissões de todos os outros, principalmente, se eles estiverem utilizando o mesmo canal de comunicação (Figura 1).

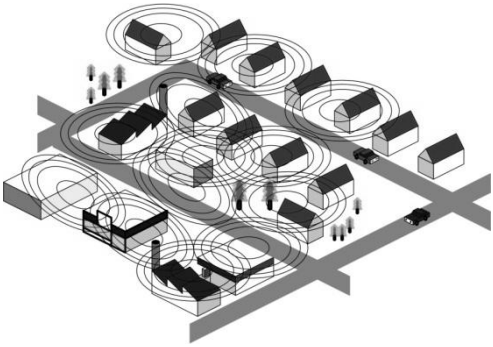

Figura 1: Sobreposição de canais de comunicação.

Há uma competição pelo uso do meio físico quando existem múltiplos sinais emitidos por diferentes dispositivos de comunicação. Em redes cabeadas, essa coexistência é possível, por exemplo, através de mecanismos de suavização de tráfego aplicados às estações que se deseja estabelecer uma maior prioridade de comunicação (LO BELLO; KACZYNSKI; MIRABELLA, 2005). Infelizmente, esta e outras abordagens que consideram um meio de comunicação fechado não são adequadas para ambientes de comunicação sem fio, uma vez que não é possível impor qualquer restrição de tráfego às estações que não pertencem ao mesmo domínio de comunicação (MORAES, RICARDO et al., 2011). Então, pode-se prever a possibilidade de intersecção de faixas espectrais de frequência, o que pode causar problemas na comunicação, como a queda da vazão (*throughput*) (RAMAKRISHNA, 2007). Para que haja soluções nesses tipos de deficiências faz-se necessário o estudo dos níveis interferências. Portanto, este trabalho justifica-se por abordar um problema de especial relevância na comunicação em redes sem fio, que pode ser resumido pela seguinte questão:

Como analisar e propor soluções para minimizar as interferências causadas pela utilização do mesmo canal de comunicação entre as redes IEEE 802.11 e IEEE 802.15.4 que operam em uma mesma área de cobertura?

1.2 OBJETIVOS

Os objetivos deste trabalho são assim dispostos:

1.2.1 Objetivo Geral

Avaliar experimentalmente as interferências causadas pela coexistência de dispositivos de redes sem fio, operando de acordo com os padrões IEEE 802.11 e IEEE 802.15.4, em ambientes abertos.

1.2.2 Objetivos Específicos

- Apresentar uma revisão bibliográfica sobre os padrões de redes sem fio: IEEE 802.11 e IEEE 802.15.4.
- Construir os cenários experimentais para análise das interferências causadas pela coexistência de redes padrões IEEE 802.11 e IEEE 802.15.4.
- Coletar e analisar os dados dos experimentos práticos.

1.3 METODOLOGIA

Tradicionalmente, as propostas de novos mecanismos de comunicação são avaliadas através de métodos analíticos, simulação e análise experimental. Com relação às redes padrão IEEE 802.11, um dos estudos analíticos mais detalhados do protocolo foi apresentado por Bianchi (2000), e estendido mais tarde em muitos aspectos por outros autores, como: Kim (2004), Pham (2005) e Ziouva (2002). Entretanto, uma suposição comum dos estudos analíticos é que, no início da tentativa da transmissão, todas as estações da rede participam no processo de “disputa” pelo acesso ao meio. Assim, este tipo de análise somente aborda cenários de redes saturadas. Para cenários mais realísticos, as técnicas da simulação e/ou análise experimental necessitam ser usadas. Em Moraes et al.(2010), analisou-se o comportamento temporal do mecanismo EDCA quando utilizado para o suporte de comunicação de TR. Basicamente, avaliou-se através de simulação o desempenho da categoria de mais alta prioridade para a transmissão de mensagens em ambientes de comunicação abertos, ou seja, em ambientes sujeitos a perturbações externas.

A metodologia principal a ser aplicada neste Trabalho de Conclusão de Curso (TCC) é a análise experimental, o que o difere dos

trabalhos anteriormente citados. Basicamente, o cenário experimental consiste em dois padrões de redes operando na mesma área de cobertura e, em algumas situações, na mesma frequência de transmissão. Na Figura 2 observa-se, identificada pela letra "W", a representação de uma rede IEEE 802.11 e pela letra "Z", uma rede de padrão IEEE 802.15.4, as duas operando simultaneamente.

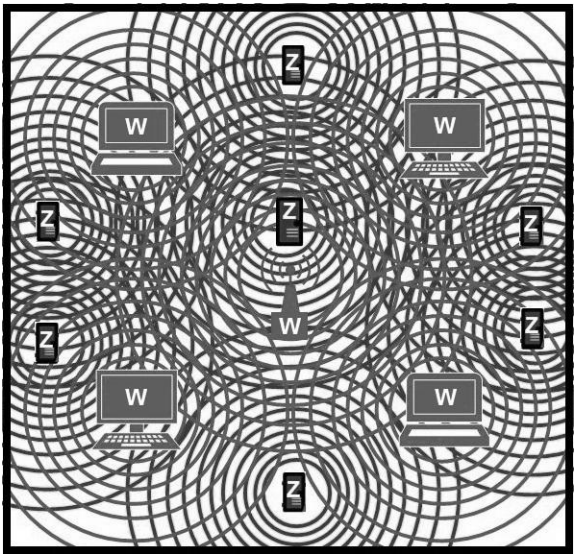

Figura 2 - Exemplo de um cenário experimental.

Algumas métricas de desempenho destas duas redes são analisadas, tais como: taxas de perdas de mensagens, tempo de transmissão, etc. Em um primeiro experimento, as medidas são obtidas somente com as redes IEEE 802.11 ou IEEE 802.15.4 operando isoladamente e, posteriormente, as medidas são obtidas com as duas redes operando simultaneamente e, ainda, variando-se o canal de operação.

1.3.1 Primeira Etapa - Cenário IEEE 802.11

A primeira etapa das análises se dará de forma individual para cada padrão. Para o IEEE 802.11 será construído um cenário com quatro estações conectadas a um *Access Point* (AP) central. O ambiente deverá estar livre de interferências externas, ou seja, não deve existir outros dispositivos transmitindo na mesma área de cobertura. A Figura 3 ilustra

o ambiente onde acontecem as coletas dos dados referentes ao IEEE 802.11.

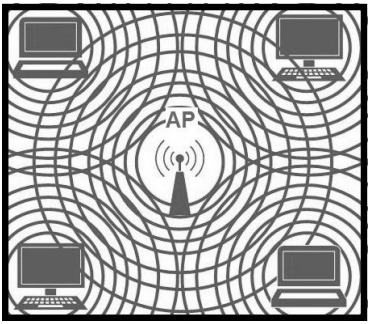

Figura 3: Primeira Etapa - Cenário IEEE 802.11.

1.3.2 Primeira Etapa - Cenário IEEE 802.15.4

Ainda como parte da primeira etapa dos experimentos, são analisadas algumas métricas para o padrão IEEE 802.15.4 individualmente, ou seja, com o mínimo de interferência externa possível. Nesse sentido, sete dispositivos MICAz, de fabricação Crossbow Tech[1], são utilizados para os testes, os quais tem taxa máxima de transmissão de 250kbps, operando na frequência ISM em 2,4 GHz.

Para a comunicação entre os dispositivos será utilizada a topologia estrela, centralizada por um dispositivo de função completa (FDD) operando como coordenador e onde deverão conectar-se os demais nodos da rede. O canal de operação da rede é definido pelo coordenador (Figura 4).

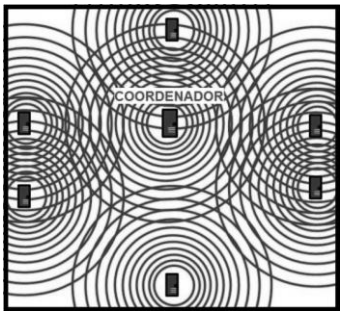

Figura 4: Primeira Etapa - Cenário IEEE 802.15.4

[1]Disponível em: http://www.xbow.com/

Para a coleta de dados referentes ao funcionamento da rede de sensores será usado um dispositivo capturador de pacotes (*sniffer*) IEEE 802.15.4. Então, os dados são compilados pelo software "ZENA™ Wireless Network Analyzer", desenvolvido pela Microchip Technology[2].

1.3.3 Segunda Etapa e Resultados

A segunda etapa da fase experimental deste trabalho consiste - na junção das duas tecnologias operando num mesmo ambiente, conforme demonstrado na Erro! Fonte de referência não encontrada.. onsiderando a possibilidade de sobreposição de sinal mesmo no caso dos dispositivos operando em canais diferentes, faz-se necessário que o experimento contemple algumas possibilidades de canais em ambas as tecnologias de rede sem fio.

Os resultados são analisados considerando as variações nas taxas de transmissão e perda de mensagens em cada canal. Comparando os resultados obtidos no cenário em que o meio de comunicação é exclusivo com o cenário de meio compartilhado, será possível analisar os efeitos concretos das interferências geradas por redes externas.

1.4 ORGANIZAÇÃO DO TRABALHO

Este trabalho está dividido em duas partes. Inicialmente, apresenta-se uma revisão bibliográfica abordando questões referentes às redes sem fio. A segunda parte do trabalho compreende a parte prática, onde são coletados os dados necessários às análises das possíveis interferências entre as redes.

A primeira parte do trabalho ainda compreende o estudo dos modelos de referência e topologias de rede, bem como as camadas e subcamadas do padrão 802. Além da apresentação das características próprias de cada um dos padrões estudados, IEEE 802.11 e IEEE 802.15.4.

[2] Disponível em: http://www.microchip.com/

2 - FUNDAMENTAÇÃO TEÓRICA

O presente capítulo tem por objetivo apresentar a base teórica dos estudos relacionados com este trabalho. Para tanto, serão expostos os modelos de referência: ISO/OSI (*International Standards Organization/Open Systems Interconnection*), tratando individualmente de cada camada; e, de maneira mais breve, o modelo TCP/IP (*Transmission Control Protocol/Internet Protocol)*.

Em seguida, apresentam-se algumas das topologias de rede mais comuns, relatando seu funcionamento tanto para o padrão IEEE 802.11 quanto para o IEEE 802.15.4. E por fim, são abordadas algumas formas de comunicação sem fio, enfatizando a operação de redes baseadas em radiofrequência.

2.1 MODELO DE REDE ISO/OSI

O modelo de referência OSI (Figura 5) foi desenvolvido com base em uma proposta já existente desenvolvida pela *International Standards Organization* (ISO). Este modelo trata da interconexão de sistemas abertos à comunicação com outros sistemas. Neste sentido, o OSI foi o primeiro modelo desenvolvido com o intuito de padronizar, em níveis internacionais, os protocolos utilizados pelas várias camadas de uma rede.

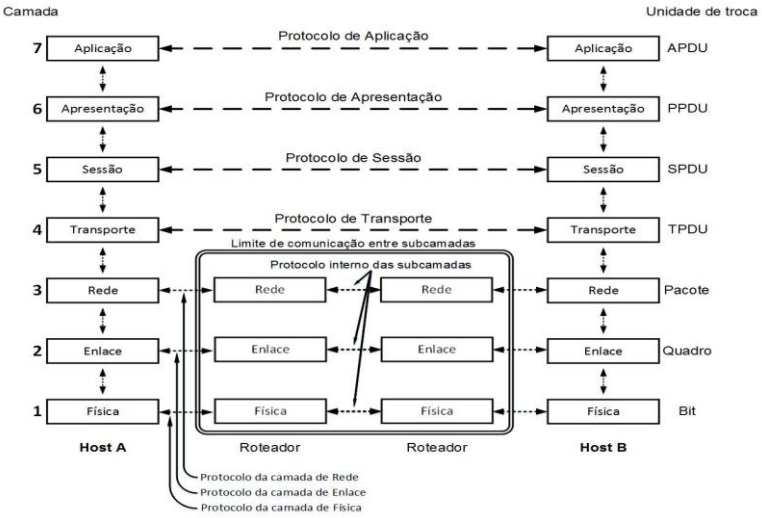

Figura 5 - Modelo de referência OSI.

Tanenbaum e Wetherall (2011) propõem um resumo dos princípios aplicados no desenvolvimento das sete camadas do modelo OSI. São eles:

> "1. Uma camada deve ser criada onde houver necessidade de outro grau de abstração;
> 2. Cada camada deve executar uma função bem definida;
> 3. A função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente;
> 4. Os limites de camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces;
> 5. O número de camadas deve ser grande o bastante para que funções distintas não precisem ser, desnecessariamente, colocadas na mesma camada e pequeno o suficiente para que a arquitetura não se torne difícil de controlar."

Em suma, cada uma das sete camadas previstas deve fornecer serviço de comunicação com confiabilidade à camada seguinte. A transferência de dados e informações de controle é realizada junto à camada imediatamente anterior até chegar à camada Física, onde ocorre efetivamente a transmissão da informação por meios físicos. E, ao chegar a mensagem ao receptor, esse processo é repetido inversamente pelo sistema até que se chegue à camada de aplicação.

Portanto, cada camada pode comunicar-se apenas com outra camada imediatamente superior ou inferior, além de todas terem responsabilidades individuais de processamento da mensagem.

2.1.1 Camada Física (PHY)

Kurose e Ross (2006) definem que a principal tarefa da camada física é "movimentar os bits individuais que estão dentro do quadro de um nó, para o nó seguinte". Ou seja, a camada física se responsabiliza em transmitir os bits pelo canal de comunicação.

Porém, os protocolos desta camada são dependentes dos meios de transmissão do enlace. Por exemplo, a *Ethernet* tem muitos protocolos para a camada física, entre eles: o *Token Ring* , que atua em meio de transmissão em par de fios de cobre trançados. Dessa maneira, também existem protocolos para cabo coaxial e para fibra ótica e, em cada caso, a movimentação do bit ocorre de maneira singular.

A questão de camada física mais comum é como os impulsos elétricos devem ser usados para representar corretamente um bit=1 ou um bit=0. Neste sentido, Kurose e Ross (2006) propõem que "o projeto

da rede deve garantir que, quando um lado enviar um bit=1, o outro lado deverá receber o bit=1, não um bit=0".

Ainda, é responsabilidade da camada física determinar o tempo de duração de um bit, normalmente em nanossegundos. Além da verificação da possibilidade de que os dados sejam transmitidos simultaneamente em sentidos opostos e, é claro, determinar a forma como a conexão inicial será estabelecida e encerrada. A quantidade de pinos de um conector de rede e a função de cada um também deve ser prevista pela camada física.

Segundo Semprebom (2012), tratando-se do padrão IEEE 802.15.4, a principal responsabilidade da camada física está na "transmissão e recepção de dados utilizando um determinado canal de rádio de acordo com alguma modulação ou técnica de difusão".

A padronização proposta pelo IEEE 802.15.4 (802.15.4A, 2007) designa a camada física destes dispositivos como responsável pelas seguintes tarefas:

- Ativação e desativação do transceptor de rádio: ligar ou desligar, de acordo com o pedido da subcamada MAC, o transceptor de rádio em um dos seguintes estados: transmitindo, recebendo, ou desligado (*sleeping*).
- Detecção de energia (*Energy Detection* - ED) no canal atual: consiste em fornecer uma estimativa da energia do sinal recebido dentro da largura de banda de um canal IEEE 802.15.4, que determina o estado do canal: ocioso ou ocupado. É utilizado pelo método *Clear Channel Assessment* que avalia como ocupado o canal onde é detectada energia acima de um limiar de energia predefinido.
- Indicação de qualidade de enlace (*Link Quality Indication* - LQI): fornece uma medida de indicação de qualidade de enlace que é realizada para cada pacote recebido. Pode ser utilizado pelas camadas de rede e aplicação para a implementação de suas políticas.
- Avaliação de canal disponível (*Clear Channel Assessment* - CCA): a camada PHY pode realizar a CCA usando o modo de detecção de energia (ED) ou de detecção de portadora, modo este que consiste em reportar o cenário de canal ocupado quando as mesmas características de modulação e difusão do IEEE 802.15.4 são detectados no sinal. Existe ainda um modo híbrido que combina os dois modos de operação supracitados.

- Seleção da frequência do canal: ao receber uma solicitação da subcamada MAC, a camada física deve estar apta a sintonizar o seu transceptor em um dos canais possíveis pra a operação do enlace.

2.1.2 Camada de Enlace (*Data Link*)

A camada de enlace é responsável por dividir os dados de entrada em quadros de dados e transmiti-los sequencialmente. Se o serviço for confiável o receptor retornará um quadro de confirmação (ACK), informando que a informação foi recebida corretamente.

A principal tarefa desenvolvida pela camada de enlace de dados, segundo Tanenbaum e Wetherall (2011) "é transformar um canal de comunicação normal em uma linha que pareça livre de erros de transmissão".

A regulação do tráfego também representa uma importante questão para a camada de enlace. Por exemplo: o que fazer quando um ponto transmite os quadros em uma velocidade ao qual o ponto receptor não tem capacidade de suportar? Para tanto, deve-se haver um mecanismo que informe ao transmissor quando o receptor está apto receber mais quadros.

As redes sem fio, que representam o foco do presente trabalho, são denominadas redes de *broadcast*, ou seja, a informação é difundida a todos os integrantes da rede, porém, apenas a estação de destino deverá abrir a mensagem. Isso representa um agravante adicional a ser resolvido pela camada de enlace: como melhor realizar o controle de acesso a um meio compartilhado. Neste sentido, foi desenvolvida uma subcamada especial para a camada de enlace (TANENBAUM; WETHERALL, 2011), a subcamada de controle do acesso ao meio (MAC).

2.1.3 Camada de Rede (*Network*)

Enquanto, movimentar quadros inteiros de um elemento de rede até um elemento adjacente é tarefa da camada de Enlace (KUROSE; ROSS, 2006), a camada de rede se responsabiliza pela movimentação de pacotes, chamados de datagramas nesta camada, de uma máquina para a outra.

A camada de rede define dois componentes principais: um protocolo de roteamento que determina as rotas que os datagramas percorrem entre a origem e o destino, e o protocolo IP, que deve ser

executado por todos os dispositivos que definam uma camada de rede. Este fato reflete o elemento fundamental que mantém a integridade da rede, a impossibilidade de duplicidade de identificadores de dispositivos que estejam interconectados por um enlace, formando uma rede (KUROSE; ROSS, 2006).

Dessa maneira, as rotas que serão percorridas pelos pacotes são definidas pela camada de rede com base em tabelas estáticas constantemente atualizadas, o que evita componentes defeituosos (TANENBAUM; WETHERALL, 2011). Assim, a maneira como os pacotes são roteados, da origem até o seu destino, representa uma questão fundamental para essa camada.

Muitos problemas podem surgir no percurso de um pacote que precisa trafegar de uma rede para outra até encontrar seu destino. Poderão ocorrer "gargalos" de rede quando existirem muitos pacotes dividindo o mesmo caminho, ao mesmo tempo na sub-rede. A carga imposta à rede deve ser adaptada pelas camadas superiores, porém, a responsabilidade de informá-las da necessidade de um possível controle de congestionamento pertence à camada de rede, ou seja, a qualidade de serviço fornecido (QoS), considerando fatores como: atraso, tempo em trânsito, instabilidade, etc, também são questões pertinentes a essa mesma camada.

A camada de rede em redes *broadcast* é, geralmente, estreita ou mesmo inexistente, pelo fato de não existirem muitos problemas de roteamento com redes desta natureza (TANENBAUM; WETHERALL, 2011).

No modelo TCP/IP, a camada de rede recebe do protocolo de camada de transporte (TCP ou UDP) um endereço de destino e um segmento de camada de transporte, devendo entregá-lo à camada de transporte do dispositivo destinatário (KUROSE; ROSS, 2006).

2.1.4 Camada de Transporte (*Transport*)

A camada de transporte garante a integridade da comunicação, dividindo o arquivo em vários segmentos menores no sistema transmissor e remontando-os em sua formatação original no sistema receptor. Também deve advertir a camada seguinte quando do sucesso ou insucesso da comunicação realizando, dessa forma, uma transmissão de informação tida como confiável.

Tanenbaum e Wetherall (2011) determinam que "a camada de transporte é uma verdadeira camada ponta a ponta, que liga a origem ao destino". De maneira prática, essa expressão pode ser compreendida ao

analisar, por exemplo, uma aplicação executando em uma estação origem que mantém uma conversação com uma aplicação semelhante que executa em uma estação destino. A camada de transporte dá condições para a existência desses cenários através de cabeçalhos de mensagem e mensagens de controle periódicas.

O modelo TCP/IP não prevê a existências das camadas de sessão e de apresentação, dessa maneira, a camada de transporte carrega mensagens da camada de aplicação entre os lados do cliente e servidor de uma aplicação. Esse mesmo modelo ainda define dois protocolos de transporte: TCP, serviço orientado à conexão e a confiabilidade de entrega dos dados; e o UDP, protocolo muito utilizado em sistemas VoIp e de videoconferência, por se tratar de um serviço não orientado a conexão.

2.1.5 Camada de Sessão (*Session*)

Segundo Tanenbaum e Wetherall (2011), "a camada de sessão permite que os usuários em diferentes máquinas estabeleçam sessões de comunicação entre si". Entre os serviços fornecidos por uma sessão estão: controle de diálogo, determinando quem deve transmitir em cada momento; gerenciamento de *tokens*, impedindo uma operação crítica de ser executada por duas partes ao mesmo tempo; e sincronização, realizando a recuperação subsequente de possíveis falhas ocorridas em transmissões longas, permitindo que as mesmas continuem a partir do ponto em que estavam, isso é possível por causa de um método de verificação periódica de longas transmissões.

2.1.6 Camada de Apresentação (*Presentation*)

Estruturas de dados de alto nível requerem também níveis mais altos de abstração. Para realizar a definição e o intercambio dessas estruturas nas redes é que se pensou no desenvolvimento de uma camada de Apresentação.

Tanenbaum e Wetherall (2011) dizem que "para tornar possível a comunicação entre computadores com diferentes representações internas dos dados, as estruturas de dados a serem trocadas podem ser definidas de maneira abstrata, com uma codificação padrão que será usada durante a conexão". Portanto, enquanto as camadas mais baixas relacionam-se com a movimentação de bits, a camada de apresentação preocupa-se principalmente com a sintaxe e a semântica das informações transmitidas.

2.1.7 Camada de Aplicação (*Application*)

A camada de aplicação definida pelo modelo TPC/IP, concentra as funções das camadas de sessão e apresentação definidas no modelo OSI. Para Tanenbaum e Wetherall (2011) "a experiência com o modelo OSI demonstrou que essa visão está correta: elas (as camadas de sessão e apresentação) são pouco usadas na maioria das aplicações".

Os protocolos HTTP (*HyperTextTranfer Protocol*), SMTP (*Simple Mail Transfer Protocol*) e FTP (*File Transfer Protocol*) figuram entre os protocolos mais utilizados na atualidade, em especial o HTTP que constitui a base para a *World Wide Web* (KUROSE; ROSS, 2006).

Também está na lista de tarefas da camada de aplicação, realizar a interface com os servidores DNS (*Domain Name System*) que realizam a tradução de nomes em endereços de 32 bits (KUROSE; ROSS, 2006), além da utilização do protocolo de terminal virtual TELNET.

2.2 MODELO DE REDE TCP/IP

Impulsionado pela ideia do desenvolvimento de uma rede que pudesse suportar a tudo, inclusive um ataque nuclear, o Departamento de Defesa dos Estados Unidos (DoD) iniciou o desenvolvimento de uma rede de pesquisa que interligou por linhas telefônicas dedicadas, universidades e repartições públicas dos EUA. Essa rede, conhecida como ARPANet, antecedeu o modelo de referência TPC/IP, desenvolvido para que as conexões permanecessem intactas enquanto as máquinas de origem e destino estiverem funcionando, mesmo que algumas máquinas intermediárias tivessem deixado de operar (TANENBAUM; WETHERALL, 2011).

Existem algumas semelhanças entre o modelo de referência OSI e o modelo TCP/IP. Ambos propõem a divisão em camadas, algumas com definições bem próximas aos dois modelos. É o caso das camadas de transporte e de rede, que definem tarefas semelhantes nas duas modelagens. Além da tecnologia de comutação de pacote, em detrimento da comutação de circuitos, presumida por ambos.

Algumas camadas definidas no TCP/IP tem denominação coincidente com o modelo OSI, porém definem funções não correspondentes. Por exemplo, a camada de aplicação no modelo TCP/IP combina aspectos definidos pelas camadas de apresentação e sessão da modelagem OSI, como questões de representação, codificação

e controle de diálogo. Outro caso semelhante é a combinação de elementos que, no modelo OSI correspondem às camadas física e de enlace, em uma única camada: a camada de acesso à Rede.

Porém, a credibilidade do modelo TCP/IP está diretamente relacionada aos protocolos em torno dos quais a Internet se desenvolveu. São protocolos desenvolvidos para o TCP/IP: *File Transfer Protocol* (FTP), *Hypertext Transfer Protocol* (HTTP), *Simple Mail Transfer Protocol* (SMTP) e Sistema de Nomes de Domínios (DNS) (KUROSE; ROSS, 2006).

2.3 TOPOLOGIAS DE REDE

A organização dos enlaces físicos em um sistema de comunicação confronta-se com diversas formas possíveis de utilização das vias de transmissão. Basicamente, as interconexões físicas podem se dar de duas maneiras: Multiponto (Figura 6) ou ponto a ponto (Figura 7).

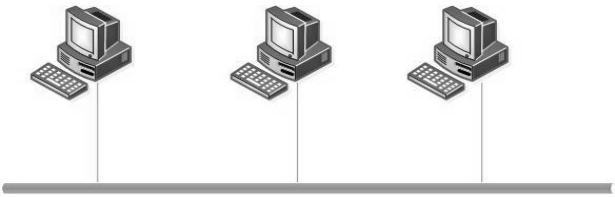

Figura 6: Conexão Multiponto.

Figura 7: Conexão ponto a ponto.

Dessa maneira, as conexões multiponto caracterizam-se pela presença de três ou mais hosts com a possibilidade de utilização do mesmo enlace. E em ligações ponto a ponto observa-se a utilização de apenas dois dispositivos de comunicação, um em cada extremidade do enlace.

Todavia, a topologia ponto a ponto definida para o padrão IEEE 802.15.4 determina que cada dispositivo pode se comunicar diretamente com qualquer outro, desde que esteja dentro de sua área de abrangência.

Esse modo de operação prevê a atuação de um coordenador da rede PAN (*Personal Area Network*), o qual será determinado pela ordem de transmissão no canal, ou seja, o coordenador será o primeiro nó a comunicar na rede (SEMPREBOM, 2012). A Figura 8 ilustra essa topologia em redes PAN.

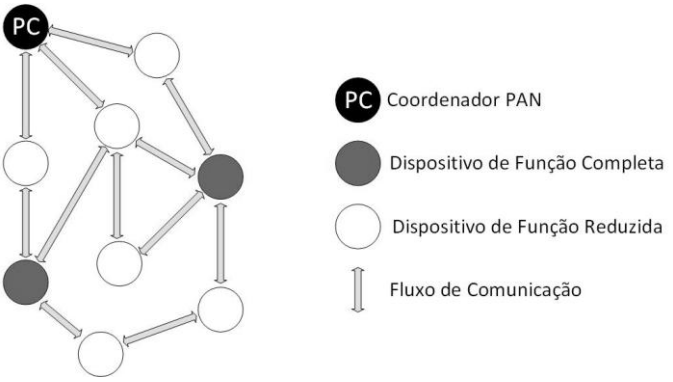

Figura 8: Topologia ponto a ponto com padrão IEEE 802.15.4.
Fonte: (SEMPREBOM, 2012).

O modo como o meio físico que conecta as estações é utilizado, no que diz respeito à forma de comunicação no enlace, pode ser classificado da seguinte maneira: *simplex*, *half-duplex* e *full-duplex*.

Segundo Andrighetto (2008), no modo *simplex* o enlace é utilizado apenas em um dos dois possíveis sentidos de transmissão. Já no modo *half-duplex* o enlace é utilizado nos dois possíveis sentidos de transmissão, porém apenas um por vez. E quando o enlace é utilizado nos dois possíveis sentidos de transmissão simultaneamente, observa-se o modo *full-duplex*.

Redes de computadores podem ser classificadas também pela topologia que assumem. Trata-se da topologia física e da maneira como os dispositivos de rede estarão conectados, ou seja, é a descrição do projeto básico da rede.

As redes sem fio podem operar em duas topologias básicas: topologia estruturada, onde as estações estão dispostas em uma célula controlada e limitada pelo alcance de um *Access Point* (AP); e topologia *ad hoc*, onde vários dispositivos de rede se interconectam diretamente dispensando, assim, a figura de um controlador central (MORAES, R.; PORTUGAL; et al., 2010).

2.3.1 Topologia Estrela

A topologia de rede em formato estrela caracteriza-se por prever a figura de um nó mestre na configuração do sistema. Todos os dispositivos deverão estar conectados ao mestre, que desempenhará a função de entregar mensagens aos hosts escravos. Essa técnica é conhecida como *Master/Slave*, onde todas as mensagens devem passar por um nó central que age como centro de controle da rede.

Essa topologia pode ser desvantajosa em cenários de grande circulação de mensagens, pois poderá haver uma sobrecarga do dispositivo que realiza a função de nó mestre da rede. Os limites de transmissão da topologia estrela são impostos pela capacidade de processamento do nó central.

As poucas vias de comunicação subordinam a estabilidade da rede ao bom funcionamento do nó mestre, ou seja, a rede inteira terá problemas quando existirem falhas no dispositivo central. A Figura 9 apresenta uma rede de computadores comum organizados conforme a topologia estrela, ao centro encontra-se o nó mestre e nas bordas os nós escravos.

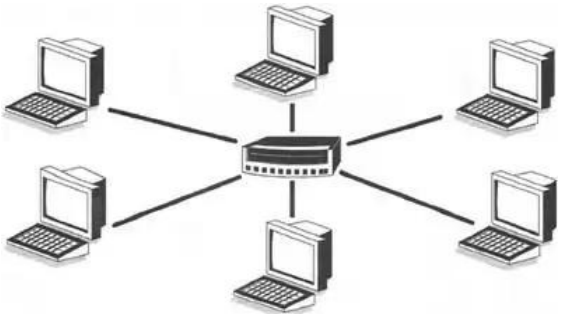

Figura 9: Topologia Estrela.

No caso de redes formadas por dispositivos de padrão IEEE 802.15.4, a topologia em estrela substitui a figura do nó mestre pela figura de um Dispositivo de Função Completa (FDD) que desempenha a função de coordenador da Rede PAN, conforme ilustra a Figura 10.

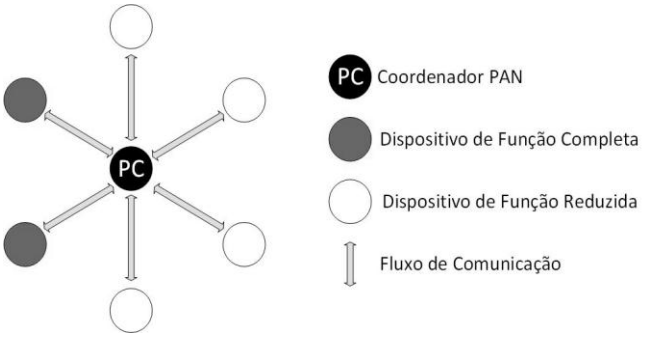

Figura 10: Topologia ponto a ponto - padrão IEEE 802.15.4.
Fonte: (SEMPREBOM, 2012).

Um FDD é um dispositivo que pode operar em três modos diferentes: Coordenador PAN, que é o identificador e controlador central da rede, todos os demais nós devem estar associados ao Coordenador PAN; Coordenador local ou líder de agrupamento, que realiza a função de um sub-coordenador em agrupamentos de dispositivos, oferecendo serviços de sincronização através da transmissão periódica de sinais de *beacon* e devendo sempre estar associado a um coordenador PAN; e Dispositivo Simples, onde nenhuma das configurações supracitadas são implementadas (SEMPREBOM, 2012).

Há ainda outro tipo de dispositivo IEEE 802.15.4 que opera com uma implementação mínima, chamado de Dispositivo de Função Reduzida. Esses dispositivos sempre estão associados a um único FDD e é destinado a exercer funções mais simples, onde não exista a necessidade de transmissão de grandes quantidades de dados (SEMPREBOM, 2012).

2.3.2 Topologia Anel

Na topologia de rede em Anel, o sinal originado por um nó é regenerado e retransmitido a cada vez que passa por um host. Nestes casos, a mensagem só é aberta quando chega ao seu nó de destino, que é identificado por um endereço único na rede e, ao reconhecer-se como destino da mensagem, aceita-a.

Redes em topologia anel podem transmitir dados em qualquer direção, porém, é mais comum a sua utilização unidirecional simplificando, assim, o processo de regeneração e retransmissão do sinal. Este modo de utilização tende a evitar problemas com roteamento

e simplificar o processo de comunicação entre os nodos. Observa-se, na Figura 11, a representação desta topologia com seus nós e ligações.

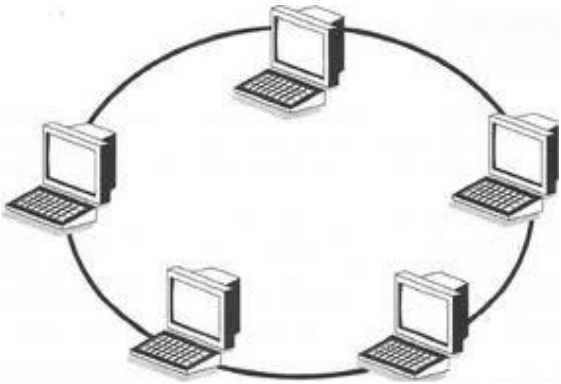

Figura 11: Topologia em Anel.

Uma confirmação de recebimento de mensagem deve ser enviada ao transmissor no ato da sua recepção, caso contrário, este irá identificar uma interrupção no anel e tentará isolá-la. Uma simples cronometragem da mensagem pode informar a localização da estação defeituosa ou mesmo a falta do *status* de estação.

Essa topologia pode gerar problemas com mensagens que tentem a circular eternamente no anel por conta de erros de processamento ou transmissão, pois uma mensagem enviada a um nó específico precisa circular até ser retirada pelo nó que se identifica como destino da mesma.

2.3.3 Agrupamento em Árvores

O agrupamento em árvore é um caso especial da topologia ponto a ponto, onde alguns nodos podem assumir a função supracitada de coordenador local. Neste caso, o coordenador PAN é único na rede e tem a função de identificá-la como um todo e, para realizar a função de líder de agrupamento o dispositivo precisa, necessariamente, ser FDD. Os RFDs podem se conectar ao agrupamento como um nodo livre no final da árvore (SEMPREBOM, 2012).

De acordo com a especificação do padrão IEEE 802.15.4 (802.15.4A, 2007), o agrupamento em árvore é possível e deve ser iniciado pelas camadas superiores, porém não há definição específica de como construí-lo.

Existem duas visões distintas na formação de um agrupamento: a visão do coordenador PAN e a visão dos nós que pretendem integrarem-se à rede (SEMPREBOM, 2012).

Cabe ao nó que forma o primeiro agrupamento a função de nomear a si mesmo como líder do agrupamento (*Cluster Head* - CH) sendo detentor do identificador do agrupamento (*Cluster Identificator* - CID), ao qual será atribuído o valor zero. Em seguida, o mesmo nó escolhe um Identificador PAN ainda não utilizado e passa a difundir sinais de *beacon* para os dispositivos vizinhos, anunciando a existência da sua rede.

A junção de um novo nó ao agrupamento acontece quando o dispositivo recebe um quadro de *beacon* proveniente do coordenador e, então, solicita a sua entrada no grupo. No caso de o coordenador aceitar a solicitação enviada, o dispositivo é adicionado como um dispositivo filho em sua lista de vizinhos. O próximo passo é o novo *host* adicionar o CH como nodo pai em sua lista de vizinhos e então passa a transmitir *beacons* periodicamente. Outros dispositivos podem juntar-se à rede por meio do novo nó, caso recebam uma mensagem de *beacon* deste mesmo dispositivo. Caso o nó candidato não consiga juntar-se à rede por meio do CH, este deverá procurar por um outro dispositivo vizinho qualquer.

A Figura 12 demonstra o funcionamento do agrupamento em árvore aplicado a dispositivos de padrão IEEE 802.15.4.

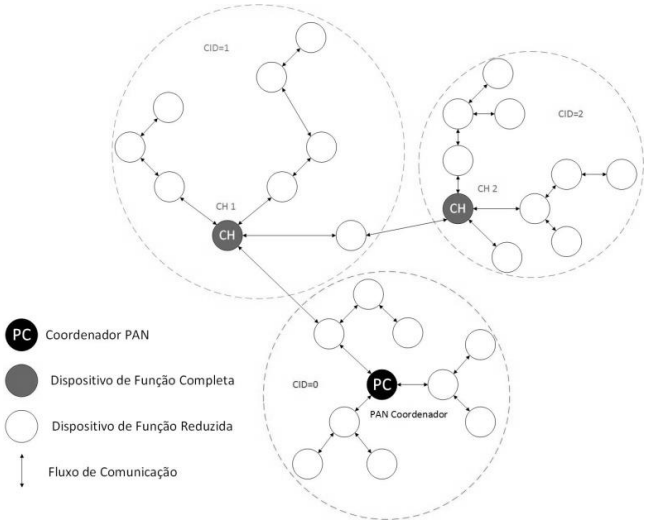

Figura 12: Agrupamento em árvore.
Fonte: (SEMPREBOM, 2012).

2.4 REDES SEM FIO

As redes wireless, ou redes sem fio, configuram uma extensão ou mesmo uma alternativa às redes locais onde os *hosts* são interconectados via cabo (LANs cabeadas). Trata-se de um sistema de comunicação de dados extremamente flexível que combina a conectividade de dados com mobilidade. Atualmente, esse tipo de rede está largamente difundida devido, principalmente, à facilidade em instalar e utilizar.

Além das características de mobilidade, rapidez e simplicidade na instalação e de flexibilidade no uso de redes sem fio, esse tipo de tecnologia apresenta variados benefícios se comparada às redes tradicionais. Escalabilidade e redução no custo de instalação são fatores que justificam a sua utilização em quase todos os mercados. As redes wireless podem ser aplicadas em hospitais, universidades, fábricas, lojas, bancos, escritórios e prover necessidades de pequenas, médias e grandes empresas.

Existem fatores críticos a serem analisados quando da instalação de redes sem fio. Moraes et al. (2010) elencam alguns: segurança dos dados, conectividade com redes locais existentes, mobilidade/portabilidade/compatibilidade, performance, gerenciamento, facilidade de instalação, custo acessível e imunidade a interferências.

Para prover a comunicação em redes que não utilizam cabos para conectar seus *hosts* existem tecnologias baseadas em sistemas óticos e de radiofrequência para transmissão dos dados.

Tecnologias de comunicações ópticas pelo espaço livre (FSO, *free space optic communication system*) pretendem realizar a comunicação sem fio por meio da emissão, recepção e interpretação de sinais luminosos. Para tanto estão disponíveis quatro faixas de comprimentos de onda luminosa. São elas: entre 800nm a 900nm, em torno de 1,3μm, 1,55μm, e 1,6μm (VILELA, 2013).

Entretanto, as redes sem fio que utilizam espectro de rádio frequência para realizar a comunicação, são qualificadas considerando sua extensão e abrangência e de acordo com a especificação e os protocolos que cada tecnologia emprega. Esses modelos podem ser definidos com: *Wireless Personal Area Network* (WPAN) que são as redes pessoais de curto alcance; *Wireless Local Area Network* (WLAN) que são as redes locais formadas entre um conjunto de equipamentos dentro de uma empresa ou casa, por exemplo; *Wireless Metropolitan Area Network* (WMAN) que são as redes capazes de abranger e comunicar dispositivos em diferentes pontos de uma mesma cidade; e a

Wireless Wide Area Network (WWAN) que são capazes de intercomunicar diferentes cidades e comunicar dispositivos de um lado a outro no globo terrestre como o caso das telefonias celulares, como observa-se no Quadro 1.

Faixa de Freqüência (Hz)	Denominação Técnica	Denominação Popular	Exemplos de Utilização
300 a 3000	E.L.F (*Extremely Low Frequency*)	Ondas Extremamente longas	Comunicação para submarinos, escavações de minas etc.
3K a 30K	V.L.F. (*Very Low Frequency*)	Ondas muito longas	Comunicação para submarinos, escavações de minas etc.
30K a 300K	L.F. (*Low Frequency*)	Ondas longas	Auxílio à navegação aérea, serviços marítimos, radiodifusão local.
300K a 3M	M.F. (*Medium Frequency*)	Ondas médias	Auxílio à navegação aérea, serviços marítimos, radiodifusão local.
3M a 30M	H.F (*High Frequency*)	Ondas tropicais / Ondas curtas	Radiodifusão local e distante, sistemas marítimos (estações costeiras).
30M a 300M	V.H.F. (*Very High Frequency*)	Microondas	Transmissão de TV, sistemas comerciais e particulares de comunicação, serviços de segurança pública (Polícia, Bombeiros etc.).
300M a 2G	U.H.F. (*Ultra High Frequency*)	Microondas	Transmissão de TV, sistemas comerciais e particulares de comunicação, serviços de segurança pública (Polícia, Bombeiros etc.).
2G a 3G	U.H.F. (*Ultra High Frequency*)	Microondas	Comunicação pública à longa distância: sistemas interurbanos e internacionais em radiovisibilidade, tropodifusão e satélite.
3G a 30G	S.H.F. (*Super High Frequency*)	Microondas	Comunicação pública à longa distância: sistemas interurbanos e internacionais em radiovisibilidade, tropodifusão e satélite.
30G a 300G	E.H.F (*Extremely High Frequency*)	Microondas	Comunicação pública à longa distância: sistemas interurbanos e internacionais em radiovisibilidade, tropodifusão e satélite.

Quadro 1 - Faixas de frequência em telecomunicações.
Fonte: (KUROSE; ROSS, 2006).

2.4.1 Sistemas Infravermelho

Os equipamentos utilizados para transmissão de dados com infravermelho têm como características principais a não obrigatoriedade de licença para operação além do baixo custo na sua utilização e implantação. Um bom exemplo da utilização de comunicação infravermelho no dia-a-dia são os controles remotos de eletrodomésticos como: televisões, rádios, etc.

A transmissão via sinal infravermelho pode acontecer de duas formas: linha de visada, onde o sinal de infravermelho é emitido em uma faixa relativamente estreita e direcionada; ou difuso, quando o sinal é transmitido em uma faixa maior, não necessitando de visada entre os equipamentos (DE MORAES, 2012). A Figura 13 apresenta as duas formas de transmissão infravermelho.

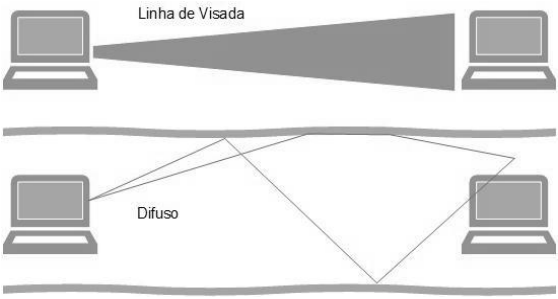

Figura 13: Formas de transmissão do infravermelho.

Os sistemas infravermelhos diretos de baixo custo fornecem uma distância muito limitada, em torno de 1,5 metros (ANDRIGHETTO, 2008), porém conseguem taxas de transmissão de até 16Mbps. Assim como a luz visível, a luz infravermelha também não atravessa materiais opacos como paredes e mobília, limitando a atuação do transmissor ao seu campo de visão (MARTINCOSKI, 2003). Esse tipo de sistema de comunicação é principalmente aplicadas às redes WPAN, Wireless Personal Area Network, e ocasionalmente em WLAN, Wireless Local Area Network.

2.4.2 Sistemas Laser

O uso da tecnologia laser para a comunicação e transmissão de dados não pressupõe nenhum tipo de concessão ou outorga, por se tratar de um sistema que utiliza a luz para a transmissão do sinal digital. Este tipo de sistema pode alcançar taxas de transferência de até 2.5 gigabits por segundo em uma distância média de dez quilômetros (DE MORAES, 2012) trabalhando, portanto, com alta largura de banda.

Essa tecnologia sofre interferência de condições atmosféricas como neblina e chuvas torrenciais o que pode, inclusive, causar a interrupção do canal. Outra característica é o fato de que, quando se utiliza um feixe de luz direcional o enlace permite apenas conexões ponto a ponto não existindo, portanto, a topologia multiponto. A Figura 14 mostra um equipamento que provê a comunicação laser.

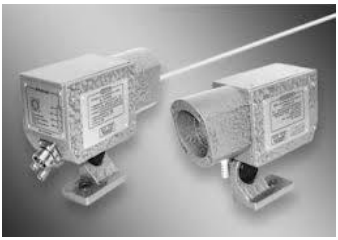

Figura 14: Equipamento laser para enlace ponto a ponto.

2.4.3 Sistemas de Radiofrequência

Sistema de rádio frequência, sistema de micro-ondas (MORAES, 2010) ou mesmo sistemas de espalhamento espectral (*Spread Spectrum - SS*) (ANDRIGHETTO, 2008) constituem o objeto principal do presente estudo. As redes IEEE 802.11 e IEEE 802.15.4 operam na faixa de frequência ISM, ou seja, entre 902MHz e 928MHz, entre 2.4GHz e 2.48 GHz ou entre 5.1GHz e 5.9GHz, tendendo à existência de interferências quando operam simultaneamente em um espaço comum.

A banda de 2.4GHz é a mais utilizada da faixa ISM, por isso também é a mais poluída (FRANÇA, 1997). Uma vasta quantidade de equipamentos utilizam-se desta frequência, como por exemplo: telefones sem fio, Bluetooth, forno de micro-ondas, e as camadas físicas padronizadas pelos padrões IEEE 802.11b (802.11B, 2001), IEEE 802.11g (802.11G, 2003), IEEE 802.11n (802.11N, 2009) e até mesmo pelo novo padrão que está em elaboração, o IEEE 802.11af (802.11AF, 2013).

No Brasil, existem ainda outras faixas reservadas para ISM, 24GHz – 24,25GHz e 61GHz – 61,5GHz por exemplo (FRANÇA, 1997). Todavia, a principal diferença dessas faixas que usam frequências mais altas é o alcance do sinal. Comparativamente menor em comparação ao alcance de sinal de outras frequências, o alcance das faixas de 24GHz e 61GHz podem ser tanto um problema em ambientes muito amplos quanto uma vantagem quando não se deseja grandes áreas de abrangência de sinal.

Originalmente os sistemas de rádio frequência foram desenvolvidos para prover a comunicação entre militares durante a segunda guerra mundial com o objetivo de transformar a informação a ser transmitida num sinal parecido com um ruído radioelétrico evitando assim o monitoramento pelas forças inimigas (OLIVEIRA; BERNAL, 2013).

O espalhamento do espectro de rádio frequência ocorre quando, na fase de transmissão se utiliza um código pseudo-aleatório. E na fase de recepção recupera-se o sinal espalhado utilizando o mesmo código usado no ato da transmissão.

França (1997) propõe o que chama de uma forma simples de entender como funciona o SS é fazendo a seguinte analogia:

> "Imagine uma concentração de energia (portadora) em um tubo de ensaio. Divida essa energia em várias partes, colocadas lado a lado em tubos de ensaio menores (isto seria o espectro espalhado). Para ser recuperada a energia inicial, despeje o conteúdo de cada tubinho no tubo principal."

A Figura 15 apresenta a comparação simbólica proposta por França.

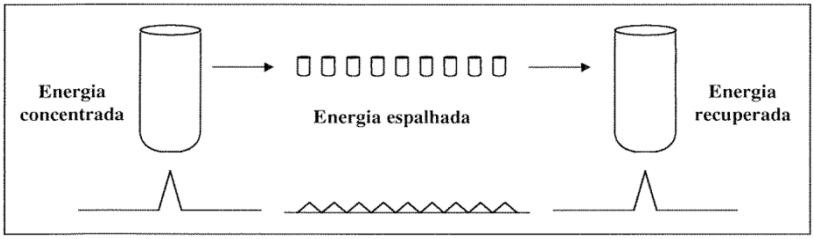

Figura 15: Espalhamento de energia.

A transmissão de dados via rádio com alta confiabilidade e com taxas de transmissão cada vez maiores só puderam ser viabilizadas pelo desenvolvimento da tecnologia de espalhamento espectral, o que possibilitou também o seu uso na implementação de redes locais, WLAN, ou mesmo regionais, WMAN (OLIVEIRA; BERNAL, 2013).

O espectro de frequência é um sinal eletromagnético propagado no espaço por alguns centímetros ou mesmo vários quilômetros. A distância percorrida está diretamente ligada à frequência de emissão do sinal. Portanto, quanto mais alta a frequência, menor será a distância alcançada. De acordo com (RUFINO, 2005), a fórmula geral que define essa proporção é:

$$PS = 32.4 + (20 \log D) + (20 \log F)$$

Onde:
PS = perda do sinal
D = distância em quilômetros
F = frequência em MHz

2.5 CONCLUSÃO

O presente capítulo apresentou os princípios básicos das redes sem fio. Foram descritos os modelos de referência: OSI e TCP/IP, abordando cada uma das camadas previstas e realizando uma breve comparação entre as duas abordagens. Esse estudo é fundamental no desenvolvimento dos próximos capítulos, onde são estudadas as subcamadas definidas para a camada de enlace: subcamada de controle do enlace lógico (LLC) e subcamada de controle do acesso ao meio (MAC)

O capítulo 2 ainda teve por objetivo elucidar a forma de organização dos nós nas redes IEEE 802.11 e IEEE 802.15.4, ou seja, as topologias de rede. Essa conceituação é de grande importância para a construção dos cenários experimentais que o presente trabalho se propõe a realizar. E, por fim, foram apresentadas algumas tecnologias de transmissão de dados sem o uso de cabos, como rádio frequência, laser e infravermelho, abordando seu funcionamento, aplicações, benefícios e limitações.

Para o próximo capítulo, espera-se um aprofundamento nas tecnologias de rede que são avaliadas por este trabalho, detalhando o funcionamento de algumas camadas, subcamadas e protocolos de comunicação. Haverá ainda seções tratando de características e peculiaridades dos padrões IEEE 802.11 e IEEE 802.15.4.

3 - O PADRÃO IEEE 802

O padrão IEEE 802 foi desenvolvido e publicado pelo Comitê 802 da IEEE (*Institute of Electrical and Electronics Engineers*) dos Estados Unidos, com o intuito de adequar o modelo RM/OSI - ISO para o desenvolvimento de redes locais (LANs). Trata-se de uma série de normas para redes metropolitanas (MANs e LANs) que foram adotadas mundialmente, inclusive pela ISO.

A padronização proposta pelo comitê 802 da IEEE é relativa às camadas Física e de Enlace, propostas pelo modelo ISO. Sendo que para a camada de Enlace, o padrão desenvolve mais duas subcamadas: uma voltada ao controle do Enlace Lógico (LLC) e a outra voltada ao controle de acesso ao meio de transmissão (MAC). As normas desse padrão são voltadas a diversos tipos de redes, entre eles: Ethernet, fibra óptica e redes sem fio.

O presente capítulo, primeiramente, apresentará a camada física, abordando as técnicas de multiplexação por divisão de tempo (TDMA) e por divisão de frequência (FDMA) e, posteriormente, a de enlace, onde são apresentadas as subcamadas de controle do enlace lógico (LLC) e de controle do acesso ao meio (MAC), abordando a questão do protocolo CSMA/CA.

Na sequência, descrevem-se algumas características próprias de cada padrão. Primeiramente, o IEEE 802.11(802.15.4A, 2007), abordando peculiaridades de sua organização e serviços integrados que caracterizam o padrão. E em seguida, abordam-se aspectos relacionados ao funcionamento e organização dos dispositivos que operam de acordo com o padrão IEEE 802.15.4 (802.15.4A, 2007).

3.1 CAMADA FÍSICA

A camada mais baixa prevista pelo modelo OSI é a camada física. Metaforicamente, é considerada o alicerce sobre o qual a rede é construída (TANENBAUM; WETHERALL, 2011). Essa camada é responsável pela definição das interfaces elétricas, de sincronização e outras, pelas quais os bits serão enviados, em forma de pulso elétrico, pelos canais de comunicação.

O modelo de camadas do IEEE 802 define apenas os protocolos das camadas física e de enlace, sem fazer nenhuma referência às camadas superiores. Dessa maneira, quem se encarrega da geração do preâmbulo que permite identificar o início do quadro e a sincronização da transmissão é a camada física, além de ser também a responsável pela

codificação e decodificação dos sinais gerados e recebidos nessa transmissão. Basicamente, essa camada responsabiliza-se, pela transmissão e recepção dos dados utilizando um determinado canal de rádio de acordo com alguma modulação ou técnica de difusão.

O padrão IEEE 802.15.4 oferece três frequências de operação ISM: 2,4 GHz, 915 MHz e 868 MHz (SEMPREBOM, 2012). A faixa de 898MHz trabalha com apenas um canal. Já a faixa de 902 e 928MHz (915MHz) possui 10 canais e a faixa 2,4 GHz (de 2,4 a 2,4835 GHz) oferece 16 canais. Na Figura 16 há uma comparação da divisão dos canais em uma rede IEEE 802.15.4 e IEEE 802.11, ambas operando na faixa de 2,4GHz.

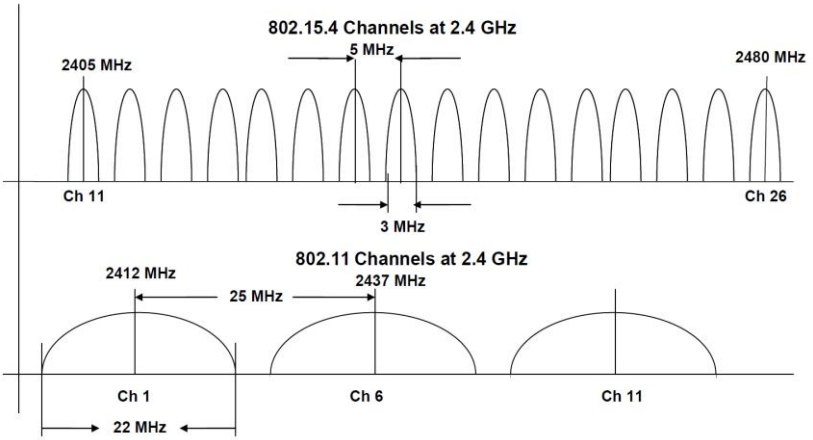

Figura 16: Divisão dos canais - IEEE 802.15.4 e IEEE 802.11.

Para Semprebom (2012) "baixas taxas de transmissão proporcionam melhor sensibilidade à área de cobertura", assim como "altas taxas de transmissão significam alta vazão e baixa latência". Dessa forma, a frequência de 2,4GHz oferece uma taxa de transmissão de dados máxima de 250 kbps, enquanto essa mesma taxa é de 40 Kbps para a frequência de 915MHz e de 20 Kbps para 868 MHz. Contudo, por apresentar menores perdas por atenuação de sinal, as baixas frequências podem ser adequadas para transmissões de longa distância.

Para o padrão IEEE 802.15.4, a camada física é responsável pela execução de 5 tarefas básicas: 1) Ativação e desativação do transceptor de rádio, que opera nos modos : transmitindo, recebendo ou adormecido; 2) Detecção de energia no canal, determinando se o canal está ocioso ou ocupado; 3) LQI (*Link Quality Indication*), que

caracteriza a qualidade do sinal recebido no enlace; 4) CCA (*Clear Channel Assessment*), através da função de detecção de energia reporta que o canal está ocupado caso detecte energia acima de um limiar de energia ou um sinal com as mesmas características de modulação e difusão do IEEE 802.15.4; 5) Seleção da frequência do canal, comando provindo das camadas superiores (SEMPREBOM, 2012).

Ainda, durante a tarefa de transmissão, é função da camada física realizar o escalonamento dos dados que serão transmitidos. Para tanto, existem algumas técnicas já desenvolvidas. Na sequência, serão apresentados os métodos de escalonamento por divisão de tempo (TDMA) e por divisão de frequência (FDMA).

3.1.1 Escalonamento TDMA (*Time Division Multiple Access*)

O escalonamento TDMA está baseado na divisão do tempo de transmissão em redes de meio compartilhado e de múltiplo acesso. Os problemas com interferência no sinal devem ser reduzidos quando se utiliza esse mecanismo (COSTA *et al*., 2011).

O acesso ao meio com o mínimo de colisões, por um conjunto de estações é condicionado pela divisão em intervalos de tempo entre uma transmissão e outra. Mesmo que as estações estejam utilizando o mesmo canal para transmitir, o mecanismo TDMA deve assegurar o acesso livre de colisões (MORAES, R.; VASQUES; PORTUGAL, 2008).

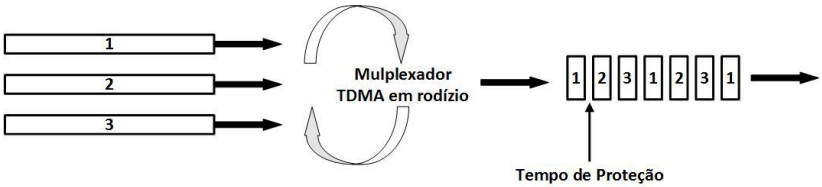

Figura 17: Multiplexação por divisão de canal.

Como pode ser observado na Figura 17, na multiplexação por divisão de canal os bits de cada fluxo de entrada são acompanhados de um *slot* de tempo fixo e enviados para o fluxo agregado. Neste processo, pequenos intervalos podem ser acrescentados entre um *slot* e outro, para acomodar pequenas variações ocasionais de tempo (TANENBAUM; WETHERALL, 2011).

3.1.2 Escalonamento FDMA (*Frequency Division Multiple Access*)

O método FDMA é um mecanismo de escalonamento do acesso ao canal. A divisão de frequência em canais com 30KHz de banda é a principal característica deste método. Dessa maneira, cada usuário tem posse exclusiva de alguma banda de frequência para enviar seu sinal (TANENBAUM; WETHERALL, 2011). A técnica é conhecida como Multiplexação por divisão de frequência, como se pode observar na Figura 18.

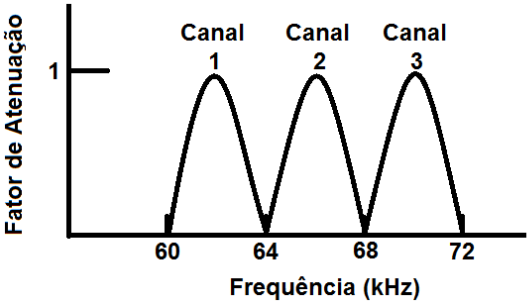

Figura 18: Canais em Multiplexação por divisão de frequência.

O FDMA foi especialmente utilizado pela telefonia celular, pois consegue suportar até três vezes mais conexões do que as tecnologias analógicas que utilizam a mesma quantidade de canais. Isso é possível porque, se tratando de uma tecnologia digital, os dados da comunicação são comprimidos, fazendo com que esta ocupe apenas um terço da capacidade do canal. Com isso, os outros dois terços podem ser aproveitados para outras chamadas (TANENBAUM; WETHERALL, 2011).

3.2 CAMADA DE ENLACE

As redes sem fio são naturalmente redes *broadcast*, ou seja, todas as máquinas recebem o sinal, porém só a máquina definida como destino pode abrir as mensagens (TANENBAUM; WETHERALL, 2011). Neste tipo de rede, a questão principal é determinar quando e quem poderá acessar o canal de transmissão. Para exercer esse controle, duas subcamadas são propostas à camada de enlace: a subcamada de controle do enlace lógico (LLC) e a subcamada de controle do acesso ao meio (MAC), que serão apresentadas na sequência.

3.2.1 Subcamada de Controle do Enlace Lógico (LLC)

No padrão IEEE 802.11(802.15.4A, 2007), que é um tipo de WLAN, a subcamada MAC determina como o canal é alocado, ou seja, quem terá a oportunidade de transmitir os dados no meio físico. Acima dela encontra-se a subcamada LLC (*Logical Link Control*), cujo trabalho é ocultar as diferenças entre as diversas variações do padrão IEEE 802 e torná-las indistinguíveis no que se refere à camada de rede. A LLC especifica os mecanismos para endereçamento de estações conectadas ao meio e para controlar a troca de dados entre usuários da rede.

Mais precisamente, o padrão IEEE 802.3 (802.3, 1985) é que define a camada LLC para toda família de redes IEEE 802. O padrão estabelece três tipos de serviço para a subcamada LLC: 1) sem conexão e sem reconhecimento, onde as unidades de dados são trocadas sem reconhecimento, sem qualquer controle de fluxo ou recuperação de erro; 2) com conexão, onde as máquinas origem e destino estabelecem uma conexão antes que quaisquer dados sejam transferidos; e 3) com reconhecimento e sem conexão, onde cabe ao receptor acusar o recebimento dos quadros que chegam corretamente.

Considerando a abordagem que o presente trabalho se propõe a desenvolver, é importante apenas a compreensão de que a subcamada LLC é responsável pela implementação de uma interface entre as camadas de enlace e de rede. Nesse processo fornece serviços de multiplexação e controle de erros e de fluxo.

3.2.2 Subcamada de Controle do Acesso ao Meio (MAC)

Quando da utilização de um meio compartilhado, a questão é sempre buscar realizar um uso ordenado e eficiente deste meio. Para tanto, existe a função de controle de acesso ao meio, também conhecida como subcamada MAC, que permite o compartilhamento da capacidade de transmissão de uma rede entre todos os dispositivos.

A subcamada MAC é parte da camada de Enlace definido pelo padrão OSI (TANENBAUM; WETHERALL, 2011). Essa subcamada, responsável pelo controle do acesso ao meio, divide-se, basicamente, em algumas funções coordenativas. Especificamente para o padrão IEEE 802.11, que padroniza a camada de enlace, são definidas as seguintes funções: *Distributed Coordination Function* (DCF), *Point Coordination Function* (PCF), *Hybrid Coordination Function* (HCF) e Mesh Coordination Function (MCF) (802.11U, 2011), que serão estudadas na

sequência. A Figura 19 ilustra de forma simples o comportamento das camadas em um modelo de comunicação.

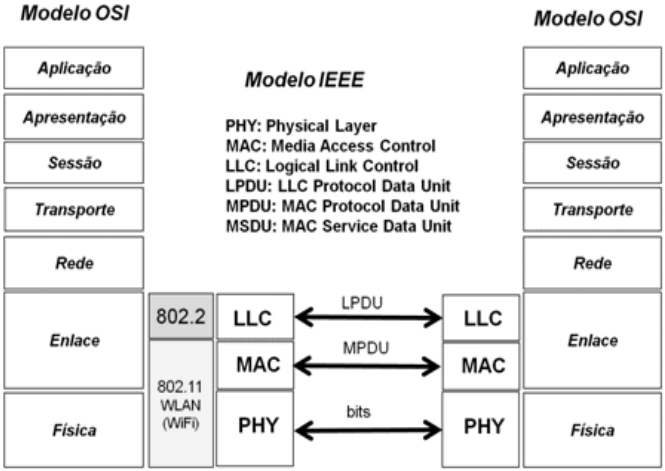

Figura 19: Relação do modelo OSI e Subcamadas.

Das funções coordenativas relacionadas à camada MAC, a que desempenha o serviço mais fundamental é o DCF (802.11, 2007), que pode ser observado na Figura 20. Este método é implementado em todas as estações que operam no padrão IEEE 802.11 para que seja possível a utilização do protocolo CSMA/CA. Esta função determina que para não haver colisões o meio precisa estar vago antes do início de uma transmissão. Por isso, antes de iniciar a transmissão, a estação precisa ouvir o meio e verificar se o mesmo ainda não está sendo utilizado e só poderá transmitir quando tiver certeza que ninguém mais está a requisitar o meio (RUFINO, 2005).

Outra função coordenativa da camada MAC é o PCF (802.11, 2007), que só é utilizado na configuração de redes infraestruturadas. Como será visto na seção 3.3, as redes 802.11 operam organizadas em Conjuntos de Serviços Básicos (BSS) coordenados por um *Access Point* (AP). A PCF atua no AP do BSS com a função de determinar qual estação tem, no momento, o direito de utilizar o meio para sua transmissão. A PCF é construída sobre a DCF e explora seus recursos para garantir acesso aos usuários, como se pode ver na Figura 20. Apesar desta função ter sido inserida nas primeiras versões do padrão IEEE 802.11, não há dispositivos que a implementem devido, principalmente, a sua complexidade (PELLEGRINI et al., 2006).

A partir das alterações realizadas pelo padrão IEEE 802.11 , foi definida uma associação entre a DCF e a PCF, determinando uma nova função de coordenação, a HCF, que é usada apenas em configurações de rede com QoS (MARTINCOSKI, 2003). O HCF atribui a cada estação uma oportunidade (TXOP) de acesso ao meio de transmissão. Cada TXOP é definida por um momento de início e um período de duração máxima que será atribuído por um dos mecanismos de acesso especificados pelo HCF:

- HCCA (HCF *Controlled Channel Access* – Acesso ao Canal Controlado HCF), que permite a reserva de TXOPs junto ao coordenador híbrido. Baseia-se nas especificações dos tráfegos admitidos para prover o serviço de escalonamento de pacotes;

- EDCA (*Enhanced Distributed Channel Access* – Acesso ao Canal DCF Aprimorado), realiza a diferenciação de prioridade de acesso ao meio através de variação da quantidade de tempo que uma estação escuta o meio livre antes do *backoff* ou da transmissão, através do tamanho da janela de contenção a ser usada no *backoff* e através da duração da transmissão de uma estação após obter o meio.

Os dois métodos apresentados definem as classes do tráfego, priorizando os fluxos de maior interesse (ANDRIGHETTO, 2008).

A última das funções de coordenação da subcamada MAC a ser abordada é a função coordenativa Mesh (MCF) (802.11U, 2011). Essa função é usada apenas em redes *mesh*, ou seja, redes que se organizam em malha. A MCF utiliza mecanismo de contenção de acesso ao meio baseado no mecanismo EDCA.

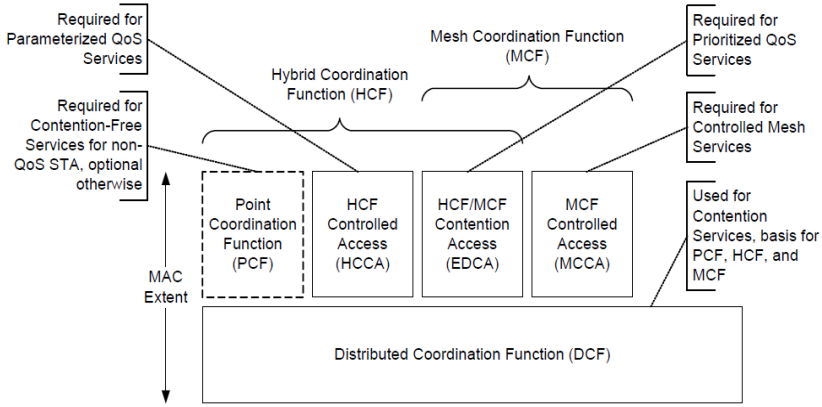

Figura 20: Funções coordenativas da subcamada MAC.

O padrão IEEE 802.11 prevê um mecanismo inteligente, baseado em intervalos de tempo (IFS) que fornece QoS às redes deste padrão. Ele opera estendendo o CSMA/CA com intervalos cuidadosamente definidos entre os quadros. Para Tanenbaum e Wetherall (2011) "o truque está em definir diferentes intervalos para diferentes tipos de quadros".

Os IFS (*Interframe Space*) (802.11, 2007) são divididos em seis períodos de tempo padrão, usados pela função CS (*Carrier Sense*) para designar níveis de prioridade no uso da portadora para transmissão. Essas seis padronizações recebem as seguintes nomenclaturas: SIFS (*Short Interframe Space*), PIFS (*PCF Interframe Space*), DIFS (*DCF Interframe Space*), AIFS (*Arbitration Interframe Space*) e EIFS (*Extended Interframe Space*). Alguns desses intervalos podem ser visualizados na Figura 21. Há ainda o intervalo RIFS, cuja a utilização é defini em no Anexo I.

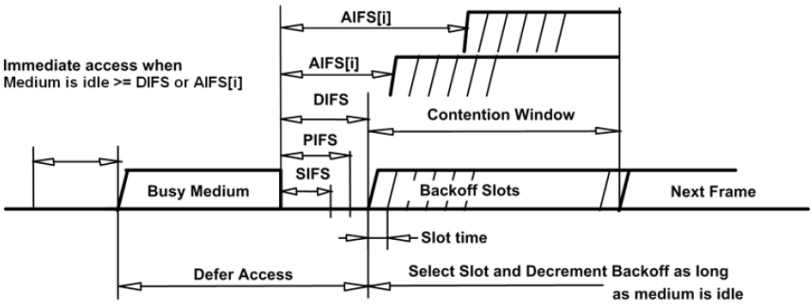

Figura 21: Intervalos de tempo da função *Carrier Sense.*

O intervalo SIFS (802.11, 2007) é o mais curto dos intervalos predefinidos pelo padrão, sendo, portanto, usado no provimento de serviços de maior relevância e com prioridade mais alta. O espaçamento SIFS, por exemplo, é inserido antes e depois do envio das seguintes mensagens: RTS (*Request to Send*), CTS (*Clear to Send*) e também antes e depois do envio de mensagens de ACK (FRANÇA, 1997). A Figura 22 demonstra a utilização de espaçamento SIFS em uma troca de mensagens e dados entre duas máquinas.

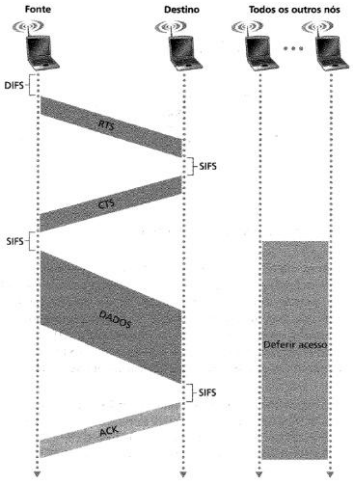

Figura 22: Exemplo de espaçamento em troca de mensagens.

É importante compreender que o SIFS fornece o mais alto nível de prioridade em uma rede sem fio. Isso acontece porque todas as estações devem ouvir o meio, aguardando que o mesmo permaneça ocioso durante este intervalo de tempo. Uma vez obtida a certeza da disponibilidade do meio, a estação que quer transmitir, espera uma quantidade de tempo (espaçamento) antes de realizar a transmissão. Esse tempo de espera é determinado pela tarefa que a estação precisa executar. Para cada tarefa em uma rede WLAN existe uma categoria de espaçamento. Tarefas com alta prioridade pertencerão à categoria de espaçamento SIFS. Se uma estação tem a necessidade de esperar por uma pequena quantidade de tempo antes do meio estar livre para fazer transmissões, ela terá prioridade maior sobre as estações que precisam esperar um período de tempo maior.

Ao tratar do intervalo PIFS (*PCF Inter Frame Space*) (802.11, 2007) é necessário a clareza de que a PCF é uma função opcional suportada pela DCF, onde se é oferecido um mecanismo com serviços livres de contenções. O PCF controla os quadros durante o período livre de contenção (CFP - *Contention Free Period*), que é seguido por um período de contenção controlado pelo mecanismo DCF, anteriormente descrito. Nessa lógica, o coordenador PC (*Point Coordination*) obtém o controle de CFP e tenta manter este controle por todo o período, já que uma estação no modo PCF aguarda um tempo menor para transmitir seus pacotes do que uma estação utilizando DCF. Para tanto, é necessário um intervalo de tempo um pouco menor que DIFS, porém

maior que SIFS. Por isso, no início de cada CFP o PC informa, após esperar um tempo PIFS, qual o tempo total de CFP e quando ocorrerá novamente, através de um pacote denominado *beacon frame*.

A descrição do padrão IEEE 802.11 de 29 de março de 2012, define algumas normas para a utilização do espaçamento PIFS. O documento determina que o referido intervalo não pode ser utilizado de outro modo, a não ser tal como descrito na lista abaixo:

- "Em estações que operam sobre a PCF;
- Em estações que transmitam quadros *Channel Switch Announcement*;
- Em estação que transmitam quadros TIM (*Traffic Indication Map*);
- Em Coordenadores Híbridos que iniciem períodos CFP ou TXOP;
- Em Coordenadores Híbridos ou estações AP sem QoS, que sejam portadoras de TXOP (*Transmission Opportunity*) recuperados da ausência de uma recepção esperada em uma CAP (*Controlled Access Phase*);
- Em estações HT (*High Throughput*), que utilizam dupla proteção CTS (*Clear To Send*) antes de uma transmissão CTS2;
- Em estações que detém a TXOP e devem continuar a transmitir após falha de transmissão;
- Em estações que iniciem um RD (*Reverse Direction*) e continuem a transmitir utilizando a recuperação de erros;
- Em APs HT que durante uma sequencia PSMP (*Power Save Multi-Poll*) tenha que transmitir um quadro de recuperação PSMP;
- Em estações HT que realizem CCA (*Clear Channel Assessment*) em canal secundário antes de transmitir máscara PPDU (PLCP - [*Physical Layer Convergence Procedure] Protocol Data Unit*) a 40MHz, utilizando o canal de acesso EDCA."

3.2.2.1 Protocolo CSMA/CA

O protocolo de acesso ao meio, CSMA/CA, é utilizado pela subcamada MAC que, no padrão IEEE 802.15.4, provê uma interface entre a camada Física e as camadas superiores das LR-WPAN's (*Low-Rates – Wireless Personal Network*). Há em comum entre as redes IEEE 802.15.4 e as redes IEEE 802.11 o fato de utilizarem o mesmo protocolo de acesso ao meio, o CSMA/CA (*Carrier Sense Multiple Access* com o método *Collision Avoidance*). O protocolo aplicado no padrão IEEE 802.15.4 está adaptado às necessidades das LR-WPAN's, eliminando as mensagens de *Request to Send* (RTS) e *Clear to Send* (CTS) que, no padrão IEEE 802.11, são utilizadas para redução da probabilidade de colisão (veja Figura 23), mas que são muito

dispendiosas no que se refere ao consumo de energia relativo a cada envio deste tipo de mensagem (SEMPREBOM, 2012).

Na Figura 23 pode-se observar o cenário onde a estação A envia um RTS para B, solicitando autorização de envio. A máquina B, por sua vez, direciona a todas as máquinas que conhecem uma mensagem CTS, isso garante que outras estações não transmitam dados a B ao mesmo tempo em que ocorre a transmissão de A. Os dados são enviados de A para B e ao final a estação B envia um sinal de ACK, informando que a transmissão obteve sucesso.

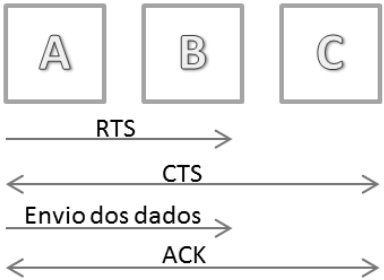

Figura 23: Transmissão com CSMA/CA.

O meio de comunicação entre redes sem fio é sempre o ar, portanto, um enlace compartilhado e de múltiplo acesso. Nesses casos, o principal problema é a melhor definição de quem irá transmitir, quando o fará e quando deverá aguardar. Com a transmissão simultânea em um meio compartilhado, vários nodos podem transmitir quadros ao mesmo tempo, e estes podem colidir entre si, ou mesmo se perderem . Os protocolos utilizados para organizar enlaces de acesso múltiplo permitem coordenar o acesso ao meio, podendo detectar e evitar algumas falhas. Em redes cabeadas (Ethernet), o protocolo utilizado é o *Carrier Sense Multiple Access* (CSMA), que se baseia no princípio de "ouvir" a portadora antes de iniciar a transmissão (MORAES, R.; VASQUES; PORTUGAL, 2010).

Em se tratando do estudo do protocolo CSMA é importante recordar seu funcionamento em redes cabeadas. Onde, antes de iniciar qualquer tipo de transmissão, determina-se se a portadora (cabo) está ou não ocupada. Verificado o cenário de canal livre, o nodo inicia imediatamente sua transmissão; caso ocorra o inverso, o caso de o canal estar ocupado, o nodo aguarda um tempo aleatório e volta a verificar a disponibilidade do canal para tentar uma retransmissão. Para prevenir colisões existe ainda o método *Collision Detection* (CD), onde os nodos

continuam a ouvir o canal enquanto transmitem. Este procedimento permite que haja detecções dos casos de sobreposição ou colisão de dados. Verificado um cenário onde há mais de um nodo transmitindo, todas as transmissões são imediatamente abortadas.

No caso das redes sem fio, os dispositivos desligam seus transceptores enquanto transmitem, tornando inviável a possibilidade de os nodos "ouvirem" o canal ao mesmo tempo em que transmitem e, portanto, impossibilitando a detecção das colisões. Desta forma, as redes sem fio tendem a evitar as colisões, por meio do método *Collision Avoidance* (CA). Este método, basicamente, produz períodos de *backoff* aleatórios antes de verificar a disponibilidade do meio, ao invés de continuar escutando o meio até que o mesmo esteja livre. Esta operação é crucial para o bom funcionamento de uma rede sem fio, pois garante uma alta economia de energia, fator fundamental para o padrão IEEE 802.15.4.

Existem duas versões para o protocolo CSMA/CA definidas apenas para o padrão IEEE 802.15.4: CSMA/CA com compartimento e CSMA/CA sem compartimento. A versão com compartimentos é utilizada quando o CSMA/CA usa, em sua organização, intervalos de *beacon*. Já a versão sem compartimentos ocorre quando o protocolo é utilizado no modo sem *beacon*. Os dois casos utilizam, para sincronização, intervalos de *backoff* onde o período é igual aUnitBackoffPeriod = 20 símbolos (SEMPREBOM, 2012).

As redes sem fio IEEE 802.11 e IEEE 802.15.4 utilizam a banda ISM (Industrial, Scientific, Medical) que tem espectro reservado entre as frequências de 2.400GHz e 2.497GHz e é subdividido em 11 canais, onde cada um deles se utiliza de uma banda de ~25MHz que varia entre três estágios de frequência: Inicial, Média e Final. Isso significa que a sobreposição de canal pode ocorrer mesmo quando dois transmissores estão utilizando canais de transmissão distintos. Apesar do problema da sobreposição de canais em uma transmissão não impossibilitar totalmente a comunicação entre dois pontos, no que trata da transferência de dados, a eficiência pode ser reduzida significativamente.

3.3 O PADRÃO IEEE 802.11

Esta seção tem como objetivo apresentar uma revisão dos serviços e arquiteturas padronizados pelo IEEE no que se refere ao estudo, aplicação e utilização de redes sem fio 802.11 para prover a comunicação entre pontos de uma rede de computadores.

Em uma transmissão sem fio deve-se considerar que o meio é compartilhado, ou seja, há disputa pela sua utilização. A menor unidade de uma LAN sem fio é o conjunto de serviços básicos (BSS), que consiste em algumas estações que executam o mesmo protocolo MAC e competem pelo mesmo meio sem fio compartilhado (VILELA, 2013). Para ter acesso a um sistema de distribuição de backbone (DS), a estação precisa estar conectada a um Ponto de Acesso(AP) que tenha acesso ao sistema. Caso contrário o BSS será uma célula isolada. Um comutador, uma rede cabeada ou uma rede sem fio, pode caracterizar um DS.

A Figura 24 representa a configuração mais simples de um conjunto de serviços estendido, onde cada estação pertence a um único BSS. Porém, é possível que dois, ou mais, BSS's se sobreponham geograficamente, assim uma única estação poderia pertencer a mais que um BSS. Um conjunto de Serviços Estendido (ESS) nada mais é que um ou mais BSS's interconectados por meio de um Sistema de Distribuição. Em nível de controle de enlace, o ESS representa apenas uma única LAN lógica.

O ponto de acesso (AP) trabalha como uma interface entre o BSS e o Sistema de Distribuição, fornecendo, além do acesso, os serviços do DS e podendo atuar também como uma estação. Considerando que um Sistema de Distribuição fornece integração de redes tradicionais com fio e redes IEEE 802.11 faz-se necessário a presença de um portal, que pode ser implementado em um dispositivo como uma ponte ou roteador, que é a parte de LAN com fio que é conectada ao DS (VILELA, 2013).

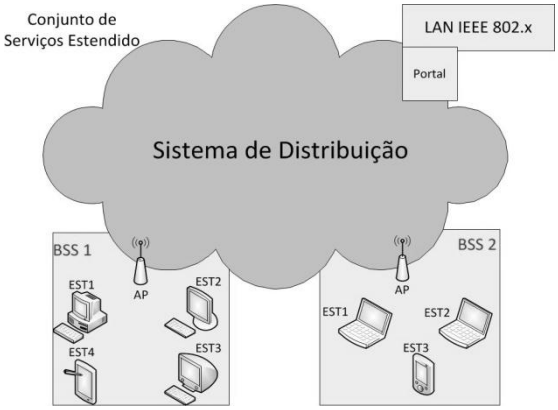

Figura 24: Conjunto de Serviços IEEE 802.11.

Os diversos serviços definidos pelo padrão IEEE 802.11 que precisam ser fornecidos pela LAN sem fio, têm como objetivo prover funcionalidades equivalentes às que são inerentes às LANs com fio. Os serviços considerados mais importantes e básicos para o bom funcionamento de uma WLAN são cinco: associação, re-associação, dissociação, autenticação e privacidade (TANENBAUM; WETHERALL, 2011), que serão abordados a seguir.

Antes de transmitir ou receber quadros em uma LAN sem fio, uma estação precisa ter sua identidade e seu endereço conhecidos. Com esse objetivo, a estação estabelece uma Associação com o AP, que pode então comunicar essas informações aos outros Pontos de Acesso, facilitando, assim, o roteamento e a entrega de quadros endereçados à referida estação. Basicamente, o serviço de associação pretende associar uma estação a um AP.

Para garantir a mobilidade das estações, o padrão IEEE 802.11 estabelece o serviço de Re-associação, que deve ser capaz de viabilizar que uma associação já estabelecida possa transferir-se de um ponto de acesso a outro. No caso da figura 01, o AP está representado por uma antena, mas os pontos de acesso também podem ser conhecidos por estações-base, ou seja, qualquer estação capaz de prover um serviço de comunicação entre as estações de um mesmo BSS e dessas com estações que não pertencem ao seu conjunto de serviços básicos podem ser APs.

Quando uma estação precisa ser desligada ou retirada da área de alcance do AP a que está associada, é necessário que um sinal de Dissociação seja emitido. Uma notificação de dissociação pode ser emitida também pelo ponto de acesso, para definir que uma associação existente até então, será encerrada. Entretanto, existem maneiras do recurso de gerenciamento do MAC se proteger contra estações que desaparecem sem notificação prévia.

Um dos critérios básicos para que se estabeleça a comunicação entre dois pontos é a identificação e a autorização mútua. No caso das redes cabeadas, considera-se a conexão física como uma autorização para conectar-se à LAN. Isso não acontece com redes sem fio pelo fato de que a conectividade poderia ser obtida simplesmente com uma antena corretamente sintonizada. Para isso, um dos serviços definidos no padrão de rede sem fio IEEE 802.11 é o serviço de Autenticação, que é usado para estabelecer a identidade das estações uma para outra. O padrão, em si, não exige um esquema de autenticação específico, por isso esse serviço pode variar de "*handshaking*" até esquemas de criptografias de chaves públicas (VILELA, 2013).

O último, mas não menos importante, é o serviço de Privacidade que objetiva impedir que os conteúdos das mensagens possam ser vistos por estações diferentes da estação destinatária. Uma sugestão feita pela padronização é a opção do uso de criptografia na troca de mensagem, para melhorar o controle da privacidade.

3.4 O PADRÃO IEEE 802.15.4

A seção 15.4 da padronização sugerida pela IEEE 802 refere-se às normas relativas à utilização de *Wireless Personal Area Network* - WPANs, ou seja, redes pessoais de curto alcance.

Atualmente, vem tornando-se cada vez mais comum o uso de dispositivos sem fio de curto alcance nos mais variados ambientes: escritórios, salas comerciais, lanchonetes, etc. São celulares com Bluetooth (IEEE 802.15.1), computadores e radiotransmissores com WiFi (IEEE 802.11) e mesmo rede de sensores que podem intercomunicar-se através do uso da tecnologia ZigBee (IEEE 802.15.4), tudo isso pode, facilmente, ser encontrado operando em um mesmo ambiente.

No caso apresentado, os padrões: Bluetooth e ZigBee representam as tecnologias de curto alcance, porém, pertencem a padronizações distintas na IEEE. Isso porque o padrão IEEE 802.15.4 especifica normas para redes pessoais de baixa taxa de transmissão, as LR-WPANs.

As LR-WPANs caracterizam-se principalmente por terem um curto alcance e por trabalharem com um volume pequeno de dados, além, é claro, das baixas taxas de transmissão. Essas características tornam a tecnologia muito difundida para o uso no controle de equipamentos eletrônicos, como se pode observar na figura 06.

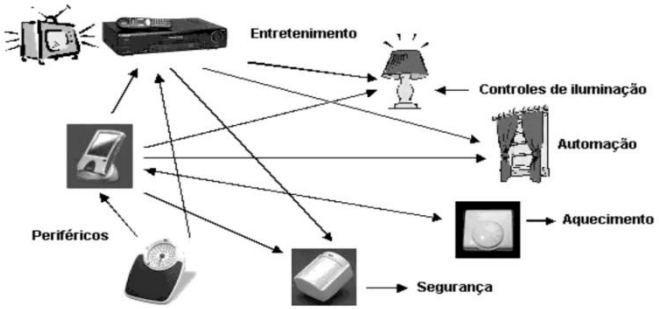

Figura 25: Aplicações padrão IEEE 802.15.4.

Uma rede de sensores sem fio (RSSF) típica consiste em um conjunto de nodo sensores dispostos em uma determinado ambiente a ser monitorado e controlado (SEMPREBOM, 2012). Assim, a possibilidade de coexistir um conjunto heterogêneo de nodos, onde alguns desenvolvem funções não integradas aos outros, é uma característica dessas redes. Dessa maneira, os nós da rede podem possuir diferentes conjuntos de recursos e suportar múltiplos tipos de tráfego, incluindo dados periódicos, intermitentes e de tempo real.

Existem dois tipos básicos de dispositivos que podem operar em uma WPAN: Dispositivo de Função Completa (FDD) e Dispositivo de Função Reduzida (RFD)(SEMPREBOM, 2012).

Um FDD pode suportar três modos diferentes de operação: como dispositivo simples de uma WPAN; como coordenador local (no caso da topologia de agrupamento em árvore), podendo transmitir sinais de beacon, mas sempre associado a um coordenado PAN; e como coordenador PAN, onde pode criar e controlar uma WPAN. Já um RFD só pode operar no modo de dispositivo simples.

3.5 CONCLUSÃO

O presente capítulo apresentou aspectos relacionados às proposições do comitê 802 da IEEE. Entre eles o funcionamento da camada física prevista para essa padronização, bem como a relação da camada de enlace de dados com as subcamadas de controle do enlace lógico e, principalmente, a subcamada de controle do acesso ao meio, especificando as funcionalidades do protocolo CSMA/CA.

O capítulo 3 objetivou, ainda, conceituar individualmente as padronizações IEEE 802.11 e IEEE 802.15.4, que são o foco do presente trabalho, abordando as peculiaridades relativas a cada padrão.

O próximo capítulo terá o objetivo de descrever os cenários experimentais onde serão desenvolvidas simulações de interferências na comunicação das redes sem fio supracitadas. Além de apresentar os resultados e conclusões com base nos dados obtidos com os experimentos.

4 – DESCRIÇÃO DOS CENÁRIOS E RESULTADOS

O principal objetivo deste capítulo é avaliar experimentalmente as interferências na comunicação entre redes IEEE 802.11 e IEEE 802.15.4, operando em uma mesma área de cobertura. Inicialmente, os cenários analisados serão detalhados destacando-se que os mesmos foram, preliminarmente, descritos no capítulo 1 (Metodologia). Então, detalham-se as implementações realizadas nos nodos IEEE 802.15.4, as métricas avaliadas, os experimentos e, por fim, discutem-se os resultados.

Alguns efeitos podem ser observados quando ocorrem interferências em transmissões sem fio. A perda de pacotes e a diminuição nas taxas de transmissão são os mais comuns, fazendo com que as estações transmitam com maior dificuldade.

Os resultados apresentados neste capítulo são avaliados com base na taxa média de perdas de pacotes e na taxa média de envio. A taxa média de perdas de pacotes é dada pela razão entre a taxa de envio efetiva e a taxa de envio desejada.

A construção do cenário experimental ocorreu em duas etapas: a primeira voltada à análise do desempenho dos dois padrões em separado; a segunda etapa consiste na coleta dos dados com as duas tecnologias de rede sem fio operando em conjunto, com algumas variações nos canais de comunicação.

Para cada teste foram executados 10 experimentos de 60 segundos, dessa maneira, este capítulo apresenta os resultados referentes às médias desses experimentos.

4.1 DESCRIÇÃO DOS CENÁRIOS

Conforme especificado no capítulo 1, os cenários analisados consistem na coexistência de dispositivos IEEE 802.11 e IEEE 802.15.4 na mesma área de cobertura.

Para avaliar a comunicação dos dispositivos IEEE 802.11 (WiFi), construiu-se uma plataforma de testes composta por 5 estações WiFi e *Access Points* (APs) operando no modo infraestruturado. Já para avaliar a comunicação dos dispositivos IEEE 802.15.4 (ZigBee), uma plataforma de testes composta por 7 nodos conectados a um nodo coordenador foi desenvolvida.

Nas seções a seguir são descritos detalhadamente os cenários e os resultados obtidos.

4.2 CENÁRIO 1

Um primeiro experimento foi realizado com 4 estações WiFi enviando dados para uma estação denominada servidor. Estas estações operam em modo infraestruturado e estão conectadas através de um roteador sem fio Cisco WRVS4400N. A rede opera utilizando as configurações padrão definidas no IEEE 802.11g (802.11G, 2003). A Figura 26 ilustra o cenário construído e utilizado.

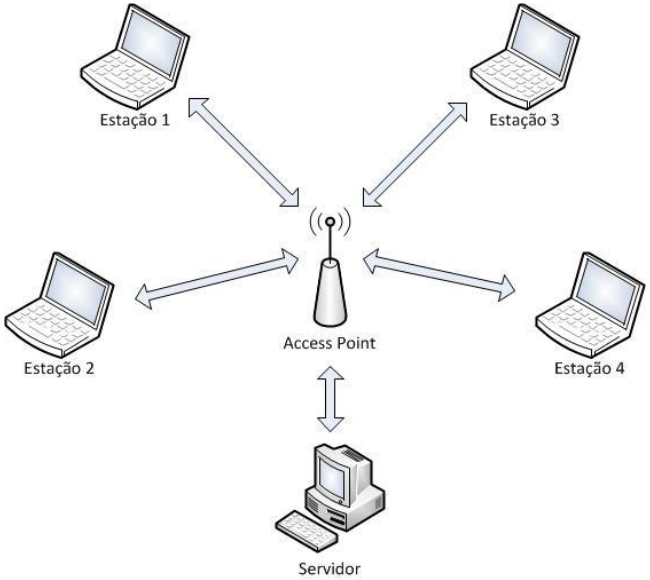

Figura 26 - Cenário WiFi.

As estações 1, 2, 3 e 4 enviam pacotes com tamanho 1500 bytes de dados para o servidor, através de uma conexão UDP. Cada estação envia 200 pacotes/segundo. Portanto, considerando os 20 bytes de cabeçalho envolvidos no envio dos dados, cada quadro transmitido tem um total de 1520 bytes. Dessa forma, as quatro estações enviam a uma taxa de 5,4 Mbps, o que corresponde à utilização de 40% da largura máxima teórica deste tipo de rede, que é de 54Mbps. É importante ressaltar que 40% é uma taxa de utilização consideravelmente alta, pois o ponto de saturação de uma rede IEEE 802.11 é aproximadamente 60% do *throughput* teórico máximo (BIANCHI, 2000; KAMERMAN; ABEN, 2000).

Para o envio dos dados foi utilizado a ferramenta IPerf[3]. As configurações dos parâmetros supracitados no IPerf podem ser visualizadas na Figura 27.

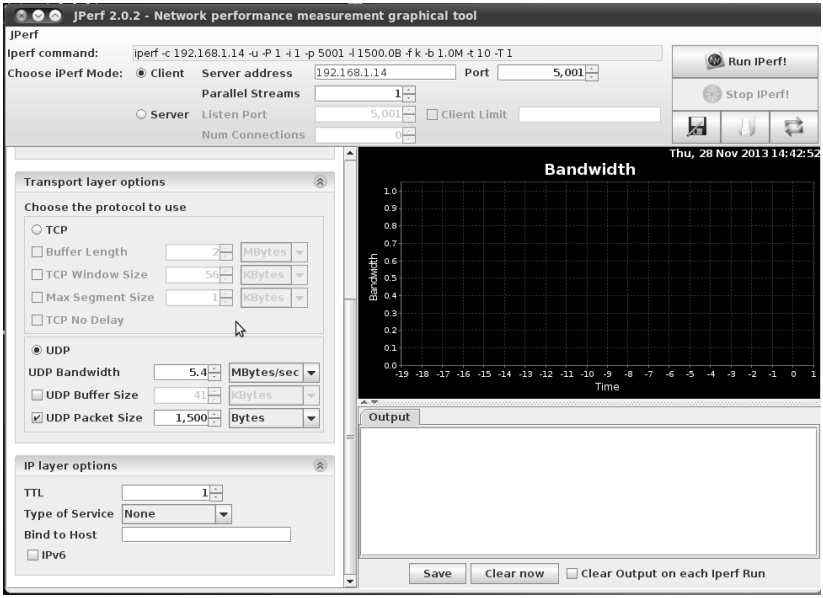

Figura 27 – Configurações do IPerf.

4.2.1 Resultados para o cenário 1

Antes da realização dos testes, foi executada uma varredura no ambiente com o intuito de identificar a existência de outras redes operando na frequência de 2,412GHz, ou seja, no canal 1 das redes WiFi.

Para garantir uma maior confiabilidade nos resultados, cada experimento foi repetido 10 vezes. A Figura 28 demonstra os resultados obtidos em um destes testes, ou seja, quando as estações WiFi operam em um ambiente livre de outras estações/equipamentos a utilizar a mesma frequência de transmissão. Pode-se observar que durante a maior parte do período de execução do teste existiu certa linearidade na variação do atraso na entrega dos dados (*Jitter*), com exceção dos últimos 20 segundos do teste onde podem-se observar variações

[3] Disponível em http://www.iperf.fr/

consideráveis. Porém, essa linearidade não é observada no gráfico que representa a taxa média de transmissão (*Bandwidth*), que atinge alguns picos de transmissão e retorna à normalidade. Isso ocorre devido à disputa pelo acesso ao meio e múltiplas colisões entre as estações.

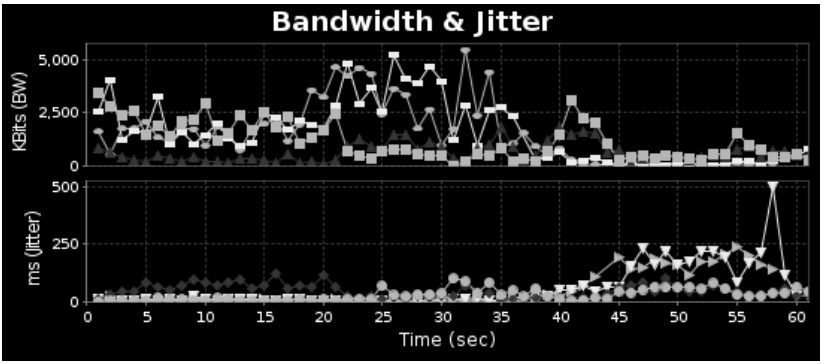

Figura 28 - WiFi operando sem interferências.

No Quadro 2 são apresentados os valores médios para os 10 experimentos onde observa-se que a taxa média de perdas ficou em torno de 32% com um desvio padrão de 20,22%. Portanto, constata-se que há uma alta variação na taxa de perdas de pacotes, mesmo em um ambiente livre de interferências externas. Esta variação é resultante do mecanismo de resolução de colisões do padrão, que é probabilístico.

Métricas	**Médias**
Perdas (%)	32,33
Desvio padrão (%)	20,22
Taxa de transmissão (KBits/s)	1631
Desvio padrão (KBits/s)	203

Quadro 2 - WiFi em ambiente livre de interferências.

4.3 CENÁRIO 2

O segundo experimento foi realizado com os nodos ZigBee operando em um ambiente também livre de interferências. Neste cenário, como demonstra a Figura 29, foram utilizados 7 dispositivos que enviam mensagens com periodicidade de 500ms para o nodo coordenador, o que equivale a uma taxa máxima de envio de 2 mensagens/segundo. Os testes foram realizados nos canais 11, 12, 13, 14

e 15, que equivale a uma faixa de frequência de ~20MHz, repedindo-se o experimento por 10 vezes para cada canal.

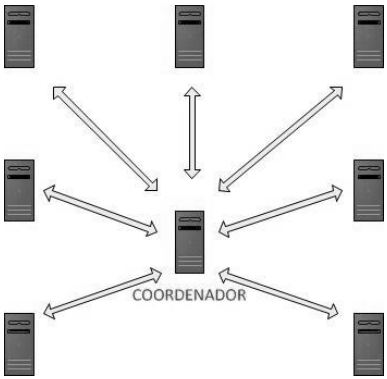

Figura 29 - Cenário ZigBee.

Nessa parte dos experimentos utilizou-se a plataforma MICAz, que pode ser observada na Figura 30. Os nodos são de desenvolvimento da empresa CrossBow[4], possuem um microcontrolador integrado, uma camada física de comunicação sem fio e expansões que permitem uma conexão com sensores mais avançados. Essa plataforma caracteriza-se por utilizar o sistema operacional TinyOS[5], utilizado para sistemas embarcados que possuem pouca capacidade de hardware (seja de memória ou processamento), o que é muito frequente em aplicações de redes de sensores sem fio. A linguagem de programação utilizada por esses dispositivos chama-se NesC, cuja descrição simplificada pode ser entendida como uma versão de C aliada às noções de comandos e eventos.

Figura 30 - Nodo MICAz.

[4] Disponível em http://www.xbow.com/
[5] Disponível em http://www.tinyos.net/

Diferente de outras plataformas, não se tem a pilha de comunicação diretamente implementada pelo sistema operacional, exceto a camada física (PHY). Nesse caso foi utilizada uma implementação de código livre específica para o TinyOS, chamada OpenZB[6], que fornece as pilhas IEEE 802.15.4.

Na composição da mensagem IEEE 802.15.4 foram implementados contadores de mensagens perdidas e enviadas. As mensagens perdidas foram incrementadas ao retorno "MAC_NO_ACK", que corresponde à falha no envio da mensagem. Da mesma maneira, a mensagem "MAC_SUCCESS" corresponde ao incremento no contador de mensagens enviadas com sucesso. Essas mensagens são obtidas através do método “MCPS-DATA” que, por padrão OpenZB, é responsável pela troca de mensagens entre a camada física e a subcamada MAC e pode ser observado na Figura 31. Por conta dessa disposição, um terceiro contador teve de ser implementado para que fosse incrementado nos dois tipos de retorno, resultando no total de tentativas de envio do nodo. O código completo embarcado nas plataformas MICAz, em linguagem NEsC, encontra-se no Anexo II.

```
event result_t MCPS_DATA.confirm(uint8_t msduHandle, uint8_t status)
{
        switch(status)
        {
                case MAC_SUCCESS:
                        mensagens_enviadas++;
                        total_tentativas++;
                        break;
                case MAC_CHANNEL_ACCESS_FAILURE:
                case MAC_NO_ACK:
                        mensagens_perdidas++;
                        total_tentativas++;
                        break;
                default:
                        return SUCCESS;
        }

        return SUCCESS;
}
```

Figura 31 - Método MCPS_DATA.

Para a obtenção dos resultados, durante a execução do experimento foi utilizada a plataforma *sniffer* BUR074190024 operando em conjunto com o software Zena 3.0, ambos desenvolvidos pela

[6] Disponível em http://www.open-zb.net/

Microchip[7]. A captura dos dados ocorre no canal estabelecido, e de acordo com o padrão que foi especificado no software, no caso do presente trabalho, pacotes de padrão IEEE 802.15.4. Como pode-se observar na Figura 32, o Zena 3.0 captura dois tipos básicos de dados: ACK, que corresponde à indicação de envio bem sucedido; e DATA, que contém os valores de perdas e envio, incrementados nas plataformas. Este último relaciona-se diretamente com os objetivos do presente trabalho, por isso será objeto de estudo.

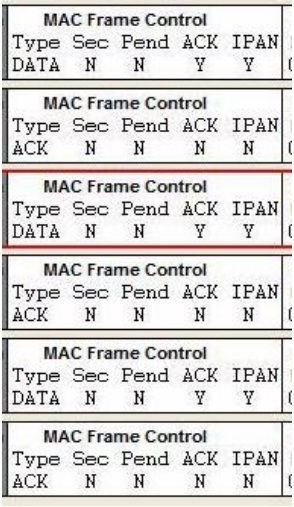

Figura 32 - Retorno *sniffer* Zena.

Após a captura dos pacotes de dados, fez-se necessária a leitura do vetor responsável por guardar os valores dos contadores. Para tanto foi utilizado como base um *script*[8] na linguagem Python[9], com algumas adequações voltadas à análise dos experimentos realizados nesse trabalho. O código do mesmo encontra-se no Anexo III. Em suma, os experimentos para o IEEE 802.15.4 foram realizados com base nos valores do *script* que verifica os pacotes retornados pelo *sniffer* com os dados produzidos pelas plataformas MICAz.

[7] Disponível em http://www.microchip.com/
[8] Desenvolvido no projeto "Uma proposta de infraestrurura Computacional Baseada em Redes de Sensores Sem Fio para o Monitoramento de Intercepção Luminosa em Pastagens", UFSC, 2012-2013.
[9] www.python.org.br

Por fim, destaca-se a necessidade de embarcar o código desenvolvido nos nodos MICAz. Esse procedimento é descrito no Anexo IV.

4.3.1 Resultados para o cenário 2

O Quadro 3 apresenta os resultados médios dos experimentos realizados, ou seja, as médias obtidas na repetição de 10 experimentos para os nodos ZigBee operando nos canais 11, 12, 13, 14 e 15. Observa-se que não houve variações significativas nas taxas de perdas, resultando em percentagem média em torno de 9%. Neste experimento, o envio médio de pacotes também demonstrou poucas variações, sem registrar taxa de envio menor que 62 pacotes por minuto.

Métricas	**Médias**				
	C11	**C12**	**C13**	**C14**	**C15**
Perdas (%)	8,00	10,58	9,07	6,60	10,14
Desvio padrão (%)	2,87	3,79	3,77	2,42	3,85
Taxa de Envio (pkt/min)	71,22	68,44	62,44	67,51	74,51
Desvio padrão (pkt/min)	25,22	23,93	25,36	23,63	36,37

Quadro 3 - ZigBee em ambiente livre de interferências.

4.4 CENÁRIO 3

Este cenário consiste no primeiro teste em que as tecnologias de rede IEEE 802.11 e IEEE 802.15.4 operam conjuntamente. As configurações para cada padrão permanecem as mesmas dos cenários descritos anteriormente (cenários 1 e 2). Portanto, o padrão IEEE 802.11 opera durante todo o experimento no canal 1. Já no caso dos nodos IEEE 802.15.4 os testes foram realizados variando-se os canais de 11 até 15.

4.4.1 Resultados para o Cenário 3

O Quadro 4 apresenta os resultados obtidos pelas estações WiFi quando estas operam no canal 1 conjuntamente com os nodos ZigBee operando nos canais 11, 12, 13, 14 ou 15. Em comparação aos resultados do cenário 1, observa-se que a taxa de transmissão das estações WiFi é menor quando há nodos ZigBee transmitindo dados no canal 11, ou seja, quando as duas tecnologias de rede utilizam a mesma frequência de transmissão.

Métricas	Médias				
	C11	C12	C13	C14	C15
Perdas (%)	31,75	27,05	32,43	29,33	27,14
Desvio padrão (%)	15,94	3,75	6,21	6,82	8,17
Taxa de transmissão (KBits/s)	1526	1917	1756	2029	2000
Desvio padrão (KBits/s)	558	130	125	441	112

Quadro 4 - Resultados para WiFi no cenário 3.

É importante atentar para o número de pacotes enviados em cada teste. Apesar de existirem algumas oscilações, verifica-se um aumento no número total de tentativas bem sucedidas de envio. Além disso, deve-se considerar a diminuição do desvio padrão referente ao envio de pacotes. Pode-se concluir que a transmissão do padrão IEEE 802.11 operando simultaneamente com o padrão IEEE 802.15.4, não sofre alterações significativas no que diz respeito à taxa de envio e de perdas.

Diferentemente do que acontece com a transmissão WiFi, a transmissão dos nodos ZigBee foi altamente prejudicada pela sobreposição de canais, quando em operação simultânea. Observou-se mais de 60% de perdas nas tentativas de envio ao transmitir no canal 11. Além da baixa taxa de pacotes enviados registrada para esse mesmo canal. No Quadro 5 pode-se observar os valores médios obtidos em cada canal.

Métricas	Médias				
	C11	C12	C13	C14	C15
Perdas (%)	60,01	58,11	45,18	17,20	8,79
Desvio padrão (%)	21,24	20,79	25,13	6,17	3,62
Taxa de Envio (pkt/min)	7,31	12,94	48,33	63,66	75,30
Desvio padrão (pkt/min)	5,85	5,17	29,08	30,78	33,94

Quadro 5 - Resultados para ZigBee no cenário 3.

Observa-se também que o canal 15 é o que apresenta as melhores médias, praticamente equiparando-se às médias registradas no cenário 2, quando do seu funcionamento livre de interferências. Isso ocorre por que o IEEE 802.11 realiza sua transmissão utilizando um espectro de frequência que pode ocupar ~22MHz de banda para cada canal. Já o padrão IEEE 802.15.4 opera com espectro máximo de

~3MHz por canal, o que garante a divisão em 15 canais separados por ~5MHz, assim livres de sobreposição.

Considerando que o canal 1 do WiFi corresponde à frequência de ~2,400GHz à ~2,422GHz e os nodos ZigBee dividem essa mesma faixa de frequência em 5 canais distintos, pode-se dizer que o cenário mais apropriado para a operação conjunta das duas padronizações seria o canal 1 e o canal 15 respectivamente.

4.5 CENÁRIO 4

O cenário 4 consiste em experimentos com os dois padrões operando em simultâneo. Neste cenário utilizaram-se duas estações IEEE 802.11 operando no canal 1 e outras duas estações operando no canal 6, observando-se as mesmas configurações de protocolo, tamanho de mensagem e carga na rede mencionados na seção 4.1.1, como demonstra a Figura 33.

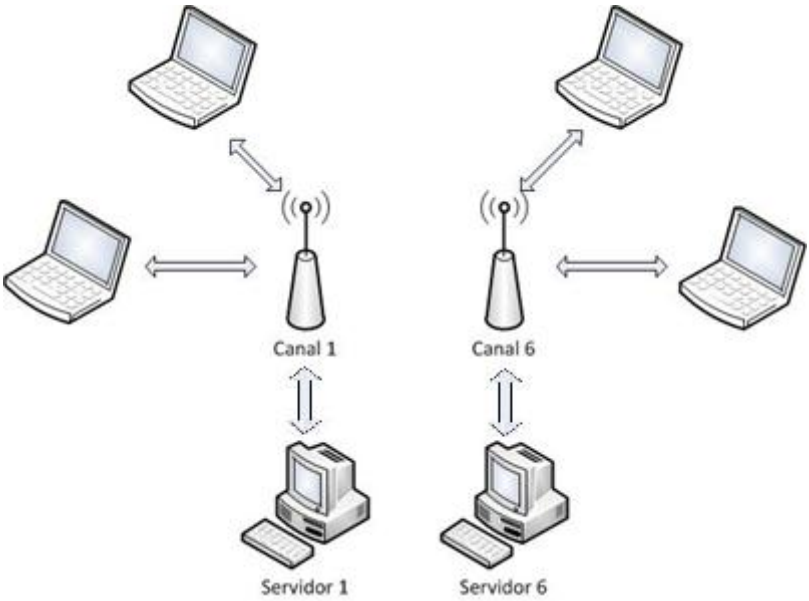

Figura 33 - Cenário 4, WiFi.

Para obter os resultados do padrão IEEE 802.15.4, foi percorrida uma banda de ~40MHz, do canal 11 ao 20. As demais configurações são idênticas às apresentadas na seção 4.3.

4.5.1 Resultados para o cenário 4

As estações IEEE 802.11 que operam no canal 1 apresentam resultados com uma variação quase insignificante, abaixo de 0,03%. Dessa maneira, os melhores resultados para taxa de transmissão podem ser observados a partir do canal 15 do IEEE 802.15.4. O Quadro 6 indica os valores médios apresentados pelo IEEE 802.11 operando no canal 1, simultaneamente ao IEEE 802.15.4 transmitindo do canal 11 ao 15. Os valores referentes à transmissão IEEE 802.15.4 dos canais 16 ao 20, podem ser observados no Quadro 7.

Registrou-se um aumento gradativo das taxa de envio durante as execuções do experimento, bem como uma redução drástica na percentagem de perdas, se comparado aos testes com a WiFi em outros cenários. Isso ocorre por que ao iniciar uma transmissão, as estações acabam por gerar interferências umas às outras. Assim, quanto maior o número de estações em operação simultânea, maior a interferência no sinal e, por consequência, maior o número de colisões e perdas de pacotes. Dessa forma, as estações WiFi praticamente não registram perdas de dados pois há somente duas estações operando em cada canal.

Métricas	**Médias**				
	C11	**C12**	**C13**	**C14**	**C15**
Perdas (%)	0,04	0,02	0,13	0,04	0,01
Desvio padrão (%)	0,03	0,01	0,10	0,05	0,03
Taxa de transmissão (KBits/s)	1602	1670	1301	1586	2713
Desvio padrão (KBits/s)	198	168	234	228	557

Quadro 6 - Resultados para WiFi no canal 1. ZigBee Canal 11 ao 15.

Métricas	**Médias**				
	C16	**C17**	**C18**	**C19**	**C20**
Perdas (%)	0,003	0,001	0,003	0,003	0,001
Desvio padrão (%)	0,003	0,001	0,002	0,003	0,001
Taxa de transmissão (KBits/s)	2927	3159	2834	3014	3119
Desvio padrão (KBits/s)	205	100	145	121	119

Quadro 7 - Resultados para WiFi no canal 1. ZigBee Canal 16 ao 20.

Da mesma maneira, também registrou-se os resultados referentes às estações IEEE 802.11 que operaram no canal 6, que podem ser observados nos Quadro 8 e Quadro 9.

Métricas	Médias				
	C11	C12	C13	C14	C15
Perdas (%)	0,00	0,00	0,00	0,00	0,00
Desvio padrão (%)	0,00	0,00	0,00	0,00	0,00
Taxa de transmissão (KBits/s)	4087	3919	4384	4184	4266
Desvio padrão (KBits/s)	528	203	90	523	153

Quadro 8 - Resultados para WiFi no canal 6. ZigBee Canal 11 ao 15.

Métricas	Médias				
	C16	C17	C18	C19	C20
Perdas (%)	0,002	0,000	0,000	0,000	0,002
Desvio padrão (%)	0,005	0,000	0,000	0,000	0,007
Taxa de transmissão (KBits/s)	4229	4139	4275	4273	4211
Desvio padrão (KBits/s)	180	565	138	156	257

Quadro 9 - Resultados para WiFi no canal 6. ZigBee Canal 16 ao 20.

Observa-se que a taxa média de perdas de pacotes no caso da transmissão WiFi no canal 6 fica muito próxima de zero. Vários fatores podem ser responsáveis por esse efeito. O principal deles é baixa utilização desse canal para outras transmissões, portanto a possibilidade da estação em questão encontrar o meio físico livre pra transmitir é maior.

Para os testes no cenário 4 com o IEEE 802.15.4, registrou-se novamente os melhores resultados quando este opera em canal não sobreposto pelo sinal IEEE 802.11, apresentados no Quadro 10 e no Quadro 11. Assim, os experimentos realizados nos canais 15 e 20 demonstram taxas de envio e perdas semelhantes aos resultados da seção 4.3, alcançando um índice de eficiência de transmissão relativamente maior se comparado aos resultados da operação em canais sobrepostos.

Métricas	Médias				
	C16	C17	C18	C19	C20
Perdas (%)	58,84	41,19	52,82	36,56	6,55
Desvio padrão (%)	17,31	13,85	15,63	16,76	2,31
Taxa de Envio (pkt/min)	35,47	45,20	23,74	20,74	101,09
Desvio padrão (pkt/min)	18,22	78,17	15,29	12,33	47,32

Quadro 10 - Resultados para ZigBee, Canal 11 ao 15.

Métricas	Médias				
	C16	**C17**	**C18**	**C19**	**C20**
Perdas (%)	60,77	66,65	72,13	69,15	9,78
Desvio padrão (%)	30,27	23,43	25,99	24,94	4,80
Taxa de Envio (pkt/min)	57,97	11,34	8,03	8,47	70,40
Desvio padrão (pkt/min)	160,09	5,95	3,38	3,14	10,03

Quadro 11 - Resultados para ZigBee, Canal 16 ao 20.

4.1 CONCLUSÃO

Este capítulo teve o objetivo de verificar experimentalmente os cenários mais eficientes para uma transmissão simultânea entre as padronizações IEEE 802.11 e IEEE 802.15.4. Conforme apresentado na Figura 16, quando o IEEE 802.11 opera nos canais 1, 6 e 11 há, para o IEEE 802.15.4, a possibilidade de transmissão nos canais 15, 20 e 26 que, nesse caso, não são sobrepostos. Isso foi comprovado pelos resultados dos experimentos propostos no presente capítulo.

As médias que refletem uma transmissão mais eficiente do padrão ZigBee podem ser observadas no quadro 3, onde os teste foram realizados em cenário ideal, ou seja, livre de interferências externas. Resultados semelhantes são observados nos testes realizados nos canais 15 e 20 em todos os experimentos em que houve simultaneidade com a transmissão WiFi.

Da mesma maneira, o IEEE 802.11 registrou melhores resultados em operação simultânea com o IEEE 802.15.4 nos canais em que não houve sobreposição. Apesar da menor relevância das interferências registradas, o cenário mais adequado para ambas as padronizações são coincidentes. A sobreposição de canal tem interferência direta e em diferentes níveis, tanto na transmissão IEEE 802.11 quanto na transmissão IEEE 802.15.4, estando a IEEE 802.11 mais favorecida nesse processo.

Portanto, os cenários de operação simultânea onde se observam os melhores resultados, apresentam as estações IEEE 802.11 operando no canais 1 e/ou 6 e os nodo IEEE 802.15.4 nos canais 15 e/ou 20, ou seja, registrou-se os melhores resultados nos testes realizados com os padrões transmitindo simultaneamente em canais não sobrepostos.

5 - CONCLUSÕES

A operação simultânea de tecnologias de redes sem fio em ambientes compartilhado, não só está se tornando cada vez mais comum, como é imprescindível que sejam propostas formas de melhorar a eficiência da comunicação nesse tipo de cenário.

O presente trabalho se propôs a analisar os efeitos da interferência mútua entre os padrões IEEE 802.11 e IEEE 802.15.4, em operação simultânea e no mesmo ambiente de comunicação. Para tanto, constatou-se que as menores taxas de perdas de pacotes, durante uma transmissão em simultâneo, são verificadas nos canais 15 e 20 do IEEE 802.15. O Gráfico 1 ilustra a relação de perdas de pacotes do padrão IEEE 802.15.4 em cada canal e para cada cenário proposto. Dessa maneira é possível concluir que para esse padrão a transmissão em canais não sobrepostos é de especial importância, haja vista o desempenho registrado quando operando em canal sobreposto.

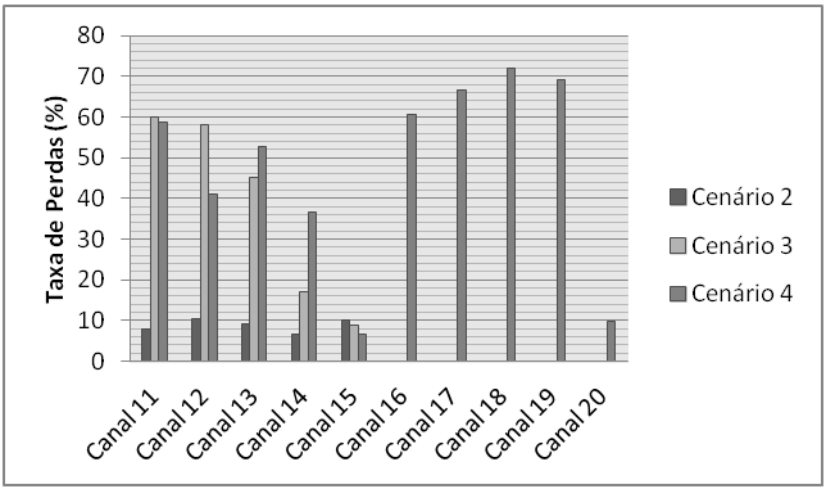

Gráfico 1 - Percentagem de Perdas, IEEE 802.15.4.

Do mesmo modo, verifica-se um aumento considerável nas taxas de sucesso no envio de pacotes quando o padrão IEEE 802.15.4 atua em canal livre de sobreposição. Os melhores resultados podem ser observados nos teste realizados com o Cenário 2, e nos canais 15 e 20 para os demais cenários. Isso indica que a sobreposição de canal não só ocasiona colisões, aumentando o número de pacotes perdidos, como

também afeta a taxa de transmissão. O **Erro! Fonte de referência não encontrada.** apresenta a relação das taxas médias de envio registradas em cada canal, podendo-se comparar os cenários.

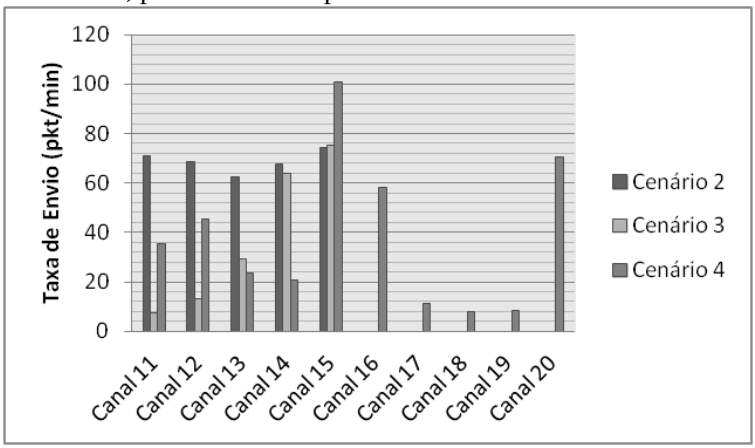

Gráfico 2 - Taxa de Envio, IEEE 802.15.4.

O padrão IEEE 802.11 também apresentou melhores resultados quando operando em canal não sobreposto. Chama-se a atenção para a linha referente ao Cenário 4 - Canal 1, apresentada no **Erro! Fonte de referência não encontrada.**. A curva ascendente significa que o distanciamento da sobreposição do canal é proporcional ao aumento na taxa de transmissão. Assim pode-se concluir que, o IEEE 802.11 também beneficia-se de um cenário livre de sobreposição de canal.

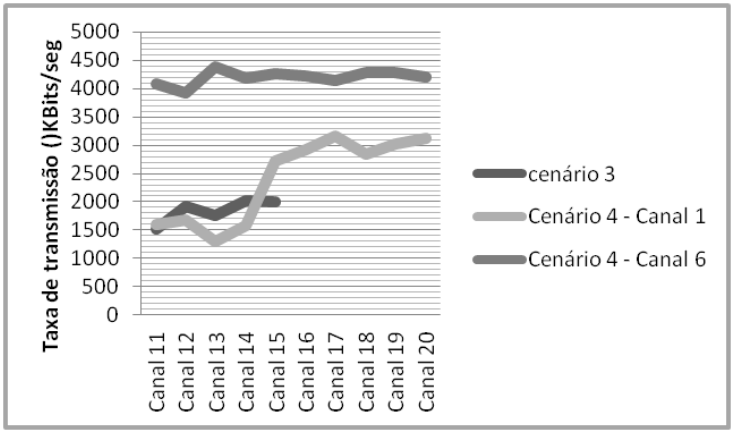

Gráfico 3 - Taxa de transmissão IEEE 802.11.

Portanto, ao final do presente trabalho é possível concluir que a interferência mútua entre padrões IEEE 802.11 e IEEE 802.15.4, não só existe como tem influência direta no desempenho dessas redes. A fonte dessas interferências está na sobreposição dos canais de frequência utilizados na transmissão. Assim, pode-se dizer que o cenário mais adequado tanto para ambas tecnologias deverá ser um ambiente de transmissão livre da sobreposição de canais.

REFERÊNCIAS

802.3, A. I. S. **IEEE standards for local area networks: carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications**. ANSI/IEEE Std 802.3-1985 1985.

802.11, I. S. **IEEE Std 802.11-2007 Information Technology-telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications**. (Revision of IEEE Std 802.11-2003)**:** i-445 p. 2007.

_____. IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. **IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)**, p. 1-2793, 2012.

802.11AF, I. IEEE Draft Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: TV White Spaces Operation. IEEE P802.11af/D5.0, . v. Amendment to IEEE Std 802.11-2012, as amended by IEEE Std 802.11ae-2012, IEEE Std 802.11aa-2012, IEEE Std 802.11ad-2012, and IEEE Std 802.11ac_D5.0, p. p. 1-336, 2013.

802.11B, I. S. IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirement. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 2: Higher-Speed Physical Layer (PHY) Extension in the 2.4 GHz Band - Corrigendum 1. . v. IEEE Std 802.11b-1999/Cor 1-2001, 2001.

802.11G, I. S. IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part Ii: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. **IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001)**, p. i-67, 2003.

802.11N, I. S. IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. IEEE Std 802.11n-2009, . v. Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009, p. p. 1-565,, 2009.

802.11U, I. IEEE Standard for Information Technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking. IEEE Std 802.11s-2011 , . v. Amendment to IEEE Std 802.11-2007 as amended by IEEE 802.11k-2008, IEEE 802.11r-2008, IEEE 802.11y-2008, IEEE 802.11w-2009, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11z-2010, IEEE 802.11v-2011, and IEEE 802.11u-2011, p. p. 1-372, 2011.

802.15.4A, I. S. IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - specific requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). **IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006)**, p. 1-203, 2007.

ANDRIGHETTO, E. **Sistema de processamento de sinais biomédicos: rede wireless zigbee com aplicação do padrão IEEE 802.15.4**. 2008. 147 Mestrado Engenharia Elétrica, Universidade Federal de Santa Catarina.

BIANCHI, G. Performance analysis of the IEEE 802.11 distributed coordination function. **IEEE Journal on Selected Areas in Communications,** v. 18, n. 3, p. 535-547, 2000.

COSTA, R. et al. RT-WiFi: um mecanismo TDMA para suportar comunicações de tempo real em redes IEEE 802.11. XXIX Simpósio Brasileiro de Telecomunicações (SBrT), 2011. Curitiba - Brasil.

DE MORAES, A. F. **Redes sem fio: Instalação, Configuração e Segurança**. 2012. 288.

FRANÇA, G. A. T. **Estudo e especificação de um sistema de telemetria usando a tecnologia Spread Spectrum**. 1997. Engenharia Elétrica, Universidade Estadual de Campinas.

GARCÍA, L. N.; ALONSO, J. I. Novel Method for Interference Analysis in IEEE 802.11 WLAN's in Coexistence with Bluetooth. **Universidad Politécnica de Madrid**, 2009.

KAMERMAN, A.; ABEN, G. Throughput performance of wireless LANs operating at 2.4 and 5 GHz. Personal, Indoor and Mobile Radio Communications, 2000. PIMRC 2000. The 11th IEEE International Symposium on, 2000. 2000. p.190-195 vol.1.

KUROSE, J.; ROSS, K. **Redes de Computadores e Internet**. 2006.

LO BELLO, L.; KACZYNSKI, G. A.; MIRABELLA, O. Improving the real-time behavior of ethernet networks using traffic smoothing. **Industrial Informatics, IEEE Transactions,** v. vol. 1, p. 10, 2005.

MARTINCOSKI, D. H. **Sistema para Telemetria de Eletrocardiograma Utilizando Tecnologia Bluetooth**. 2003. Mestrado Engenharia Elétrica, Universidade Federal de Santa Catarina.

MATHEW, A. IEEE 802.11 & Bluetooth Interference: Simulation and Coexistence. ANNUAL COMMUNICATION NETWORKS AND SERVICES RESEARCH CONFERENCE, 2009. Bridgeport. p.217 - 223.

MORAES, R. et al. Enforcing the timing behavior of real-time stations in legacy bus-based industrial Ethernet networks. **Computer Standards and Interfaces,** v. 33, n. 3, p. 249-261, 2011.

MORAES, R. et al. Assessment of the IEEE 802.11e EDCA Protocol Limitations when Dealing with Real-Time Communication. **EURASIP Journal on Wireless Communications and Networking,** v. 2010, p. 1-14, 2010.

MORAES, R.; VASQUES, F.; PORTUGAL, P. A TDMA-Based Mechanism to Enforce Real-Time Behavior in WiFi Networks. 7th IEEE International Workshop on Factory Communication Systems - WFCS, 2008. Dresden, Germany. p.109-112.

_____. Survey of Real-Time Communication in CSMA-Based Networks. **Network Protocols and Algorithms,** v. 2, n. 1, p. 158-183, 2010.

OLIVEIRA, F. T. X. D.; BERNAL, H. Rádio Spread Spectrum: Técnica de Espalhamento Espectral. 2013. Disponível em: < http://www.teleco.com.br >. Acesso em: Jun 29.

PELLEGRINI, F. D. et al. On the use of wireless networks at low level of factory automation systems. **IEEE Transactions on Industrial Informatics,** v. 2, n. 2, p. 129-143, 2006.

RAMAKRISHNA, G. **Understanding and mitigating the impact of rf interference on 802.11 networks**. Proc. of Sigcomm'07. SIGCOMM 2007.

RUFINO, N. M. D. O. **Segurança em Redes sem Fio: aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**. 2005.

SEMPREBOM, T. **Explorando descartes de ativações periódicas para provimento de qualidade de serviço em redes IEEE 802.15.4**. 2012. Doutorado, Universidade Federal de Santa Catarina.

SHUAIB, K. et al. Co-existence of Zigbee and WLAN: A Performance Study. **Al-ain: College Of Information Technology**, 2005.

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores**. 2011. 584 ISBN 978-85-7605-924-0.

VILELA, D. F. L. **Estudo da Viabilidade de Comunicações Ópticas no Espaço Aberto.** 2013.

ANEXO I - Nota - Reduced Interframe Space (RIFS)

O intervalo RIFS (802.11, 2007) é um meio de aumentar a eficiência da rede reduzindo a sobrecarga de utilização. RIFS pode ser utilizado no lugar do SIFS para separar várias transmissões a partir de um único transmissor, no caso de uma transmissão que não necessite esperar por uma resposta SIFS. O RIFS não pode ser utilizado entre de quadros com valores diferentes no que se trata do campo de endereço da estação receptora. Esse intervalo pode ser considerado o tempo desde o fim do último símbolo do quadro anterior até o início do primeiro símbolo do preâmbulo da estrutura posterior. A estação transmissora que utiliza RIFS, não deve permitir que o espaço entre os quadros que são definidos para serem separadas por um tempo RIFS variem em relação ao valor nominal RIFS (aRIFSTime) para mais do que 10% da aRIFSTime.

ANEXO II - Código NesC embarcado nas plataformas MICAz

```
1   /*
2     Baseado em DataSendExample
3    * @author IPP HURRAY http://www.hurray.isep.ipp.pt/art-
4   wise
5    * @author Andre Cunha
6    * Adaptado por Joao Carlos Cichaczewski, 2013
7    */
8
9   module Implementacao
10  {
11    provides  interface StdControl;
12
13    uses {
14         interface Timer;
15         interface Leds;
16         interface Random;
17
18         interface MLME_START;
19
20         interface MLME_ASSOCIATE;
21         interface MLME_DISASSOCIATE;
22
23         interface MLME_SCAN;
24         interface MLME_RESET;
25
26         interface MLME_SYNC;
27         interface MLME_SYNC_LOSS;
28
29         interface MLME_BEACON_NOTIFY;
30
31         interface MLME_COMM_STATUS;
32
33         interface MLME_SET;
34         interface MLME_GET;
35
36         interface MLME_GTS;
37
38         interface MLME_POLL;
39
40         //MCPS
41
42         interface MCPS_DATA;
43         interface MCPS_PURGE;
44
```

```
45          interface StdControl as Mac_control;
46
47          interface Time;
48
49          interface Timer as Timer_send;
50
51          interface Timer as Timer_conf;
52
53             }
54    }
55    implementation
56    {
57          uint8_t exp_time(uint8_t lambda);
58          uint32_t my_short_address;
59          uint32_t DestinationMote[2];
60
61          //Variáveis de Configuração
62          bool    config_flag;
63
64          //Variáveis do Experimento
65          uint16_t mensagens_enviadas=0;
66          uint16_t mensagens_perdidas=0;
67          uint16_t total_tentativas=0;
68
69          uint8_t i= 0;
70
71    command result_t StdControl.init()
72    {
73          //Destinatário é sempre o COORDENADOR
74          DestinationMote[0]=0;
75          DestinationMote[1]=0;
76
77          //Inicia sem Configuracao
78          config_flag=FALSE;
79
80          return SUCCESS;
81    }
82
83    command result_t StdControl.start()
84    {
85          call Timer.start(TIMER_ONE_SHOT,2000);
86          return SUCCESS;
87    }
88
89    command result_t StdControl.stop()
90    {
91          call Mac_control.stop();
92          return SUCCESS;
```

```
93  }
94
95  //Disparado após o nodo ligar
96  event result_t Timer.fired()
97  {
98        uint8_t v_temp[2];
99
100       if (TYPE == COORDINATOR)
101       {
102             my_short_address= 0x0000;
103
104             v_temp[0] = (uint8_t)(my_short_address >>
105 8);
106             v_temp[1] = (uint8_t)(my_short_address );
107
108             //Cria Rede
109             call
110 MLME_SET.request(MACSHORTADDRESS,v_temp);
111
112             //Inicia o envio de Beacons
113             call MLME_START.request(PANID,
114 LOGICAL_CHANNEL, BEACON_ORDER,
115 SUPERFRAME_ORDER,1,0,0,0,0);
116
117             //Sinaliza Início da Rede
118             call Leds.greenOn();
119
120             //Inicia Timer_conf (para enviar mensagem
121 de configuracao)
122             call
123 Timer_conf.start(TIMER_ONE_SHOT,10000);
124       }
125       else
126       {     //Estabelece conexao com Rede Criada pelo
127 Coordenador
128             my_short_address= TOS_LOCAL_ADDRESS;
129
130             v_temp[0] = (uint8_t)(my_short_address >>
131 8);
132             v_temp[1] = (uint8_t)(my_short_address );
133
134             call
135 MLME_SET.request(MACSHORTADDRESS,v_temp);
136
137             v_temp[0] = (uint8_t)(PANID >> 8);
138             v_temp[1] = (uint8_t)(PANID );
139
140             call MLME_SET.request(MACPANID,v_temp);
```

```
141
142                 //Só inicia o envio de mensagens após a
143     configuração
144         }
145
146         return SUCCESS;
147     }
148
149     //Inicia processo de configuracao dos outros nodos para
150     o experimento
151     event result_t Timer_conf.fired()
152     {
153         uint8_t payload[8];
154         uint32_t SrcAddr[2];
155
156         //Zera vetor
157         payload[0] = (uint8_t) 00;
158         payload[1] = (uint8_t) 00;
159         payload[2] = (uint8_t) 00;
160         payload[3] = (uint8_t) 00;
161         payload[4] = (uint8_t) 00;
162         payload[5] = (uint8_t) 00;
163         payload[6] = (uint8_t) 00;
164         payload[7] = (uint8_t) 00;
165
166         //Remetente
167         SrcAddr[0]=0x00000000;
168         SrcAddr[1]=TOS_LOCAL_ADDRESS;
169
170         //Envia broadcast (todos recebem)
171         DestinationMote[0]=0x00000000;
172         DestinationMote[1]=0xFFFFFFFF;
173
174         //set_txoptions(ack, gts, indirect_transmission,
175     security)
176         call MCPS_DATA.request(SHORT_ADDRESS, PANID,
177     SrcAddr, SHORT_ADDRESS, PANID, DestinationMote, 8,
178     payload,1,set_txoptions(0,0,0,0));
179
180         //Sinaliza Envio de Configuracao
181         call Leds.redOn();
182
183         return SUCCESS;
184     }
185
186     //Envia mensagem para outros nodos
187     event result_t Timer_send.fired()
188     {
```

```
189         uint32_t SrcAddr[2];
190 
191         uint8_t payload[8];
192 
193         if(TYPE == NODO)
194         {
195                 //Primeiros bytes são referentes às
196 variáveis de análise do experimento
197                 payload[0] = (uint8_t) (mensagens_enviadas
198 >> 8);
199                 payload[1] = (uint8_t)
200 (mensagens_enviadas);
201                 payload[2] = (uint8_t) (mensagens_perdidas
202 >> 8);
203                 payload[3] = (uint8_t)
204 (mensagens_perdidas);
205                 payload[4] = (uint8_t) (total_tentativas >>
206 8);
207                 payload[5] = (uint8_t) (total_tentativas);
208 
209                 //O resto dos bytes é randomico
210                 for (i=6;i<8;i++)
211                       payload[i]=call Random.rand()*10;
212 
213         }
214 
215         //Remetente
216         SrcAddr[0]=0;
217         SrcAddr[1]=TOS_LOCAL_ADDRESS;
218 
219         //Transmite Dados
220         call MCPS_DATA.request(SHORT_ADDRESS, PANID,
221 SrcAddr, SHORT_ADDRESS, PANID, DestinationMote,
222 sizeof(payload), payload,1,set_txoptions(1,0,0,0));
223 
224 return SUCCESS;
225 }
226 /*******************MLME  EVENTS*******************/
227 
228 /**********************MLME-GTS**********************/
229 
230 event result_t MLME_GTS.confirm(uint8_t
231 GTSCharacteristics, uint8_t status)
232 {
233         return SUCCESS;
234 }
```

```
235   event result_t MLME_GTS.indication(uint16_t DevAddress,
236   uint8_t GTSCharacteristics, bool SecurityUse, uint8_t
237   ACLEntry)
238   {
239         return SUCCESS;
240   }
241
242   /**********************MLME-START*******************/
243
244   event result_t MLME_START.confirm(uint8_t status)
245   {
246         return SUCCESS;
247   }
248
249   /*******************MLME-ASSOCIATE*****************/
250
251   event result_t MLME_ASSOCIATE.indication(uint32_t
252   DeviceAddress[], uint8_t CapabilityInformation, bool
253   SecurityUse, uint8_t ACLEntry)
254   {
255         return SUCCESS;
256   }
257   event result_t MLME_ASSOCIATE.confirm(uint16_t
258   AssocShortAddress, uint8_t status)
259   {
260         return SUCCESS;
261   }
262
263   /*******************MLME-DISASSOCIATE****************/
264
265   event result_t MLME_DISASSOCIATE.indication(uint32_t
266   DeviceAddress[], uint8_t DisassociateReason, bool
267   SecurityUse, uint8_t ACLEntry)
268   {
269         return SUCCESS;
270   }
271   event result_t MLME_DISASSOCIATE.confirm(uint8_t status)
272   {
273         return SUCCESS;
274   }
275
276   /****************MLME-BEACON NOTIFY******************/
277
278   event result_t MLME_BEACON_NOTIFY.indication(uint8_t
279   BSN,PANDescriptor pan_descriptor, uint8_t PenAddrSpec,
280   uint8_t AddrList, uint8_t sduLength, uint8_t sdu[])
281   {
```

```
282         //Se já foi configurado, inicia o envio de
283   mensagens
284         if (config_flag)
285         {
286               if (TYPE == NODO)
287                     call
288   Timer_send.start(TIMER_ONE_SHOT,exp_time(500));
289         }
290
291         return SUCCESS;
292   }
293
294   /******************MLME-SYNC_LOSS******************/
295
296   event result_t MLME_SYNC_LOSS.indication(uint8_t
297   LossReason)
298   {
299         return SUCCESS;
300   }
301
302   /*********************MLME-RESET*********************/
303
304   event result_t MLME_RESET.confirm(uint8_t status)
305   {
306         return SUCCESS;
307   }
308
309   /*********************MLME-SCAN*********************/
310
311   event result_t MLME_SCAN.confirm(uint8_t status,uint8_t
312   ScanType, uint32_t UnscannedChannels, uint8_t
313   ResultListSize, uint8_t EnergyDetectList[],
314   SCAN_PANDescriptor PANDescriptorList[])
315   {
316         return SUCCESS;
317   }
318
319   /*****************MLME-COMM_STATUS*****************/
320
321   event result_t MLME_COMM_STATUS.indication(uint16_t
322   PANId,uint8_t SrcAddrMode, uint32_t SrcAddr[], uint8_t
323   DstAddrMode, uint32_t DstAddr[], uint8_t status)
324   {
325          return SUCCESS;
326   }
327
328   /*******************MLME-GET*********************/
329
```

```
330   event result_t MLME_GET.confirm(uint8_t status,uint8_t
331   PIBAttribute, uint8_t PIBAttributeValue[])
332   {
333           return SUCCESS;
334   }
335
336
337   /*******************MLME-SET************************/
338
339   event result_t MLME_SET.confirm(uint8_t status,uint8_t
340   PIBAttribute)
341   {
342         return SUCCESS;
343   }
344   /*******************MLME-POLL************************/
345
346   event result_t MLME_POLL.confirm(uint8_t status)
347   {
348         return SUCCESS;
349   }
350
351   /*******************MCPS EVENTS **********************/
352
353
354
355   /*******************MCPS-DATA ************************/
356
357   event result_t MCPS_DATA.confirm(uint8_t msduHandle,
358   uint8_t status)
359   {
360         switch(status)
361         {
362               case MAC_SUCCESS:
363                     mensagens_enviadas++;
364                     total_tentativas++;
365                     break;
366               case MAC_CHANNEL_ACCESS_FAILURE:
367               case MAC_NO_ACK:
368                     mensagens_perdidas++;
369                     total_tentativas++;
370                     break;
371               default:
372                     return SUCCESS;
373         }
374         return SUCCESS;
375   }
376
```

```
377   event result_t MCPS_DATA.indication(uint16_t
378   SrcAddrMode, uint16_t SrcPANId, uint32_t SrcAddr[2],
379   uint16_t DstAddrMode, uint16_t DestPANId, uint32_t
380   DstAddr[2], uint16_t msduLength,uint8_t
381   msdu[100],uint16_t mpduLinkQuality, uint16_t
382   SecurityUse, uint16_t ACLEntry)
383   {
384         //Mensagem de Broadcast (Enviada pelo Coordenador
385   ->id=0 ) -> Configuração dos Nodos ao início do
386   experimento
387         if (SrcAddr[0]==0 && TYPE==NODO)
388         {
389               //Sinaliza configuracao realizada com
390   sucesso
391               call Leds.redOn();
392
393               config_flag=TRUE;
394         }
395         return SUCCESS;
396   }
397
398   /******************MCPS-PURGE************************/
399
400   event result_t MCPS_PURGE.confirm(uint8_t msduHandle,
401   uint8_t status)
402   {
403         return SUCCESS;
404   }
405
406   /******************OTHER FUNCTIONS*******************/
407
408   /*************************************
409   ****** Distribuição Exponencial ********
410   *************************************/
411
412   uint8_t exp_time(uint8_t mean){
413         //Algoritmo para gerar valores numa distribuição
414   exponencial com media mean
415         float u, k;
416         u = (call Random.rand() & 1000) / 1000.0; // Gera
417   numero aleatorio entre 0 e 1
418         k = -log(u)*mean;
419         return (int) k;
420   }
421   }
```

ANEXO III - Script de leitura dos pacotes ZENA (Python)

```
#CLASSE AnalyseSubFolders.py

#python2
#Analyze all subfolders inside a folder

import analyzeFolder
import sys
import os

def listFoldersContainingZF(rFolder):
    """Returns a list of folders, inside rFolder, that
contains Zena Files"""

    lf = []

    for (path, dirs, files) in os.walk(rFolder):
        for f in files:
            if '.zna' in f:
                lf.append(path)
                break

    #remove repeated
    lf = list(set(lf))

    return lf


if len(sys.argv)<2 :
    print('ERRO!\nUso: python2 analyzeSubFolders.py
"/pasta/raiz/que/contem/outras/pastas" <format>\nOnde
format = csv ou txt')
    sys.exit(0)

rootFolder = sys.argv[1]
format = sys.argv[2].lower()

folders = listFoldersContainingZF(rootFolder)

for folder in folders:
    print('forders contem: ', folders)
    print('format contem: ', format)
    print('folder contem: ', folder)
    analyzeFolder.processFolder(folder, format)

print('Resultado gerado com sucesso')
```

```
46  #CLASSE AnalyseFolders.py
47
48  #python2
49  #Analyze one Folder of ZenaFiles
50
51  import sys
52  import os
53  import zenafile
54
55  def processEnsaio(f):
56      '''Process zna file'''
57
58      zF = zenafile.myZenaFile()
59
60      zF.open(f)
61      zF.readPackets()
62
63      ensaio=[]
64
65      for i in range (1,8):
66          ensaio.append(zF.getLastDataFromAddr(i))
67
68      print('ensaio contem: ', ensaio)
69      return ensaio
70
71  def processFolder(folder, format):
72      "Process folder that contains .zna files"
73
74      folderName = folder.split('/')[-1]
75      print('folderName contem: ', folderName)
76
77      ensaios=[]
78
79      #Processa Ensaios
80      for f in sorted(os.listdir(folder)):
81          ext = f.split('.')[-1]
82
83          if ext == 'zna':
84              ensaios.append(processEnsaio(folder+'/'+f))
85
86      print('ensaios contem: ', ensaios)
87
88      #Faz Medias/Desvio
89      tEnviadas = tPerdidas = tPerdas = nE = nP =
90  tTentativas = tent = float(0)
91      n = float(len(ensaios))*7
92
93      for ensaio in ensaios:
```

```
94          for nodo in ensaio:
95              tEnviadas += nodo['enviadas']
96              tPerdidas += nodo['perdidas']
97             tTentativas +=
98  (nodo['enviadas'])+(nodo['perdidas'])
99
100     #medias
101     mEnviadas = tEnviadas/n
102     mPerdidas = tPerdidas/n
103     mTentativas = tTentativas/n
104
105     print('Media Enviadas: ', mEnviadas)
106     print('Media Perdidas: ', mPerdidas)
107     print('Media Tentativas: ', mTentativas)
108
109     #porcentagem
110     mPerdas = mPerdidas/mTentativas*100
111
112     print('Percentual de perdas: ', mPerdas)
113
114     resultF = open(folder+'/resultado.txt', 'w')
115     resultF.write('Resultado do Teste
116 '+folderName+'\n\n')
117
118 resultF.write('{0:^5}{1:^10}{2:^10}{3:^20}{4:^20}\n'.for
119 mat('ID', 'Enviadas', 'Perdidas','Tentativas',
120 'Percentual de perdas'))
121
122     for ensaio in ensaios:
123         resultF.write('\n{0:^10}\n'.format('Teste
124 '+str(ensaios.index(ensaio)+1)))
125         for nodo in ensaio:
126            nE = float(nodo['enviadas'])
127            nP = float(nodo['perdidas'])
128            tent = float(nE+nP)
129            if (nP != 0):
130                tPerdas = nP/tent*100
131            else:
132               tPerdas = 0
133             txt =
134 '{0:^5}{1[enviadas]:^10}{1[perdidas]:^10}{2:^20.0f}{3:^2
135 0.3f}'.format(ensaio.index(nodo)+1, nodo, tent,tPerdas)
136             resultF.write(txt+'\n')
137
138     #Imprime medias
139     resultF.write('\n\n')
140     resultF.write('Resultados Medios:\n')
```

```
141
142     resultF.write('{0:^5}{1:^10.3f}{2:^10.3f}{3:^20.3f}{4:^2
143     0.3f}\n\n'.format('',mEnviadas, mPerdidas, mTentativas,
144     mPerdas))
145
146         #Fecha Arquivo
147         resultF.close()
148
149     if __name__ == '__main__':
150         #Running stand-alone
151
152         #Help
153         if len(sys.argv) < 2:
154             print('ERRO!\nUso: python2 analyzeFolder.py
155     "/local/armazenado/arquivos/zena" <format>\nOnde format
156     = csv ou txt')
157             sys.exit(0)
158
159         folder = sys.argv[1]
160
161         #Obtem Formato do Arquivo
162         format = sys.argv[2].lower()
163
164         processFolder(folder, format)
165
166         print('Resultado gerado com sucesso')
167
168
169     #CLASSE ZenaFile.py
170
171     #python2
172
173     import mmap
174     import struct
175
176     class ZenaFile:
177         '''Class to open .zna files, from Zena Packet
178     Analyzer'''
179
180         packets = []
181
182         def open(self, file):
183             '''Open file'''
184
185             try:
186                 self.f = open(file, 'r+b')
187                 self.map = mmap.mmap(self.f.fileno(),0)
188             except:
```

```
189             raise Exception("Couldn't open the file")
190
191     def readPackets(self):
192         '''Populate list of packets with packets from
193 file'''
194
195         while self.map.tell() != self.map.size():
196             frameNumber = self.map.read(4)
197             time = self.map.read(4)
198
199             len = self.map.read(1)
200             len = struct.unpack('B',len)[0] #hex str to
201 int
202
203             data = self.map.read(len)
204             data = data.encode('hex')
205
206             self.packets.append({'data':data,
207 'len':len})
208
209         self.f.close()
210
211     def getBytesAsStr(self, b, pktnum):
212         '''Return the 2-bytes in the b position of
213 packet as string'''
214
215         try:
216             return
217 self.packets[pktnum]['data'][2*b:2*b+2]
218         except:
219             raise Exception('Byte does not exist')
220
221     def getBytesAsInt(self, b, pktnum):
222         '''Return the 2-bytes in the b position of
223 packet as integer'''
224
225         try:
226             b = self.getBytesAsStr(b, pktnum)
227             b = int(b, 16)
228             return b
229         except:
230             raise Exception('Could not convert bytes to
231 int')
232
233     def getPackets(self):
234         '''Return the packets list.'''
235
236         return self.packets
```

```
237
238 ################################
239
240 class myZenaFile(ZenaFile):
241
242     def readPackets(self):
243         '''Ler todos os pacotes, mas manter apenas
244 aqueles com len == 21'''
245
246         #Use base class to read packets
247         ZenaFile.readPackets(self)
248
249         #Keep only the ones with size 21
250         self.packets = [p for p in self.packets if
251 p['len']==21]
252
253     def getSrcAddr(self, pktnum):
254         '''Obter o endereco de origem do pacote
255 pktnum'''
256
257         #Address is stored in 2 2-bytes num 9, 10
258         addr =
259 self.getBytesAsInt(9,pktnum)+256*self.getBytesAsInt(10,p
260 ktnum)
261         return addr
262
263     def getExperimentData(self, pktnum):
264         '''Obter tupla com dados experimentais do pacote
265 pktnum'''
266
267        #posicao do vetor payload
268         enviadas = self.getBytesAsInt(11,
269 pktnum)*256+self.getBytesAsInt(12, pktnum)
270         perdidas = self.getBytesAsInt(13,
271 pktnum)*256+self.getBytesAsInt(14, pktnum)
272        tentativas = self.getBytesAsInt(15,
273 pktnum)*256+self.getBytesAsInt(16, pktnum)
274        #o resto dos bytes eh randomico, nao corresponde
275 aos atributos esperados
276
277         return {'enviadas':enviadas,
278 'perdidas':perdidas, 'tentativas':tentativas}
279
280     def getLastDataFromAddr(self, addr):
281         '''Obter os dados a partir do ultimo pacote cujo
282 endereco eh addr'''
283
284         for i in reversed(range(len(self.packets))):
```

```
285                 if self.getSrcAddr(i) == addr:
286                     return self.getExperimentData(i)
```

ANEXO IV - Procedimento para embarcar os códigos nas plataformas MICAz

Neste anexo é descrito o procedimento para realizar o upload do código NesC para um nodo MICAz utilizando o sistema operacional (SO) TinyOS e fazendo uso da pilha OpenZB. Pressupoe-se que o usuário já tenha instalado o sistema operacional XubunTOS[10] (versão modificada da distribuição linux Xubuntu), numa maquina virtual, assim como a pilha OpenZB[11].

1. Inicia-se a máquina virtual com o SO supracitado;
2. Abre-se, através do terminal, o diretório que contém o código a ser embarcado nos nodos;
3. Digita-se o comando *tos1* para habilitar a versão 1.0 do TinyOS;
4. Digita-se o comando *make micaz*, responsável por compilar os arquivos. Se nenhum erro ocorrer uma imagem do SO TinyOS será criada;
5. Com a imagem criada deve-se embarcar o código. Para isso, deve-se montar o nodo na placa de configuração (sem pilhas) e conectar à porta USB do computador. É necessário que a placa de configuração seja reconhecida[12] pelo SO para que possa ser importado pela máquina virtual;
6. Após o nodo estar conectado na USB deve-se verificar se o nodo foi reconhecido no XubunTOS, utilizando o comando *dmesg |grep tty* no terminal. Deverá constar duas entradas. A primeira delas, em geral nomeada */dev/ttyUSB0,*será utilizada para configurar o nodo;
7. O próximo passo é o *upload* da imagem através do comando *make micaz reinstall*, **ID** *mib510*, **PORTA**
   onde, **ID** é o número de identificação do próprio nodo e **PORTA**[13] refere-se à porta USB em que a placa de configuração está conectada, no caso a *mib510;*

[10] Disponível em: http://www.eecs.berkeley.edu/~klueska/Xubuntos%202.1/
[11] Disponível em: http://www.hurray.isep.ipp.pt/art-wise
[12] No caso de uso do software *Oracle Virtual Box*, pode-se usar a barra inferior para autorizar o uso das portas USB pela máquina virtual.
[13] No caso do presente trabalho, utilizou-se a porta USB0. Portantato, o campo **PORTA** foi contém o caminho para a mesma, ou seja, */dev/ttyUSB0*.

8. Uma mensagem no terminal informará o sucesso, ou insucesso, do processo.