

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL  
ESCOLA DE ENGENHARIA  
DEPARTAMENTO DE ENGENHARIA ELÉTRICA  
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

**JEAN MICHEL WINTER**

**ANALISE DE COEXISTÊNCIA EM REDES WIRELESSHART**

Porto Alegre

2013

**JEAN MICHEL WINTER**

# **ANALISE DE COEXISTÊNCIA EM REDES WIRELESSHART**

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica, da Universidade Federal do Rio Grande do Sul, como parte dos requisitos para a obtenção do título de Mestre em Engenharia Elétrica.

Área de concentração: Controle e Automação

**ORIENTADOR:** Carlos Eduardo Pereira

Porto Alegre

2013

JEAN MICHEL WINTER

## **ANÁLISE DE COEXISTÊNCIA EM REDES WIRELESSHART**

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Engenharia Elétrica e aprovada em sua forma final pelo Orientador e pela Banca Examinadora.

Orientador: \_\_\_\_\_

Prof. Dr. Carlos Eduardo Pereira, UFRGS

Doutor pela Universität Stuttgart – Stuttgart, Alemanha

Banca Examinadora:

Prof. Dr. João César Netto, UFRGS.

Doutor pela Universite Catholique de Louvain – Louvain-la-Neuve, Bélgica.

Prof. Dr. João Manoel Gomes da Silva Junior, UFRGS

Doutor pela Universite Paul Sabatier – Toulouse, França.

Prof. Dr. Leandro Buss Becker, UFSC

Doutor pela Universidade Federal do Rio Grande do Sul, Brasil.

Coordenador do PPGEE: \_\_\_\_\_

Prof. Dr. João Manoel Gomes da Silva Junior

Porto Alegre, maio de 2013.

## **AGRADECIMENTOS**

Ao Professor Carlos Eduardo Pereira, pelo apoio e pela oportunidade de trabalho nesta área de pesquisa.

Aos colegas Alexandre Lorençato, Gustavo Künzel, Ivan Muller e Professor João César Netto pelo auxílio e pela participação nas atividades desenvolvidas.

À minha família pelo apoio e incentivo durante esta jornada.

Ao Programa de Pós-Graduação em Engenharia Elétrica, PPGEE.

À CAPES pela provisão da bolsa de mestrado.

## RESUMO

Os sistemas de comunicação sem fio vem ganhando cada vez mais espaço no cenário das comunicações digitais. Em relação aos tradicionais sistemas cabeados, as tecnologias de comunicação sem fio evitam a necessidade de infraestruturas de alto custo, tornam a rede mais flexível, trazem facilidades de reconfiguração e a portabilidade para terminais móveis. Com o crescimento e aprimoramento nos usos das redes de automação novas soluções de comunicação estão surgindo entre elas sistemas de comunicação sem fio que possam ser confiáveis e para aplicações em ambientes mais críticos. Em paralelo o espectro de frequência tem sido cada vez mais ocupado devido à grande demanda, especialmente a faixa de espectro não licenciada. A faixa de frequência de 2.4 GHz (ISM), por exemplo, tem sido vastamente explorada e deve ser atualmente a mais utilizada no mundo, especialmente pela aplicação das grandes redes de comunicação como a *world wide web*. Este trabalho aborda um estudo sobre coexistência do primeiro protocolo certificado para comunicação sem fio aplicado à indústria, o *WirelessHART*. É apresentada uma visão geral do protocolo, os diferentes mecanismos de coexistência propostos no padrão e ainda um conjunto de ferramentas desenvolvidas para a análise de desempenho do protocolo *WirelessHART*. Os estudos de caso utilizam os padrões IEEE 802.11g, IEEE 802.15.1 e o próprio *WirelessHART*, sendo aplicados a análises experimentais estando presentes condições reais de propagação de sinais de rádio frequência, as quais são muitas vezes simplificadas nos tradicionais trabalhos em ambientes simulados.

**Palavras-chave:** Coexistência em redes sem fio, *WirelessHART*, Automação e Controle.

## ABSTRACT

Wireless communication systems are gaining more space in digital communications area. Compared to traditional wired systems, wireless communication technologies avoid the need for costly infrastructure, making the networks more flexible, improving portability and allowing an easier reconfiguration of mobile terminals. With the growth and improvement in the use of automation networks, new solutions are emerging in the communication systems, including reliable wireless communication for applications in critical environments. In parallel the frequency spectrum has become increasingly busy due to high demand, especially the unlicensed spectrum band. The frequency range of 2.4 GHz (ISM), for example, has been widely explored worldwide, especially by the application of large communication networks such as the world wide web. This work discusses a study on coexistence of the first certified industrial wireless communication protocol, the *WirelessHART*. It presents an overview of the protocol, the different coexistence mechanisms proposed in the standard and also a set of tools developed for the performance and coexistence analysis of *WirelessHART*. Case studies assessing the impact of IEEE 802.11g, IEEE 802.15.1 as well as of other *WirelessHART* networks experimentally are presented, on which real conditions of propagation of radio frequency signals, which are often simplified in traditional work in simulated environments, are evaluated. Obtained results indicated the adequacy of *WirelessHart* for industrial applications.

**Keywords:** Coexistence in wireless communication. *WirelessHART*. Automation and Control.

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	<b>13</b>
<b>2</b>	<b>FUNDAMENTAÇÃO TEÓRICA</b>	<b>16</b>
<b>2.1</b>	<b>CONCEITOS DE REDE DE COMUNICAÇÃO SEM FIO</b>	<b>16</b>
<b>2.1.1</b>	<b>Modulação</b>	<b>16</b>
<b>2.1.2</b>	<b>Espalhamento do Espectro</b>	<b>17</b>
<b>2.1.3</b>	<b>Ciclo de Trabalho</b>	<b>18</b>
<b>2.1.4</b>	<b>Topologia da Rede</b>	<b>18</b>
<b>2.2</b>	<b>MODELO OSI</b>	<b>19</b>
<b>2.2.1</b>	<b>Camada Física</b>	<b>19</b>
<b>2.2.2</b>	<b>Camada de Enlace</b>	<b>20</b>
<b>2.2.2.1</b>	<b>CSMA e CSMA-CA</b>	<b>21</b>
<b>2.2.3</b>	<b>Camada de Rede</b>	<b>21</b>
<b>2.3</b>	<b>RUÍDO E INTERFERÊNCIA</b>	<b>22</b>
<b>2.4</b>	<b>PROTOCOLOS DE COMUNICAÇÃO EM 2.4 GHz</b>	<b>25</b>
<b>2.4.1</b>	<b>IEEE 802.11</b>	<b>26</b>
<b>2.4.1.1</b>	<b>IEEE 802.11b</b>	<b>26</b>
<b>2.4.1.2</b>	<b>IEEE 802.11g</b>	<b>26</b>
<b>2.4.2</b>	<b>IEEE 802.15.1</b>	<b>27</b>
<b>2.4.3</b>	<b>IEEE 802.15.4</b>	<b>29</b>
<b>2.4.4</b>	<b>WirelessHART</b>	<b>30</b>
<b>2.4.4.1</b>	<b>WirelessHART e o Modelo OSI</b>	<b>32</b>
<b>2.4.4.1.1</b>	<b>Camada Física</b>	<b>32</b>
<b>2.4.4.1.2</b>	<b>Camada de Enlace</b>	<b>33</b>
<b>2.4.4.1.3</b>	<b>Camada de Rede</b>	<b>35</b>
<b>2.4.4.1.4</b>	<b>Camada de Aplicação</b>	<b>36</b>
<b>3</b>	<b>MECANISMOS DE COEXISTÊNCIA DO WIRELESSHART</b>	<b>37</b>
<b>3.1</b>	<b>ACESSO AO MEIO</b>	<b>37</b>
<b>3.2</b>	<b>MODULAÇÃO</b>	<b>38</b>
<b>3.3</b>	<b>SALTO DE CANAIS</b>	<b>38</b>
<b>3.4</b>	<b>CCA – CLEAR CHANNEL ASSESSMENT</b>	<b>39</b>
<b>3.5</b>	<b>LISTA PROIBIDA DE CANAIS</b>	<b>41</b>
<b>3.6</b>	<b>DSSS</b>	<b>42</b>
<b>3.7</b>	<b>REDE DO TIPO MALHA</b>	<b>42</b>
<b>3.8</b>	<b>BAIXO CICLO DE TRABALHO</b>	<b>44</b>
<b>4</b>	<b>ANÁLISE DO ESTADO DA ARTE EM ESTUDOS SOBRE COEXISTÊNCIA DE REDES SEM FIO</b>	<b>45</b>
<b>4.1</b>	<b>MODELAGEM MATEMÁTICA</b>	<b>45</b>
<b>4.2</b>	<b>ANÁLISE DE COEXISTÊNCIA BASEADO EM SIMULAÇÕES</b>	<b>47</b>
<b>4.3</b>	<b>ANÁLISE EXPERIMENTAL</b>	<b>49</b>
<b>5</b>	<b>ANÁLISE DE COEXISTÊNCIA EM REDES WIRELESSHART</b>	<b>54</b>
<b>5.1</b>	<b>MÉTODOS E MÉTRICAS UTILIZADAS</b>	<b>54</b>
<b>5.1.1</b>	<b>Latência e Jitter</b>	<b>55</b>
<b>5.1.2</b>	<b>Taxa de Pacotes Perdidos</b>	<b>57</b>
<b>5.1.3</b>	<b>Deteção de Energia</b>	<b>60</b>

<b>5.1.4</b>	<b>Confiabilidade.....</b>	<b>63</b>
<b>5.2</b>	<b>ESTUDO DE CASO .....</b>	<b>63</b>
<b>5.2.1</b>	<b>Parâmetros da Rede <i>Wireless</i>HART .....</b>	<b>64</b>
<b>5.2.2</b>	<b>Desempenho da Rede <i>Wireless</i>HART sem Interferência .....</b>	<b>65</b>
<b>5.2.3</b>	<b>Rede <i>Wireless</i>HART sob Interferência do IEEE 802.11 .....</b>	<b>66</b>
<b>5.2.3.1</b>	<b>Sobreposição Parcial de Canais .....</b>	<b>66</b>
<b>5.2.3.2</b>	<b>Sobreposição Total de Canais .....</b>	<b>77</b>
<b>5.2.3.3</b>	<b>CCA E IEEE 802.11g.....</b>	<b>81</b>
<b>5.2.4</b>	<b>Interferência do IEEE 802.15.1 .....</b>	<b>84</b>
<b>5.2.5</b>	<b><i>Wireless</i>HART x <i>Wireless</i>HART .....</b>	<b>86</b>
<b>5.2.5.1</b>	<b>Interferência de uma rede <i>Wireless</i>HART .....</b>	<b>89</b>
<b>5.2.6</b>	<b>Interferência por Canal Adjacente .....</b>	<b>91</b>
<b>5.2.7</b>	<b>Tamanho e Tráfego de Pacotes de uma Rede WH .....</b>	<b>92</b>
<b>6</b>	<b>CONCLUSÃO.....</b>	<b>94</b>
<b>7</b>	<b>TRABALHOS FUTUROS .....</b>	<b>96</b>
<b>7.1</b>	<b>PROPOSTA DE ANÁLISE DE DESEMPENHO E LIMITES DE POTÊNCIA INTERFERENTE.....</b>	<b>96</b>
<b>7.2</b>	<b>PROPOSTA DE MECANISMOS ATIVOS DE COEXISTÊNCIA .....</b>	<b>97</b>
	<b>REFERÊNCIAS .....</b>	<b>99</b>



## LISTA DE ILUSTRAÇÕES

Figura 1 Alguns protocolos de comunicação e faixas não licenciadas do espectro de frequência. ....	14
Figura 2 Ciclo de trabalho .....	18
Figura 3 Diagrama de bloco de um sistema de comunicação. (HAYKIN, 2008) .....	20
Figura 4. Espectro utilizado protocolos IEEE 802.11 b/g. ....	27
Figura 5. Salto de canais do padrão IEEE 802.15.1. ....	28
Figura 6 Exemplo de redes IEEE 802.15.4. ....	30
Figura 7. Uma rede <i>Wireless</i> HART típica.....	31
Figura 8 Modelo OSI e o padrão WH. (CHEN, 2010) .....	32
Figura 9 Estrutura da DLPDU WH. (HCF, 2008) .....	33
Figura 10 Exemplo de salto de canais .....	39
Figura 11 . Tempo do <i>slot</i> . (Adaptado de CHEN, 2010).....	40
Figura 12 Modos de operação versus consumo de corrente de um transceptor típico IEEE 802.15.4. (FREESCALE, 2012) .....	41
Figura 13 Rede tipo malha: a) rotas diretas para o gateway; b) rotas alternativas.....	43
Figura 14 Perda de pacotes de uma rede WH sob interferência IEEE 802.11 entre 3 e 22 horas.....	52
Figura 15. Comunicação da aplicação com os dispositivos de campo.....	55
Figura 16 Diagrama de sequência da aplicação HART sobre UDP .....	56
Figura 17. Dados obtidos na interface da aplicação. ....	56
Figura 18. Comunicação da aplicação diretamente com dispositivo WH.....	57
Figura 19 Interface de aplicação para acesso a porta de manutenção do dispositivo WH.....	58
Figura 20 Imagem dos tempos de envio de mensagem do dispositivo WH e do chaveamento do modem para detecção de energia.....	61
Figura 21. Comunicação entre os dispositivos e a aplicação para detecção de energia.....	62
Figura 22 Diagrama de sequência da detecção de energia .....	62
Figura 23 Dispositivos WH. ....	64
Figura 24 Jitter da rede WH em condições livre de interferência .....	65
Figura 25. Frequências utilizadas (a) WH e (b) IEEE 802.11. (Adaptado de ANGRISANI, 2008).....	67
Figura 26 Cenário utilizado para a rede WH.....	68
Figura 27 Desempenho do protocolo WH para diferentes condições de interferência .....	69
Figura 28 Jitter para um ciclo de trabalho de 4% e pacotes de 540 bytes da WLAN .....	69
Figura 29 Jitter para um ciclo de trabalho de 7% e pacotes de 540 bytes da WLAN .....	70
Figura 30 Jitter para um ciclo de trabalho de 40% e pacotes de 540 bytes da WLAN .....	70
Figura 31 Jitter para um ciclo de trabalho de 60% e pacotes de 540 bytes da WLAN .....	70
Figura 32 Jitter para um ciclo de trabalho de 80% e pacotes de 540 bytes da WLAN .....	71
Figura 33 Jitter para um ciclo de trabalho de 100% e pacotes de 540 bytes da WLAN .....	71
Figura 34 Jitter para um ciclo de trabalho de 4% e pacotes de 1024 bytes da WLAN .....	71
Figura 35 Jitter para um ciclo de trabalho de 7% e pacotes de 1024 bytes da WLAN .....	72

Figura 36 Jitter para um ciclo de trabalho de 40% e pacotes de 1024 bytes da WLAN .....	72
Figura 37 Jitter para um ciclo de trabalho de 60% e pacotes de 1024 bytes da WLAN .....	72
Figura 38 Jitter para um ciclo de trabalho de 80% e pacotes de 1024 bytes da WLAN .....	73
Figura 39 Jitter para um ciclo de trabalho de 100% e pacotes de 1024 bytes da WLAN .....	73
Figura 40 Jitter para um ciclo de trabalho de 4% e pacotes de 1500 bytes da WLAN .....	73
Figura 41 Jitter para um ciclo de trabalho de 7% e pacotes de 1500 bytes da WLAN .....	74
Figura 42 Jitter para um ciclo de trabalho de 40% e pacotes de 1500 bytes da WLAN .....	74
Figura 43 Jitter para um ciclo de trabalho de 60% e pacotes de 1500 bytes da WLAN .....	74
Figura 44 Jitter para um ciclo de trabalho de 80% e pacotes de 1500 bytes da WLAN .....	75
Figura 45 Jitter para um ciclo de trabalho de 100% e pacotes de 1500 bytes da WLAN .....	75
Figura 46 Latência da rede WH para uma rede interferente com mensagens de 540 bytes .....	76
Figura 47 Latência da rede WH para uma rede interferente com mensagens de 1024 bytes .....	77
Figura 48 Latência da rede WH para uma rede interferente com mensagens de 1500 bytes .....	77
Figura 49 Segundo cenário utilizado – interferência or downlink .....	78
Figura 50. Canais utilizados: a) WH; b) rede WLAN e c) imagem real do espectro de frequência utilizado. ....	78
Figura 51 Terceiro cenário utilizado - interferência por <i>uplink</i> .....	79
Figura 52 Perda de pacotes do WH para condições de interferência por <i>uplink</i> e <i>downlink</i> .....	80
Figura 53 Níveis de energia e LQI medidos sem interferência. ....	81
Figura 54 Níveis de energia e LQI medidos com interferência.....	81
Figura 55 Distribuição dos dispositivos para análise de desempenho do CCA. ....	82
Figura 56. Distribuição dos dispositivos Bluetooth na rede WH .....	84
Figura 57 Jitter da rede WH sob interferência do IEEE 802.15.1 .....	85
Figura 58 Latência da rede WH sob interferência do IEEE 802.15.1 .....	85
Figura 59 Distribuição e conexão dos dispositivos WH .....	87
Figura 60 Quadros de tempo dos dispositivos 3 e 4 dentro do superframe 0.....	88
Figura 61 Alteração das conexões dos dispositivos da rede WH .....	90
Figura 62 a) Sinal de potência modulado. Em b, as relações de intensidades com canais adjacentes.....	92
Figura 63 Fluxo de pacotes de uma rede WH .....	93
Figura 64 Cenário proposto para análise de interferência .....	97

## LISTA DE TABELAS

Tabela 1	Comandos do WH relacionados ao compartilhamento do espectro de frequência ..	36
Tabela 2	Trabalhos relacionados .....	52
Tabela 3	Média de ciclo de trabalho IEEE 802.11g para diferentes atividades. ....	66
Tabela 4	Média e o desvio padrão do jitter da rede WH sobe diferentes condições de operação da rede IEEE 802.11 .....	76
Tabela 5	Desempenho WH com CCA.....	83
Tabela 6	Tempo e tamanho dos pacotes utilizados no ensaio com Bluetooth .....	84
Tabela 7	Conexões do dispositivo 3 .....	87
Tabela 8	Conexões do dispositivo 4 .....	88

## **LISTA DE ABREVIATURAS**

AFH: Associação Brasileira de Normas Técnicas

ASN: Absolute Slot Number

CRC: Cyclic Redundancy Check

CSMA: Carrier Sense Multiple Access

DLPDU: Data Link Protocol Data Unit

DSSS: Direct Sequence Spread Spectrum

FFD: Full Function Device

FHSS: Frequency Hop Spread Spectrum

GPIO: General Purpose Input/Output

HCF: HART Communication Foundation

ICMP: Internet Control Message Protocol

ISM: Industrial Scientific and Medical

LLC: Logical Link Control

LQI: Link Quality Indicator

MAC: Medium Access Control

MIC: Message Integrity Check

PLR: Packet Loss Rate

PN: Pseudo Noise

RFD: Reduced Function Device

RSSI: Received Signal Strength Indication

TCP: Transmission Control Protocol

**TDMA: Time Division Multiple Access**

**UDP: User Datagram Protocol**

**WLAN: Wireless Local Area Network**

**WSN: Wireless Sensor Network**

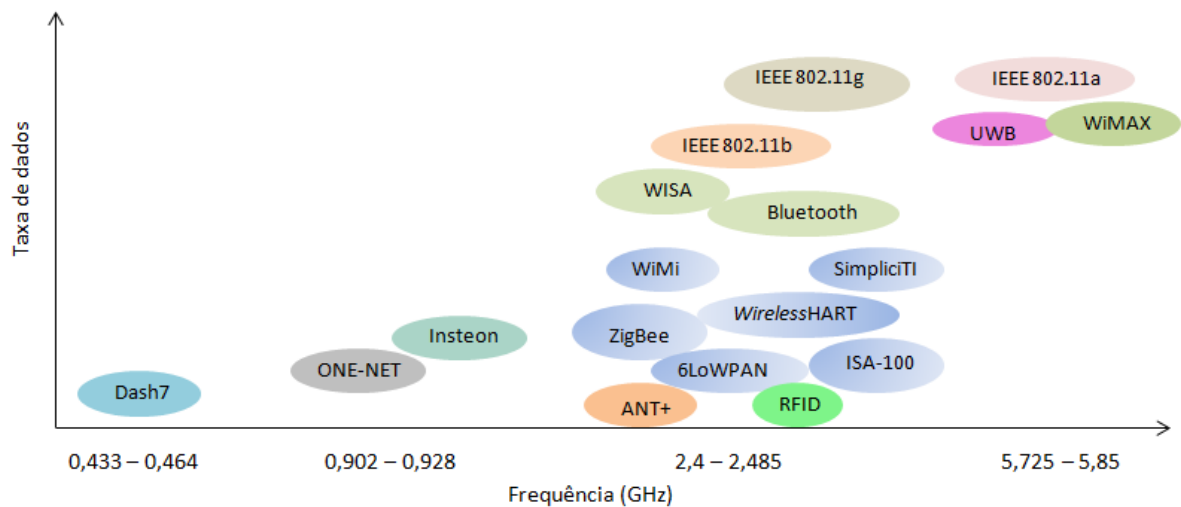
## 1 INTRODUÇÃO

Nas últimas décadas os sistemas de automação tem ganhado destaque para a busca de maior eficiência e qualidade na produção ao mesmo tempo em que busca-se reduzir o esforço e a interferência humana sobre processos e máquinas através da automatização dos processos. A comunicação entre os diversos dispositivos que compõem o cenário da indústria tornou-se elemento fundamental para a garantia de qualidade em processos cada vez mais complexos. Em paralelo, os sistemas de automação industrial têm sido caracterizados por uma redução progressiva no uso de cabos. Os esforços por parte da indústria têm consagrado diversos protocolos de comunicação como Fieldbus (THOMESSE, 2005), HART (HCF, 2007), Profibus (TOVAR, 1999) entre outros, os quais propõem o uso de estruturas de comunicação na forma de redes do tipo barramento, com algumas bifurcações, reduzindo consideravelmente a quantidade de cabeamento necessária nas ligações ponto a ponto, como por exemplo, demandada pelo protocolo baseados em laços de corrente de 4 a 20 mA (usualmente conhecido como “protocolo 4 a 20”).

Mais recentemente algumas organizações industriais tem promovido o uso de tecnologias de comunicação sem fio, as quais trazem ganhos como flexibilidade (cobertura de locais de difícil acesso para cabos), facilidade (instalação rápida) e escalabilidade (diversidade nas topologias). Os benefícios dos sistemas de comunicação sem fio têm motivado o surgimento e a utilização de um grande número de diferentes padrões e dispositivos que muitas vezes competem pelo uso de uma mesma faixa do espectro de frequência (vide Figura 1). A presença de diferentes padrões de comunicação sem fio em uma mesma área de cobertura pode resultar em efeitos típicos de interferência como, perda de dados, jitter, atraso nas transmissões e perda de sincronismo entre os dispositivos. Problemas que muitas vezes podem resultar em grandes perdas e falhas no processo. Estes são fatores que trazem

preocupação e relutância quanto à adoção de tecnologias de comunicação sem fio para o uso industrial.

Entre as várias tentativas de lançar um padrão para uso industrial, tais como o Bluetooth, WiFi, Zigbee e WINA, nenhuma obteve uma aceitação definitiva por parte da indústria. Atualmente, os padrões existentes não tratam o problema de possível coexistência com outros protocolos (são intrinsecamente “egoístas”) e não possuem mecanismos que permitam descobrir e coexistir efetivamente com outros dispositivos que utilizam diferentes soluções (DOMINICS, et al., 2009). Fatores como confiabilidade, segurança e determinismo são geralmente requisitos críticos para aplicações industriais e podem ser comprometidos sob condições de interferência com outros protocolos.



**Figura 1** Alguns protocolos de comunicação e faixas não licenciadas do espectro de frequência.

Recentemente a IEC (*International Electrotechnical Commission*) certificou o padrão *WirelessHART* (WH) como o primeiro protocolo de comunicação sem fio para controle de processo industrial (IEC 62591, 2010). Os dispositivos WH foram lançados recentemente e ainda há uma falta de informações e estudos na literatura referente ao desempenho deste padrão, em especial sobre os problemas de coexistência com outros protocolos que operam na mesma faixa de frequência (IEEE 802.11, Zigbee, Bluetooth,...). Sob estas circunstâncias

torna-se necessário avaliar qual é o impacto destas outras redes coexistindo com uma rede WH. Questões como: o quão suscetível a falhas pode ficar o controle de um determinado processo, sob quais limites a comunicação se mantém confiável e quais parâmetros são mais influentes na interferência por coexistência, são exemplos de questões que devem ser estudadas.

Neste trabalho são abordados os seguintes temas: i) é feita uma análise dos mecanismos que o protocolo WH utiliza para coexistir com outras redes, ii) são analisados os principais padrões que podem interferir em uma rede WH e que podem afetar significativamente o seu desempenho, sendo que o presente trabalho analisa o desempenho do WH em condições danosas de coexistência. O trabalho é estruturado como segue: no capítulo dois é apresentada a fundamentação teórica e que serve de embasamento para a compreensão do trabalho, incluindo neste capítulo uma análise dos principais protocolos de comunicação que concorrem com o *WirelessHART* assim como uma visão geral do protocolo WH. No capítulo três é apresentado uma análise dos mecanismos de coexistência do protocolo WH. No capítulo 4 é realizada uma análise do estado da arte sobre outros trabalhos relacionados. O capítulo cinco apresenta uma análise de coexistência do protocolo WH, onde é detalhado o desenvolvimento de ferramentas específicas para avaliar o desempenho deste padrão e também os resultados experimentais para situações de interferência. No capítulo 6 e 7 são apresentadas as conclusões e trabalhos futuros.



## 2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados alguns dos conceitos de base que ajudam no entendimento das redes de comunicação sem fio. Primeiramente são abordadas questões da camada física, onde ocorre a propagação do sinal. Na segunda parte é abordado o modelo OSI que ajuda a caracterizar e padronizar as funções internas dos sistemas de comunicação através da partição abstrata das camadas. Em seguida são apresentados as principais definições de ruído e interferência. A última parte apresenta brevemente outros protocolos que operam na faixa de 2.4 GHz, inclusive o protocolo WH.

### 2.1 CONCEITOS DE REDE DE COMUNICAÇÃO SEM FIO

Nesta etapa são introduzidos alguns conceitos utilizados nos protocolos de comunicação sem fio.

#### 2.1.1 Modulação

A modulação é o processo utilizado para o mapeamento de bits de dados para sinais em forma de onda que podem ser transmitidos em um canal (analógico). A modulação digital transforma um grupo de  $n$  bits, também conhecido por símbolos, em formas de onda. A forma de onda pode ser expressa conforme equação um.

$$s(t) = A(t) \cos[w_0 t + \phi(t)] \quad (1)$$

onde  $A(t)$  é a amplitude do sinal,  $\phi(t)$  é o ângulo ou fase, e  $w_0$  é o centro da frequência utilizada. São três os tipos básicos de técnicas de modulação: ASK (*Amplitude-Shift Keying*), FSK (*Frequency-shift keying*) e PSK (*Phase-shift keying*).

**ASK:** Modulação em amplitude por chaveamento é uma das técnicas mais simples. Consiste na alteração da amplitude da onda portadora em função do sinal digital a ser transmitido, codificando os  $M$  símbolos, vide equação (2).

$$s_i = A(t) \cos[w_0 t + \emptyset] \text{ para } i = 1, \dots, M \quad (2)$$

**FSK:** Modulação em frequência por chaveamento, neste caso a frequência é o elemento variante, conforme equação (3).

$$s_i = A \cos[w_i(t) + \emptyset] \text{ para } i = 1, \dots, M \quad (3)$$

**PSK:** Modulação em fase por chaveamento, esta técnica altera a fase da onda portadora, e é demonstrado na equação (4).

$$s_i = A \cos[w_0 t + \emptyset_i(t)] \text{ para } i = 1, \dots, M \quad (4)$$

### 2.1.2 Espalhamento do Espectro

O conceito básico do espalhamento do espectro é transmitir o sinal desejado sobre uma largura de banda adicional, usando menos potência por frequência e mais frequências. A informação  $s(t)$  é multiplicada por um sinal  $c(t)$  constituído de um pseudo-ruído (PN), vide equação (5).

$$m(t) = c(t)s(t) \quad (5)$$

onde  $m(t)$  é o resultado do sinal multiplicado, o qual tem as mesmas características de largura de banda do sinal PN.

Através do espalhamento do espectro, obtêm-se alguns benefícios como:

- Rejeição a interferência intencional (*jamming*): sendo as transmissões vizinhas na mesma faixa de frequência do sinal de interesse são descorrelacionadas e assim fortemente atenuadas no receptor;
- Rejeição a interferência natural: ocorre em função do ganho de processamento presente no processo de espalhamento;
- Baixa probabilidade de interceptação: o sinal apresenta uma faixa mais larga para monitoração assim como a densidade de potência do sinal reduzido pelo processo de espalhamento do espectro.

### 2.1.3 Ciclo de Trabalho

Ciclo de trabalho ou carga na rede  $\lambda(\%)$ , é definido como a taxa ativa de duração do tempo de transmissão  $t_{ativo}(s)$  do tempo total  $t_{total}$  (s) e um determinado sinal. O ciclo de trabalho é inversamente proporcional ao tempo de ócio entre as transmissões (VERLOOCK et al., 2010), vide equação seis e Figura 2. Para uma determinada taxa de dados, quanto maior a carga de dados demandada menor o tempo de ócio da rede.

$$\lambda = 100 \cdot \frac{t_{ativo}}{t_{total}} (\%) \quad (6)$$

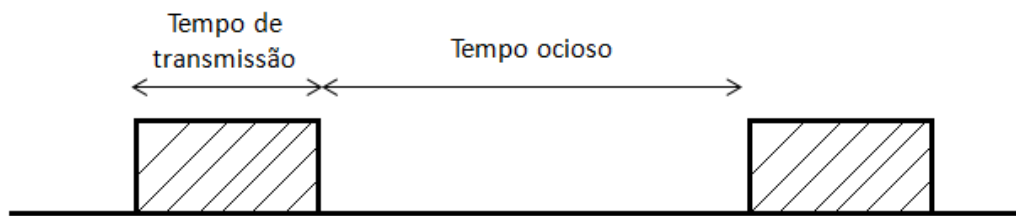


Figura 2 Ciclo de trabalho

### 2.1.4 Topologia da Rede

A topologia da rede representa o padrão no qual os elementos que compõem a rede estão conectados. A topologia de rede mais simples é constituída de dois nodos (ponto-a-ponto). Outras topologias de rede básicas são: estrela, malha, árvore e híbrida. A topologia da rede pode variar em tamanho e complexidade dependendo do cenário utilizado. Para diferentes tecnologias de comunicação existem diferentes parâmetros que determinam a topologia a ser utilizada. Na comunicação sem fio esta é uma importante característica que deve ser considerada, uma vez que os mecanismos de encaminhamento de mensagens estão intrinsicamente relacionados à forma de conexão adotada entre os nodos podendo implicar no desempenho da rede através da latência, jitter e confiabilidade.

## 2.2 MODELO OSI

Podemos diferenciar os tradicionais sistemas de comunicação com fio dos sistemas de comunicação sem fio através das camadas: física, de enlace e rede, de acordo com o modelo OSI (*Open System Interconnection*).

### 2.2.1 Camada Física

Esta camada fornece os mecanismos físicos para a transmissão binária, codificada nos dígitos binários zero e um, entre dois nós de uma rede. Nos sistemas de comunicação sem fio, é a camada responsável por selecionar as frequências que serão utilizadas, gerar a portadora, detectar, modular e codificar o sinal. Esta camada possui três componentes básicos (vide Figura 3):

**Transmissor:** tem como função modificar e transmitir a informação recebida da fonte no canal (meio de transmissão) utilizando-se dos recursos limitados do meio (como o espectro de frequência). Também é responsável por minimizar a interferência de outros usuários, uma vez que o canal é compartilhado;

**Canal:** Este é o componente referente ao caminho físico de transporte do sinal gerado pelo transmissor. Em sistemas de comunicação sem fio, perdas no canal podem ocorrer e são frequentemente causadas por:

- Interferência natural e ou artificial, originadas por fontes cujos sinais ocupam a mesma banda de frequência do sinal transmitido;
- Distorção no canal que pode estar associado aos múltiplos caminhos que uma onda de sinal propagada pode percorrer até chegar ao seu destino final, que pode gerar interferência destrutiva no sinal desejado;
- Ruídos do receptor gerados dentro do próprio dispositivo eletrônico utilizado para transmitir e receber o sinal, esses ruídos são considerados efeitos do canal. Estes

sinais são dependentes da intensidade do sinal recebido que por sua vez depende do caminho de propagação entre o transmissor e o receptor.

**Receptor:** Este atua no sinal recebido, de forma a identificar o sinal de informação original transportado através do canal utilizado. Usa técnicas de compensação e de correção de erros de forma que seja possível corrigir as perdas inevitáveis no canal.



**Figura 3 Diagrama de bloco de um sistema de comunicação. (HAYKIN, 2008)**

### 2.2.2 Camada de Enlace

Os enlaces de sistemas de comunicação sem fio são normalmente não confiáveis (HAYKIN, 2008). Esta camada realiza as tarefas de controle de erros, detecção de quadros e multiplexação do fluxo de dados. Frequentemente, a camada de enlace retransmite pacotes recebidos com erros. Essa camada também é responsável pelo modo como os diferentes usuários compartilham o meio de transmissão. Para os sistemas de comunicação sem fio, o meio de transmissão é o espectro de frequências de rádio. Dentro desta camada está uma subcamada denominada MAC (*Medium Access Control*), que é a responsável pela transmissão dos quadros através do meio de transmissão compartilhado com outros nós da rede. Esse aspecto das comunicações é conhecido como comunicações de acesso múltiplo.

Existem diferentes estratégias de acesso múltiplo de compartilhamento do espectro de frequências:

**FDMA** (*Frequency Division Multiple Access*). Neste método o espectro de frequência é compartilhado entre os usuários, por meio da atribuição de faixas de frequência específicos, de modo fixo ou variável.

**CDMA** (*Code Division Multiple Access*). No acesso múltiplo por divisão de código, o compartilhamento do espectro é feito por uma forma de modulação através do espalhamento espectral, permitindo que diversos usuários utilizem todo o espectro disponível.

**TDMA** (*Time Division Multiple Access*). No acesso múltiplo por divisão no tempo, os usuários tem acesso total ao espectro durante um determinado período de tempo.

**SDMA** (*Space Division Multiple Access*). Para o acesso múltiplo por divisão no espaço, o compartilhamento do espectro entre os usuários aproveita a distribuição espacial dos terminais dos usuários através de antenas direcionais, minimizando as interferências entre os usuários.

#### **2.2.2.1 CSMA e CSMA-CA**

O Acesso Múltiplo com Sensoriamento da Portadora (*Carrier Sense Multiple Access*, CSMA) e CSMA-CA (*Collision Avoidance*) são métodos utilizados para a arbitração do acesso ao meio. No mecanismo de CSMA, o dispositivo que está pronto para transmissão deve escutar antes de transmitir o canal. Se estiver sem interferência, o dispositivo deve iniciar a transmissão, caso contrário, deve aguardar até que o canal esteja desocupado novamente. No CSMA-CA, o dispositivo deve aguardar um período randômico antes de transmitir, isto previne colisões contínuas quando diversos dispositivos tentam transmitir ao mesmo tempo.

#### **2.2.3 Camada de Rede**

A camada de rede é responsável pelo roteamento de dados entre dois ou mais sistemas de comunicação. Também tem a função de determinar a qualidade de serviço (QoS) da rede. Outra atribuição importante é a capacidade de prover o controle de fluxo para evitar o congestionamento da rede.

### 2.3 RUÍDO E INTERFERÊNCIA

Todos os parâmetros de sistemas de comunicação sem fio que afetam o desempenho como: modulação, correção de erro, espalhamento do espectro, salto de frequência, tamanho dos pacotes, ciclo de trabalho, potência de transmissão e topologia da rede, estão dentro do contexto das camadas apresentadas acima e podem ser divididos em dois tipos: i) parâmetros que afetam somente o desempenho do próprio sistema e ii) parâmetros que afetam as interações entre dois sistemas distintos de comunicação, com exceção do esquema de modulação e a correção de erros, todos os outros são parâmetros que pertencem ao segundo tipo (YANG; XU; GIDLUND, 2011). Sendo a coexistência uma questão básica para as comunicações sem fio.

Em geral, o ruído representa qualquer sinal indesejado de uma fonte externa, o qual pode perturbar ou mascarar o sinal desejado. Estes sinais podem vir de outras fontes de sinal que estão emitindo na mesma banda de frequência e no mesmo instante de tempo. Nas interferências por co-canal, a fonte interferente irradia no mesmo ou em uma frequência sobreposta ao transceptor em consideração. Outro caso é o de interferência por canal adjacente que ocorre quando a fonte interferente irradia sinal em uma banda de frequência vizinha podendo deixar algum sinal de energia na banda utilizada pelo transceptor desejado e ou o receptor pode ter imperfeições nos filtros e capturar o sinal da banda vizinha. Os sistemas de comunicação sem fio devem prover um limite mínimo de qualidade na transmissão, este limite de qualidade requer um valor mínimo de relação sinal ruído (SNR) no receptor. O ruído que perturba o sinal pode ser proveniente de diversos componentes:

**Ruído térmico:** Ocorre em função da agitação dos elétrons que geram correntes intermitentes e são em função da temperatura do ambiente. Os enlaces de comunicação ocupam apenas uma porção do espectro, sendo importante para análises a distribuição do ruído térmico em função da frequência, ou seja, a densidade de potência espectral do ruído.

Para frequências de até  $10^{12}$  Hz, a densidade espectral de ruído (watts/Hz) é aproximadamente constante. O ruído térmico pode ser caracterizado como ruído branco, pois está distribuído na frequência com o mesmo nível de potência. Para uma temperatura de 300 K a densidade espectral correspondente é de -174 dBm/Hz (MOLISCH, 2005).

**Ruído artificial:** Os ruídos artificiais podem ter níveis tão altos que podem superar o limite de sensibilidade do receptor. Fontes artificiais de ruídos podem ser provenientes de outros sistemas de comunicação operando na mesma banda de frequência, assim como de dispositivos eletrônicos com outros propósitos.

**Ruído impulsivo:** este tipo de ruído é caracterizado como um fenômeno não estacionário. O impacto do ruído impulsivo em sistemas de comunicações digitais é dependente das características do impulso, tais como potência, taxa de repetição e tempo de duração. O ruído impulsivo pode afetar diferentes estágios de um receptor causando variação da intensidade do sinal, mensagens de erro e perda de sincronização;

**Jamming:** Rádio *jamming* é um tipo de interferência deliberado para corromper comunicações. É baseado na emissão de sinais ou pulsos aleatórios, existem diferentes classificações e métodos de utilização que são detalhados no trabalho de (WENYUAN, et al., 2006). O uso de *jamming* nas comunicações resulta na diminuição da relação sinal ruído causando danos na transmissão dos dispositivos;

**Outras fontes de ruídos:** Diversos sistemas de comunicação operam em bandas não licenciadas (bandas de frequência que não apresentam custo para utilização). Muitos padrões de comunicação utilizam faixas desta banda levando à coexistência de diferentes padrões e possível interferência. As interferências também podem ocorrer fora da banda de transmissão de outros serviços de comunicação. Esse tipo de interferência ocorre em função das harmônicas de ordem elevada que podem estar sendo utilizados em uma banda de frequência



diferente, mas que produzem um segundo ou um terceiro harmônico que situa diretamente na banda de frequência de interesse.

São diversos os distúrbios que interferências podem causar em um sistema de comunicação e há uma variedade de métricas que podem ser utilizadas, tais como taxa de perda de pacotes, latência, jitter, etc., e uma série de variáveis como, por exemplo, distância entre os dispositivos, potência, taxas de transmissão, etc.), que podem ser utilizadas com as métricas de coexistência. Abaixo são citadas as definições de algumas métricas acima da camada física que podem ser utilizadas para análise de desempenho de sistemas de comunicação:

**Jitter:** representa a magnitude da variação do atraso (STALLINGS, 2007). Em aplicações de tempo real esta é uma medida importante, pois os pacotes são esperados em intervalos fixos de tempo no local de destino. Pacotes atrasados que chegam "tarde demais" são normalmente descartados para aplicações como transmissão de áudio e vídeo, bem como em aplicações que requerem uma malha de controle em laço fechado, onde pacotes atrasados podem resultar em uma resposta errônea ao sistema de controle.

**Taxa de perda de pacotes:** número de pacotes descartados na camada MAC em função de erros nos bits do pacote;

$$PLR = \frac{P_F}{P_{Tx}},$$

sendo  $P_F$  número de pacotes com falhas e  $P_{Tx}$  número de pacotes transmitidos. Esta métrica é frequentemente utilizada para avaliar condições de ruído ou interferência no meio.

**Latência:** é a quantidade de tempo que uma mensagem tem para atravessar um sistema. Em uma rede de computadores, por exemplo, é uma expressão de quanto tempo um pacote leva para ir de um ponto designado para outro. Em alguns casos é a medida do tempo necessário para que um pacote seja devolvido ao remetente. O parâmetro latência depende da velocidade do meio de transmissão (por exemplo, ondas de rádio, fios de cobre ou fibra

óptica), e também de atrasos na transmissão que podem ocorrer ao longo do caminho por meio de dispositivos (por exemplo, modems e roteadores). É uma medida fundamental de desempenho da rede e para considerações de tempo real, determinando a quantidade de tempo entre o início de uma ação e da sua conclusão. A baixa latência indica uma alta eficiência de rede.

## **2.4 PROTOCOLOS DE COMUNICAÇÃO EM 2.4 GHZ**

Definido pelo órgão ITU-R (*International Telecommunication Union – Radiocommunication*) as bandas do tipo ISM (*Industrial, Scientific and Medical*) são reservadas internacionalmente para uso com fins científico, médico, domésticos e similares. Estabelecidas primeiramente em 1947 nos Estados Unidos, algumas faixas de banda foram propostas entre elas o 2.4 GHz, inicialmente reservado para acomodar a faixa de frequência para aquecimento por micro-ondas. O interesse para o uso destas bandas tem crescido desde então principalmente para o uso em sistemas de comunicação de baixo consumo e curto alcance sendo estimuladas por diversos fatores, como a não necessidade de licenciamento o que acaba sendo um grande atrativo econômico. São muitos os padrões de comunicação como Bluetooth, ZigBee, WiFi, Bluetooth, *WirelessHART*, WIA-PA, ISA100 entre outros que operam na banda de 2.4 GHz ISM e apesar de estes sistemas apresentarem diversas diferenças (tamanho da banda, transmissão, técnicas de modulação, cabeçalhos de sincronização entre outros), podem ser elementos interferentes entre si. Neste capítulo é apresentada uma visão geral sobre alguns dos protocolos mais utilizados nesta faixa de frequência, os quais são importantes em função de coexistirem na mesma faixa de frequência que o protocolo *WirelessHART*.

### **2.4.1 IEEE 802.11**

A família IEEE 802.11 consiste em uma série de padrões que operam nas faixas de frequência de 2.4, 3.6 e 5 GHz e são utilizadas para implementação das chamadas *Wireless Local Area Network* (WLAN). Utilizado principalmente nas redes de computadores e de dispositivos móveis sendo aplicado nos mais variados ambientes desde residências, hospitais, escritórios e áreas industriais. Os padrões atualmente mais populares desta família são o IEEE 802.11b e IEEE 802.11g que são alterações do padrão original IEEE 802.11 (1997). Estes dois padrões definem um total de 14 canais de frequências, sendo cada um caracterizado por uma largura de banda de 22MHz. A Figura 4 ilustra os canais utilizados nestes dois padrões, onde também é destacado que somente três canais podem ser utilizados ao mesmo tempo sem sobreposição de canais. Como qualquer protocolo da família IEEE 802.x, o padrão 802.11 é responsável pelas camadas MAC e Física de acordo com o modelo OSI.

O padrão 802.11 suporta diferentes topologias de rede, mas a mais comum é o conjunto de serviços básicos (BSS), consistindo em um número de estações comunicando com um ponto de acesso (PA) em uma topologia do tipo estrela.

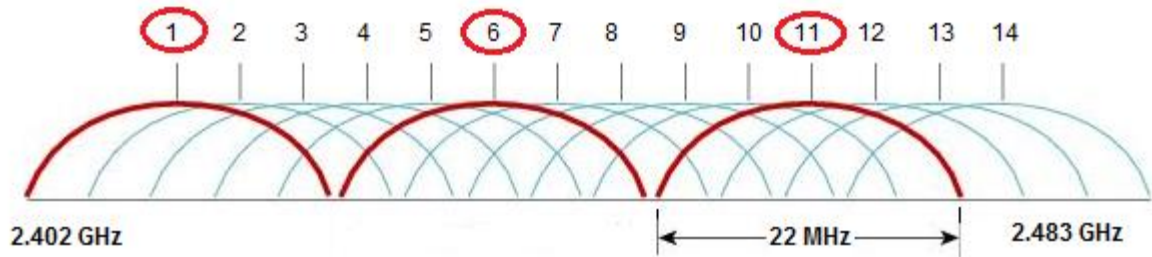
#### **2.4.1.1 IEEE 802.11b**

O padrão IEEE 802.11b também é um aperfeiçoamento do IEEE 802.11, e utiliza a faixa de frequência de 2.4 GHz ISM. Utiliza um esquema de modulação DSSS para fornecer maiores taxas de transmissão de dados. Uma taxa de dados de até 11 Mbps pode ser alcançada em condições ideais. Normalmente velocidades de 1 e 2 Mbps são utilizadas.

#### **2.4.1.2 IEEE 802.11g**

A extensão IEEE 802.11g lançada em 2003 é capaz de alcançar velocidades de 1 Mbit/s até 54 Mbit/s. A camada física utiliza o chaveamento de código complementar (CCK)

do IEEE 802.11b e modulação OFDM (*Orthogonal Frequency Division Multiplexing*) do IEEE 802.11a.



**Figura 4. Espectro utilizado protocolos IEEE 802.11 b/g.**

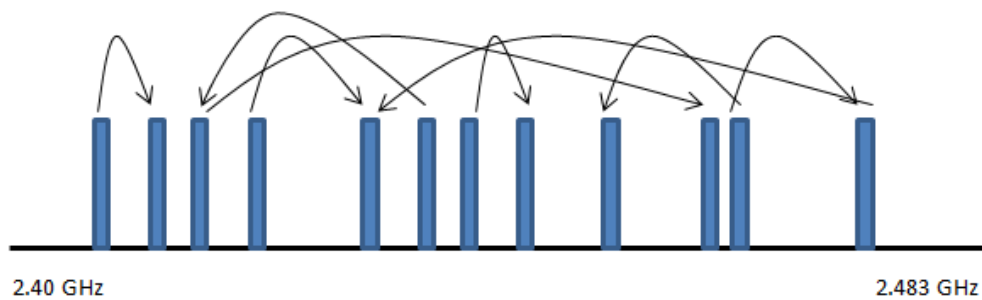
Os padrões 802.11b, o 802.11g tem integrado na camada MAC o mecanismo LBT (*Listen Before Talk*) para a transmissão de pacotes através do meio, CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Uma estação transmissora deve escutar o canal antes de transmitir o pacote, a detecção do CCA é baseada no uso da combinação da detecção de energia (ED) e sensibilidade da portadora (CS).

Para a camada física, definição de cobertura de área simplesmente não existe. Características de propagação são dinâmicas e imprevisíveis. Pequenas mudanças de posicionamento ou direção resultam em grandes diferenças na intensidade do sinal. Efeitos semelhantes ocorrem dependendo se os dispositivos são estacionários ou móveis.

#### **2.4.2 IEEE 802.15.1**

A tecnologia Bluetooth é baseada no IEEE 802.15.1 e foi desenvolvida inicialmente para uso em curtas distâncias para substituir cabos de conexão de dispositivos pessoais, como telefone, computadores, PDAs e outros dispositivos portáteis, formando as chamadas “piconets”. O padrão Bluetooth opera na banda de 2.4 GHz (2.402 – 2.483 GHz), esta faixa de frequência esta dividida em 79 canais com largura de 1 MHz. A interface com o meio é baseada em uma saída de potência de 1 mW a 100 mW dependendo da classe. A modulação

utilizada é o GFSK (*Gaussian Frequency Shift Keying*). A taxa de dados é definida em 1 Mbit/s e os canais são divididos em quadros de tempo de 625 microssegundos. A transmissão ocorre de forma que os pacotes ocupem um número ímpar de quadros de tempo (acima de 5). Cada pacote é transmitido em uma frequência diferente chegando a uma taxa de até 1600 saltos/segundo, conforme Figura 5.



**Figura 5. Salto de canais do padrão IEEE 802.15.1.**

Uma rede Bluetooth é formada por dois ou mais dispositivos, as chamadas *piconets*, um dispositivo opera como mestre e os outros (no máximo 7) operam como dispositivos escravos. Este padrão emprega o mecanismo de salto de frequência sendo o canal definido por uma única sequência pseudo aleatória de saltos fornecida pelo dispositivo mestre, os escravos da *piconet* sincronizam seus temporizadores e saltos de frequência com o dispositivo mestre após a conexão.

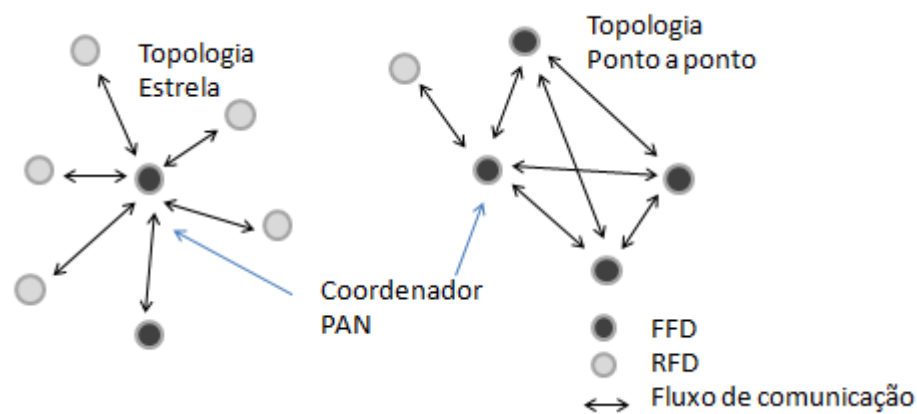
As versões mais recentes incluem salto adaptativo de canais (AFH), o qual reduz o número de canais disponíveis a partir dos 79 iniciais. Entretanto, a identificação dos canais com interferências não é especificada no padrão. O canal físico é subdividido em quadros de tempo. Os dados são transmitidos entre os dispositivos através de pacotes que são posicionados dentro destes espaços. Dependendo do tipo de pacote, é possível alocar um número consecutivo de quadros para um único pacote.

### 2.4.3 IEEE 802.15.4

O padrão IEEE 802.15.4 foi concebido para sistemas de comunicação de curta distância e baixo consumo de energia. O padrão especifica as camadas física e MAC e é utilizado como base para outros padrões tais como: ZigBee, ISA100.11A e WirelessHART. Utiliza como mecanismo de acesso ao meio o acesso múltiplo com sensoramento da portadora (CSMA-CA) e suporta diferentes topologias como, estrela e ponto a ponto. O IEEE802.15.4 inclui diferentes possibilidades de bandas de frequência:

- 868/915 MHz com modulação BPSK;
- 868/915 MHz com modulação O-QPSK;
- 868/915 MHz com modulação BPSK e ASK;
- 2450 MHz com modulação O-QPSK.

A especificação de 868/915 MHz suporta taxa de dados de 20 kb/s, 40 kb/s e opcionalmente 100 kb/s e 250 kb/s. Em 2450 MHz a taxa de dados é de 250 kb/s. Dois tipos diferentes de dispositivos podem estar presentes em uma rede: um dispositivo do tipo FFD (*Full Function Device*) ou um RFD (*Reduced Function Device*), admitindo diferentes funções em uma rede. O dispositivo FFD pode operar em três modos de operação distintos: servindo como um coordenador de uma rede pessoal (PAN), um coordenador, ou um dispositivo. Um dispositivo FFD pode comunicar-se com dispositivos RFDs e outros FFDs, enquanto um RFD pode somente comunicar-se com outro FFD. A Figura 6 ilustra as possíveis comunicações entre os diferentes dispositivos.



**Figura 6 Exemplo de redes IEEE 802.15.4.**

Existem três tipos de mecanismos para transferência de dados: de um coordenador para um dispositivo, de um dispositivo para um coordenador e entre um par de dispositivos. Os mecanismos de transmissão de dados são dependentes do suporte da rede a transmissão ou não de *beacons*. Isto determina se um dispositivo simplesmente transmite seus dados em um quadro de tempo para o coordenador ou se o dispositivo escuta o *beacon* e transmite no momento certo usando um quadro de tempo CSMA-CA. Dentro de uma rede ponto a ponto, cada dispositivo pode comunicar-se com outro dentro do alcance de transmissão usando uma das duas opções: escutando constantemente o canal ou pela sincronização com outros dispositivos transmitindo no momento determinado.

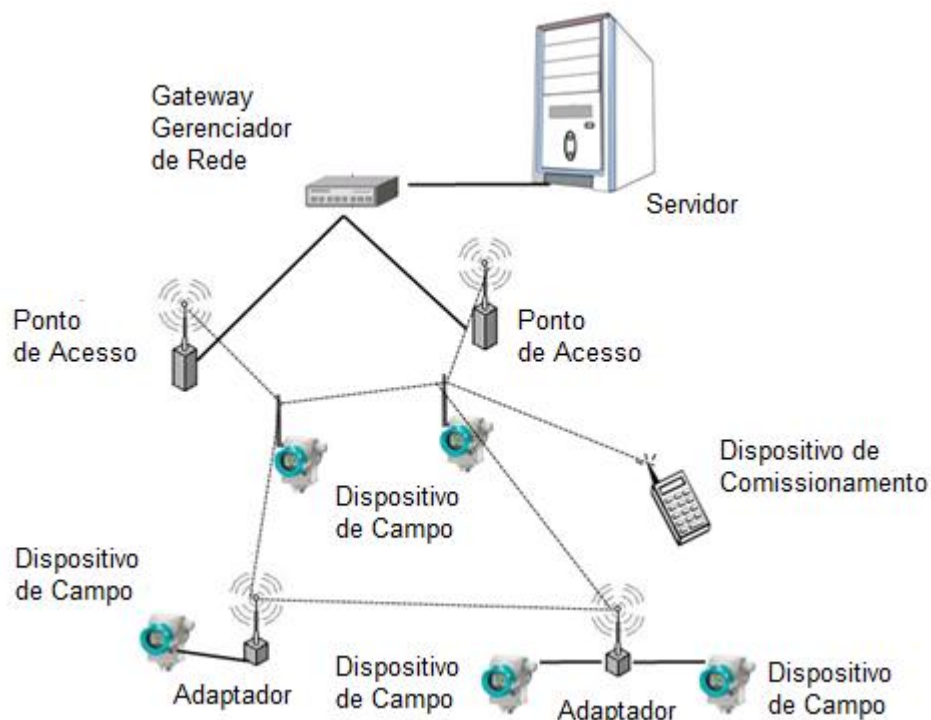
O padrão IEEE 802.15.4 utiliza somente um canal físico. Em função de o WH realizar troca de canais para cada quadro de comunicação a probabilidade de interferência é baixa entre estes dois padrões.

#### **2.4.4 WirelessHART**

O WH é o primeiro padrão aberto de comunicação sem fio certificado pela IEC para medidas e controle em processos industriais (MULLER, 2011). As aplicações são direcionadas principalmente para o uso em sensores fixos e atuadores. O WH possui uma arquitetura centralizada através de uma rede do tipo malha, apresentada na Figura 7.

A tecnologia do protocolo WH propicia uma rede segura e opera na banda de rádio de 2,4 GHz ISM. O padrão é baseado na norma IEEE 802.15.4 (camada física) com sequência direta de espalhamento do espectro (DSSS). Uma rede WH suporta uma ampla variedade de dispositivos de diversos fabricantes. Dos diversos dispositivos possíveis, são citados os principais:

- Dispositivos de campo básicos realizando funções de sensoriamento ou atuação;
- Dispositivos acessórios para roteamento, utilizados para suprir necessidades de enlace;
- Adaptador de dispositivos de campo, capazes de conectar dispositivos HART com fio à rede WH;
- Dispositivos portáteis, para comissionamento e inspeção de rede;
- Pontos de acesso, que ligam os dispositivos de campo ao gateway;
- Gerente de rede (podem ser redundantes), que criam e coordenam a rede através do gateway.



**Figura 7. Uma rede *WirelessHART* típica.**



### 2.4.4.1 WirelessHART e o Modelo OSI

A Figura 8 ilustra o padrão WH comparado às camadas do modelo OSI (*Open Systems Interconnection*). O protocolo WH compartilha a mesma camada de aplicação utilizada no padrão HART, no entanto com camada física, de enlace e rede diferentes.

Camada OSI	Função	HART	
7 Aplicação	Fornece aos usuários as aplicações da rede.	Comandos orientados. Tipos de dados pré-definidos. Procedimentos de aplicações.	
6 Apresentação	Converte dados de aplicação entre a rede e a máquina local		
5 Sessão	Conecta os serviços de gerenciamento com as aplicações.		
4 Transporte	Transfere mensagens de forma transparente e independente na rede.	Transferência de conjunto de dados. Segmentação de dados. Negociação da segmentação de dados.	
3 Rede	Roteamento dos pacotes de ponta a ponta. Endereçamento da rede.		Otimização de energia, redundância de caminhos. Auto organização da rede.
2 Enlace	Estabelece pacote da estrutura de dados. Detecção de erros.	Conexão Elétrica/mecânica, transmissão de bits.	Segurança e confiabilidade. Tempo de sincronização. TDMA/CSMA.
1 Física	Conexão Elétrica / mecânica e transmissão.	Sinal analógico e digital simultaneamente.	Wireless 2.4 GHz, baseado em rádios 802.15.4, 10dBm.

Com fio FSK/PSK e RS485                      Sem fio 2.4GHz

**Figura 8 Modelo OSI e o padrão WH. (CHEN, 2010)**

#### 2.4.4.1.1 Camada Física

Baseada no padrão IEEE 802.15.4 – 2006, utiliza banda ISM, com taxa de dados de até 250 kbit/s. Os canais são enumerados do 11 ao 26, com intervalo de 5 MHz entre dois canais adjacentes. A potência de transmissão diferentemente do IEEE 802.15.4 (0 dBm) deve ser de 10 dBm, podendo ser programada de -10 a 10 dBm.

### 2.4.4.1.2 Camada de Enlace

A camada de enlace tem como tarefa criar e gerenciar os quadros de tempo (*frames*) utilizados na comunicação, além de ser responsável pela transferência segura de dados entre os nodos da rede, detectando e corrigindo possíveis erros provenientes da camada física. Possui duas sub camadas, LLC e MAC (*Logical Link Control e Media Access Control*).

#### *Logical Link Control*

O LLC é responsável pelo controle de erros, controle de fluxo de pacotes, montagem dos quadros e endereçamento (HART COMMUNICATON FOUNDATION, 2007). É onde é especificados o formato da DLPDU. A Figura 9 ilustra a estrutura básica.

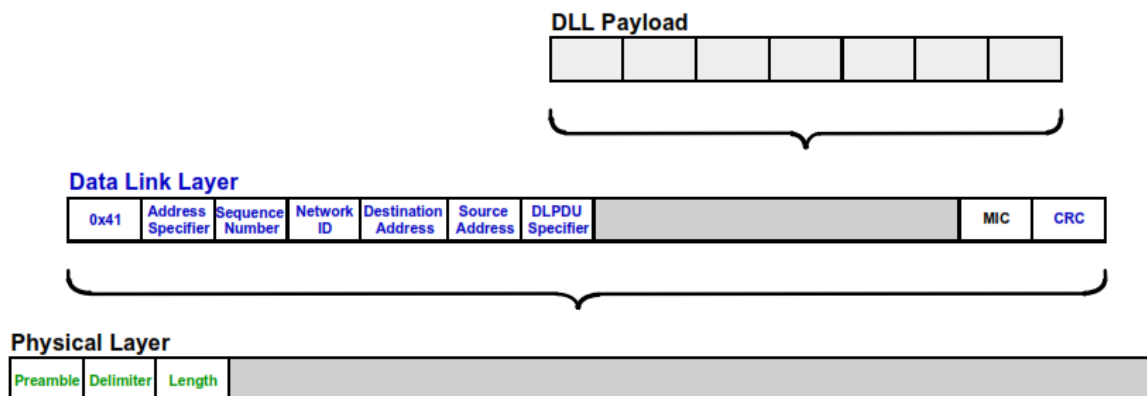


Figura 9 Estrutura da DLPDU WH. (HCF, 2008)

São cinco os tipos de DLPDU deste padrão:

**Data:** contém informação da rede e do dispositivo em trânsito para o destino do seu dispositivo final;

**Keep Alive:** responsável pela manutenção de conexão entre dispositivos vizinhos. O *payload* para este tipo de DLPDU é vazio e é utilizado para sincronização da rede e confirmação de comunicação com um dispositivo vizinho. Também na descoberta de um vizinho, o dispositivo deve emitir periodicamente DLPDUs do tipo *Keep Alive*;

**Advertise:** fornece informação para os dispositivos vizinhos que podem agregar-se à rede. É utilizado para convidar novos dispositivos a associarem-se na rede. Quando um dispositivo deseja associar-se a rede ele checa por este tipo de DLPDU e usa as informações no *payload* para sincronizar-se com a rede e iniciar o processo de associação;

**Disconnect:** o DLPDU de desconexão é gerado por um dispositivo que está deixando a rede. Implica que o dispositivo não estará mais disponível para comunicação e pode ser removido da lista de vizinhos. Todas as conexões estabelecidas com os vizinhos deste dispositivo são deletadas. Para uma DLPDU do tipo *disconnect* o *payload* está vazio;

**ACK:** representa a resposta de nível imediato para receber transmissões DLPDU de outras fontes. O ACK contém o código de resposta que indica se o dispositivo receptor aceitou a DLPDU.

Há quatro níveis de prioridade no DLPDU das mensagens, abaixo eles são apresentados em ordem de maior prioridade:

**Comando:** Nível de prioridade mais alta. No tipo comando, qualquer pacote contendo dados relacionados a diagnóstico, configuração, ou controle de informação deve ser classificado como prioridade de comando.

**Dados de Processo:** Pacotes contendo dados como, comandos 3 e 9, ou estatísticas da rede, comandos 779 e 780 por exemplo, devem ser classificados com nível de prioridade Dados de Processo. Somente o gerenciamento da rede (indicado com prioridade de Comando) é mais importante do que a entrega dos valores das variáveis de processo ou parâmetros de ajustes de dispositivos. Pacotes com nível de prioridade Dados de Processo devem ser negados de outros dispositivos quando três quartos do buffer do dispositivo está ocupado.

**Normal:** Os pacotes que não estão nos critérios citados (Comando, Dados de Processo ou Alarme), devem ser classificados com nível de prioridade Normal. Pacotes neste nível de

prioridade devem ser negados por outros dispositivos quando metade da memória do dispositivo está ocupada.

**Alarme:** Pacotes contêm apenas informações de alarme. Dispositivos não devem armazenar mais de um pacote com este nível de prioridade. Alarme é o tipo de menor prioridade.

Como existe a possibilidade de agregar múltiplos comandos em um único pacote, o DLPDU deve assumir a prioridade mais alta das mensagens dentro das mensagens agregadas.

### **MAC**

Referente à camada de Controle de Acesso ao Meio (MAC), uma política híbrida é adotada baseada em Acesso ao Meio por Divisão do Tempo (TDMA) e Acesso Múltiplo por Sensoriamento da Portadora (CSMA). A camada MAC é responsável por manter o sincronismo dos quadros de tempo, identificar os quadros de tempo que necessitam de serviços, escutar pacotes que estão sendo enviados pelos vizinhos e encaminhar os pacotes que vem da camada de rede (RAPPAPORT, 1996). Fundamentalmente a subcamada MAC é responsável pela propagação das DLPDUs através das conexões. Para realizar esta função o dispositivo deve possuir:

- Tabelas de vizinhos, superframes, links e grafos que configuram a comunicação entre o dispositivo e seus vizinhos. Estas tabelas são preenchidas pelo Gerenciador de Rede;
- Um escalonador de conexões que avalia a tabela de dispositivos e escolhe o próximo *slot* de tempo para ser usado na recepção e envio de um pacote.

#### **2.4.4.1.3 Camada de Rede**

A camada de rede e a camada de transporte cooperam para fornecer de forma segura e confiável comunicação de ponta a ponta para os dispositivos da rede. É onde os pacotes recebidos pelos serviços da camada de enlace são transferidos para os dispositivos e os

pacotes roteados de outros dispositivos são enviados para a camada de enlace, além de processar os pacotes recebidos da camada de aplicação.

No modelo de protocolo de 7 camadas OSI, a camada de rede é a responsável pelas funções de roteamento de rede designando o endereçamento e entrega dos dados. A camada de transporte controla a confiabilidade e tempo de transmissão dos dados entre os nós da rede através de controle de fluxo, segmentação ou separação, e o controle de erro. A camada de sessão controla o diálogo, a sessão, e conexões entre dois nós da rede. No padrão WH a camada de rede engloba todas estas três camadas. É neste ponto que ambas as versões, sem fio baseadas em TDMA e com fio HART *Token-Passing*, começam a assemelhar-se (HCF, 2007).

#### 2.4.4.1.4 Camada de Aplicação

A camada de aplicação é a mesma que é usada pelo protocolo HART, porém com comandos adequados para as novas funcionalidades da comunicação sem fio. A camada de aplicação é responsável pelo gerenciamento dos comandos utilizados. Através desta camada o usuário final pode acessar informações da rede. Os comandos são distribuídos em seis grupos que são Universal, Práticos, Família de Dispositivos, Funções Específicas e Comandos sem fio. Na tabela 1, estão listados os comandos pertencentes à categoria de coexistência do protocolo.

**Tabela 1 Comandos do WH relacionados ao compartilhamento do espectro de frequência**

	<b>Comando</b>	<b>Descrição</b>
<b>Coexistência</b>	804	Ler modo CCA
	805	Escrever modo CCA
	817	Ler lista negra dos canais
	818	Escrever lista negra dos canais

### **3 MECANISMOS DE COEXISTÊNCIA DO WIRELESSHART**

O protocolo WH introduz uma série de mecanismos que aumentam sua confiabilidade na coexistência com outras possíveis fontes de interferência. Estes mecanismos são estudados e detalhados abaixo. Com exceção do CCA, podem ser classificados como soluções inerentes ao protocolo, uma vez que atuam independente da ocorrência de interferência.

#### **3.1 ACESSO AO MEIO**

O protocolo WH utiliza um esquema de acesso ao meio TDMA e CSMA-CA. Através do acesso ao meio com TDMA, o canal de comunicação é particionado em intervalos de tempo. Cada dispositivo utiliza o canal de comunicação durante certa porção de tempo. Os quadros de tempo para a comunicação são agendados e distribuídos para cada dispositivo da rede. Normalmente somente um dispositivo é configurado para transmitir em um quadro de tempo. Esta estratégia mantém o tráfego em condição constante e também garante uma baixa latência na rede, resolve o problema do nodo escondido e evita colisões de pacotes na comunicação entre os dispositivos de uma mesma rede WH. O WH também possui quadros de tempo compartilhados, os quais, múltiplos dispositivos podem transmitir e outro dispositivo receber, neste caso a colisão é detectada após a transmissão pelo não recebimento da confirmação de entrega, quando isto ocorre os dispositivos que não confirmaram a entrega da mensagem tentam reenviar através de outro quadro de tempo determinado por um tempo aleatório.

Um dos pontos negativos destes mecanismos advém da utilização de uma arquitetura centralizada o que traz como desvantagem uma baixa dinamicidade nas alterações que ocorrem na rede, além da acuracidade necessária no dispositivo para manter-se sincronizado na rede.

### 3.2 MODULAÇÃO

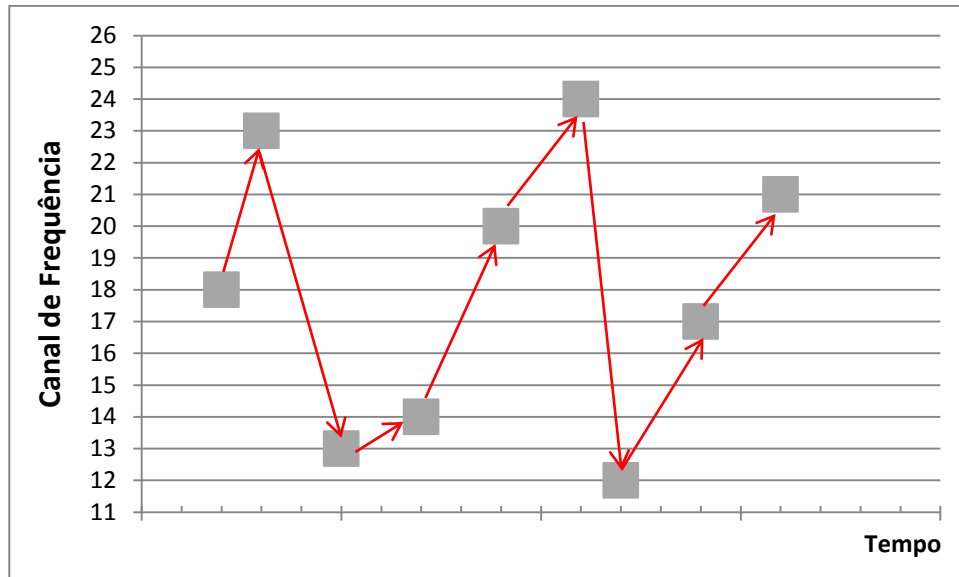
A camada física especificada para este padrão utiliza um esquema de modulação quasi-ortogonal, em que cada símbolo é representado por uma das 16 sequências de quase ortogonais PN (*pseudo-random noise*). Este é um método de modulação de potência eficiente que consegue uma relação baixa de sinal ruído (*SNR*) e da relação sinal interferência (*SIR*) requisitos em detrimento de uma largura de banda do sinal que é significativamente maior do que a velocidade de símbolo. A norma do IEEE 802.15.4 estima para um detector típico de baixo custo uma taxa de erros de pacotes de 1% (*PER*) para valores do *SNR* entre 5 a 6 dB.

### 3.3 SALTO DE CANAIS

O salto de frequência dos canais utilizados é um dos métodos de difusão do espectro, trocando o canal da frequência para cada quadro de tempo utilizado. Cada dispositivo contém uma tabela de canais o qual é passada no início da formação da rede. O canal a ser utilizado é determinado durante a operação da rede e é dado pela seguinte equação:

$$\text{Canal atual} = (\text{Deslocamento do Canal} + \text{ASN}) \% \text{Número de canais} \quad (7)$$

O *ASN* (*Absolute Slot Number*) é um valor absoluto na rede o qual é incrementado a cada transação da comunicação, ou seja, para um determinado deslocamento de canal (que é um atributo de cada conexão) os quadros de tempo devem ocorrer em diferentes frequências, vide Figura 10. Este mecanismo de diversidade de canais aumenta a confiabilidade da rede, pois além de reduzir possibilidade interferência de outros protocolos ou fontes interferentes reduz os efeitos de interferência do próprio protocolo WH, como pelos efeitos de desvanecimento por multi caminhos.



**Figura 10 Exemplo de salto de canais**

### 3.4 CCA – CLEAR CHANNEL ASSESSMENT

O WH também é provido com o mecanismo de CCA que é desempenhado antes da transmissão da mensagem pelo dispositivo fonte, o dispositivo receptor não utiliza o CCA antes de enviar a confirmação do recebimento. O CCA pode ser desempenhado através de uma das três maneiras que a norma (IEEE 802.15.4, 2006) apresenta:

**Modo 1:** Energia acima do limiar. CCA deve reportar um meio ocupado após detectar qualquer energia acima do nível limite. No WH este limite está configurado em -85dBm;

**Modo 2:** Sensibilidade da portadora somente. Neste modo CCA deve reportar um meio ocupado somente após a detecção de um sinal compatível com este padrão (mesma modulação e características de espalhamento da camada física) que está atualmente em uso pelo dispositivo. O sinal pode estar acima ou abaixo do limiar de energia.

**Modo 3:** Sensibilidade da portadora com energia acima do limiar. CCA deve reportar um meio ocupado usando uma combinação lógica da:

- Detecção de um sinal com modulação e características de espalhamento deste padrão;

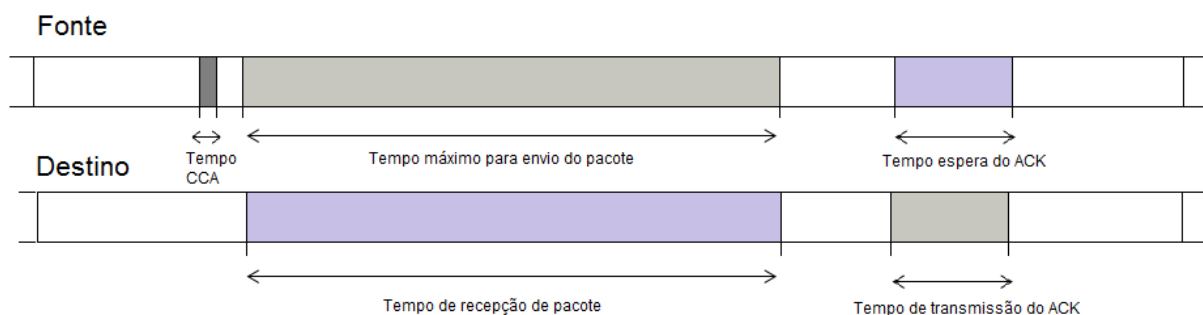


- Nível de energia acima do limiar.

Os parâmetros do CCA seguem os seguintes critérios:

- O limiar da energia detectada deve corresponder para um sinal de potência recebida de no máximo 10 dB acima da sensibilidade especificada do receptor (no WH isso corresponde a -75 dBm);
- O tempo de detecção do CCA deve ser igual a 8 períodos de símbolos.

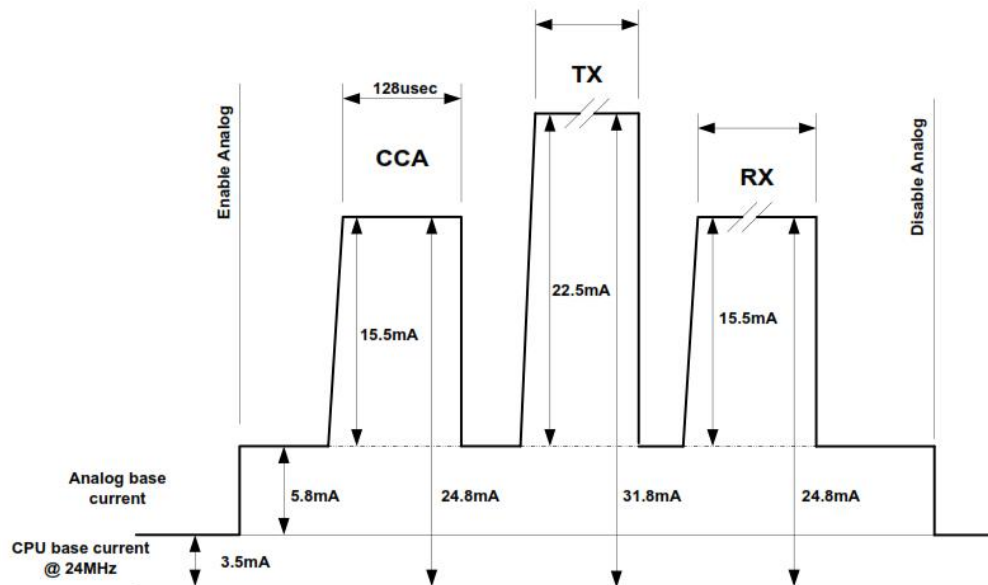
Quanto ao uso do CCA o protocolo WH utiliza o modo 2 de detecção, ou seja, sensibilidade da portadora somente. A Figura 11 ilustra o *slot* de transmissão e recepção do pacote indicando o instante no qual o CCA é ativado. O modo 2 ou detecção de preâmbulo pode tornar mais eficiente à sensibilidade, mas impede que sejam identificados coexistência com tecnologias diferentes de comunicação, sendo um mecanismo com eficácia somente para protocolos com mesma modulação que o IEEE 802.15.4. No WH ainda há a possibilidade de desabilitar o CCA através do comando 805 do protocolo, mas mesmo desabilitado o dispositivo ainda deve respeitar o tempo de CCA e transmitir apenas no tempo designado para a transmissão.



**Figura 11 . Tempo do *slot*. (Adaptado de CHEN, 2010).**

Para esta análise, é possível optar por não deixar o CCA desabilitado em caso de coexistência com uma segunda rede WH ou outra rede baseada no IEEE 802.15.4. Dependendo da plataforma do rádio utilizada, o CCA desabilitado pode representar menor consumo de energia, pois representa uma mudança de estado a menos no modem do rádio

para cada transmissão de pacote, um importante aspecto a ser considerado uma vez que os dispositivos são energizados por meio de baterias. A Figura 12 ilustra o consumo de corrente para a ativação dos diferentes modos de operação de uma plataforma que incorpora um transceptor de 2.4 GHz para uso com o padrão IEEE 802.15.4. O tempo de duração do CCA é determinado no padrão IEEE 802.15.4 e tem duração de 8 símbolos (128  $\mu$ s).



**Figura 12 Modos de operação versus consumo de corrente de um transceptor típico IEEE 802.15.4. (FREESCALE, 2012)**

### 3.5 LISTA PROIBIDA DE CANAIS

O padrão WH introduz o conceito de “lista negra” de canais (*channel black list*), permitindo que alguns canais possam ser retirados dos canais utilizados na rede. Esta opção permite uma rejeição de interferência para redes estacionárias ou de banda estreita. A lista negra pode trazer benefícios em soluções de comunicação WH em relação a interferências permanentes como, por exemplo, redes do tipo WLAN que podem ser evitadas, uma vez que a banda do WH é relativamente estreita. Sendo possível evitar situações paradoxas nas quais o desempenho de uma rede tradicional IEEE 802.15.4, que utiliza um único canal afastado de

uma fonte de frequência estacionária interferente, tenha um desempenho melhor do que uma rede WH, que periodicamente cruza a região desta frequência (DOMINICIS, et al., 2009).

Um aspecto importante deste mecanismo é o fato de ser necessário o ajuste da seleção de canais por parte do planejador da rede, não sendo um mecanismo auto adaptativo. Um ponto negativo ainda é o fato da necessidade de reiniciar a rede para cada nova lista de canais, uma vez que o mapa de canais é transmitido apenas no momento de associação do dispositivo à rede e então utilizado para determinar os saltos de canais.

### **3.6 DSSS**

O objetivo de espalhar o espectro é transmitir o sinal além da largura de banda, usando mais frequências e menos potência por frequência. Um método de espalhamento de frequência largamente utilizado é o DSSS (*Direct Spread Spectrum Sequence*). No WH o DSSS é aplicado para cada mensagem transmitida e ao invés de realizar o espalhamento sobre os 16 canais, divide cada canal em sub canais onde os dados são espalhados.

No caso do DSSS a possibilidade de coexistência é aumentada no sentido de rede interferente, neste caso mitigando a interferência em outros padrões enquanto o salto de canais é utilizado como mecanismo de defesa para outras interferências. Ambos os mecanismos ganham maior destaque para mitigar interferências temporárias.

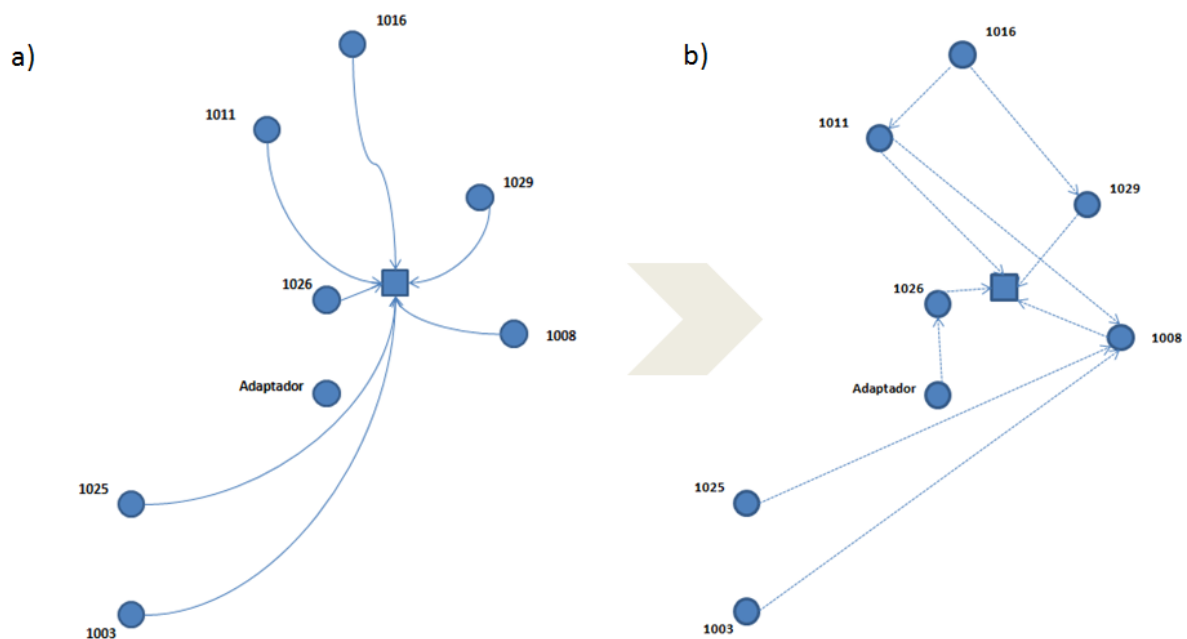
### **3.7 REDE DO TIPO MALHA**

A rede do tipo malha também deve ser considerada uma característica que torna o protocolo mais robusto às condições de coexistência, uma vez que utiliza rotas redundantes para o envio das mensagens. O padrão WH requer que cada dispositivo de campo seja capaz de fazer o roteamento das mensagens.

As mensagens podem mover-se através de dispositivos intermediários sendo que cada movimento de um pacote de um dispositivo para outro ao longo da rota para o dispositivo de

destino final é chamado de salto (*hop*). A latência da rede deve aumentar a medida que o dispositivo apresenta maior número de saltos para o destino final da mensagem (FERRARI, et al., 2012) .

A Figura 13 ilustra um exemplo de uma rede WH montada em laboratório. Neste exemplo as conexões entre os diversos dispositivos foram avaliadas. A partir dos dados coletados durante a operação neste cenário foi analisado a dinâmica de encaminhamento de pacotes entre os diversos dispositivos. A Figura 13-a identifica as rotas diretas para o gateway da rede e na Figura 13-b estão em destaque as rotas alternativas utilizadas pelos dispositivos para encaminhamento de mensagens. Durante o ensaio são observados envios de mensagens através de dispositivos intermediários bem como envios diretos para o gateway.



**Figura 13 Rede tipo malha: a) rotas diretas para o gateway; b) rotas alternativas.**

Esta é uma importante característica de confiabilidade da rede WH, pois uma vez que o enlace entre dois dispositivos não possui uma relação sinal ruído suficiente para garantir a entrega da mensagem o protocolo em nível lógico encaminha a mensagem por outra conexão

que pode ter uma relação sinal ruído melhor em função de estar fora da zona de interferência ou mesmo mais próximo do dispositivo fonte.

### **3.8 BAIXO CICLO DE TRABALHO**

A especificação do IEEE 802.15.4 é mais apropriada para aplicações com baixo consumo de potência e baixas taxas de transmissão (250kb/s e 20kb/s). Aplicações típicas do IEEE 802.15.4 são especificadas para rodar com baixos ciclos de operação (menos que 1%). Desta forma também se diminui a probabilidade de colisão de pacotes uma vez que a demanda da rede é baixa causando menos interferências em outros padrões, além da questão de reduzir o consumo da bateria.

## **4 ANÁLISE DO ESTADO DA ARTE EM ESTUDOS SOBRE COEXISTÊNCIA DE REDES SEM FIO**

Para o desenvolvimento desta pesquisa foram revisados diversos trabalhos relacionados ao tema. Para o estudo dos diferentes parâmetros relacionados à coexistência de redes de comunicação sem fio, existem diferentes possíveis cenários que podem ser estudados. Os trabalhos relacionados ao estudo de coexistência em comunicação sem fio podem ser em geral classificados em pelo menos três categorias: análise, simulação ou medições experimentais, todos sempre com o objetivo de quantificar medidas de desempenho das redes (GOLMIE, 2006). Estas categorias serão utilizadas nas seções que seguem.

### **4.1 MODELAGEM MATEMÁTICA**

Os resultados analíticos são baseados em modelos matemáticos de colisão de pacotes por diferentes transmissores e receptores correspondendo a resultados em função de uma probabilidade de erro de pacotes. Diferentes parâmetros são utilizados, tais como, número de transmissores, distância entre dispositivos, potência entre outros.

Diversos trabalhos estão dentro desta categoria, como em (HAN, et al., 2007) em que foi modelado um cenário para coexistência dos padrões IEEE 802.15.4 e IEEE 802.11b. A métrica utilizada foi a probabilidade de erro de pacote. Os resultados numéricos demonstram que interferências do IEEE 802.11b no IEEE 802.15.4 causam redução de capacidade no sistema proporcional ao deslocamento da frequência ocupada em relação aos dois padrões. O estudo verificou a ocorrência de uma degradação maior no desempenho do IEEE 802.15.4 para uma distância inferior a 11 MHz entre os canais utilizados pelos dois padrões. Foram propostos dois algoritmos para seleção de canais, baseados na detecção de energia, com o objetivo de minimizar a interferência causada do IEEE 802.11b no IEEE 802.15.4 em relação à sobreposição de canais. Resultados demonstram que uma seleção apropriada de canais pode

reduzir o impacto de interferência. O padrão WH não utiliza nenhum algoritmo de seleção de canais, no entanto, tem incorporado no protocolo o salto de canais para cada pacote transmitido diferentemente do IEEE 802.15.4 que utiliza apenas um canal fixo.

No trabalho de (YUAN, et al., 2007) é apresentado um modelo de interferência do padrão IEEE 802.11g no IEEE 802.15.4. O modelo concentra-se em dois aspectos, potência e tempo. As situações de coexistência são classificadas para diferentes distâncias (2 a 5 m) e são obtidas probabilidades de colisão considerando os mecanismos de CSMA/CA para ambos os padrões, evitando assim a sobreposição de canais. Assim como os resultados dos modelos anteriores, este trabalho também demonstra a redução no desempenho do IEEE 802.15.4 sob condições de coexistência.

O trabalho de (HUO, et al., 2009) examina a interferência mútua em dispositivos com o IEEE 802.15.4 através de uma análise teórica. O modelo proposto examina a taxa de perda de pacotes contra dispositivos com Bluetooth, IEEE 802.11b e os efeitos da radiação de fornos do tipo micro-ondas que também utilizam a banda de 2.4 GHz. Neste trabalho é determinado um parâmetro  $dr/ds$ , onde  $ds$  é a distância entre os dispositivos IEEE 802.15.4 e  $dr$  é a distância dos dispositivos interferentes. Os resultados demonstram que a interferência por Bluetooth tem um impacto menos significativo chegando a perdas de 4% para um  $dr/ds > 2$  metros. Já os efeitos do forno micro-ondas pode ser tolerado para distâncias superiores a 1,5 m chegando a perdas de até 8%, mas para uma distância de 0,5 metros as perdas podem ser superiores a 50 %. A interferência com redes IEEE 802.11b são mais severas chegando a perdas superiores a 60% no caso de interferência por co-canal.. Calcula-se que uma transmissão confiável sob a interferência do IEEE 802.11 deve ocorrer quando a relação  $dr/ds$  é maior que 6 e o deslocamento da frequência da banda de ocupação dos elementos interferentes em relação ao IEEE 802.15.4 é entre 0 e 11 MHz, enquanto para um

deslocamento de frequência entre 11 e 22 MHz a relação  $dr/ds$  é reduzida para até 2 metros de distância.

O trabalho de (CHEN, et al., 2006) é estuda a coexistência entre diferentes protocolos baseados na família do IEEE 802.15 através de modelos analíticos. Resultados demonstram que ocorrem conflitos em todos os casos quando o meio é compartilhado entre as diferentes tecnologias deste padrão. O caso mais severo ocorreu entre às redes do IEEE 802.15.3 e IEEE 802.15.4, enquanto a coexistência entre o IEEE 802.15.1 e IEEE 802.15.4 apresentou um resultado de interferência menos significativo.

Os modelos analíticos geralmente são simplificados devido à dificuldade de incluir as diversas variáveis relacionadas aos fenômenos ligados à propagação. Os resultados são úteis para uma aproximação inicial do desempenho e degradação da rede. No entanto, estes modelos frequentemente utilizam considerações relacionadas à distribuição de tráfego e à operação do protocolo de controle de acesso ao meio o que pode tornar os resultados menos realísticos. Ainda, para uma análise ser tratável, considerações sobre mudanças de tráfego em função de interferências são frequentemente ignoradas.

#### **4.2 ANÁLISE DE COEXISTÊNCIA BASEADO EM SIMULAÇÕES**

Os modelos de simulações são uma alternativa de baixo custo, sendo obtidas através de simulações em computadores com o objetivo de modelar o comportamento de um determinado protocolo sob diferentes cenários, sendo provavelmente o método mais utilizado.

Alguns trabalhos têm avaliado a perturbação em redes de 2.4 GHz por meio de simuladores como em (DOMINICS et al., 2009) em que foi desenvolvido um simulador, (somente utilizando as camadas PHY e MAC) para investigar a coexistência da rede WH, mais especificamente as diferenças de desempenho entre uma rede tradicional de IEEE 802.15.4 e uma rede WH contra uma rede do padrão IEEE 802.11. Os ensaios utilizaram uma



rede WH composta por três dispositivos e duas estações para a WLAN, sendo os dispositivos WH distribuídos em torno do ponto de acesso por uma distância com aproximadamente 2 metros de raio. A principal métrica utilizada é a taxa de erro de pacotes, sendo considerada uma colisão cada coincidência temporal durante a utilização de uma mesma faixa de frequência. Os resultados mostram que o protocolo WH apresenta um desempenho melhor do que uma tradicional rede de sensores sem fio IEEE 802.15.4. Outros pontos que devem ser considerados é a falta de detalhamento das condições de um cenário real não considerando, por exemplo, os efeitos de canais adjacentes, como demonstrado em (PETROVA, et al., 2006) que realizou uma análise entre os padrões IEEE 802.15.4 e IEEE 802.11. Os dispositivos utilizados foram dispostos dentro de um raio de 2,5 m e os ensaios foram realizados com variação nos tamanhos dos pacotes e diferentes distâncias entre as frequências dos canais dos protocolos. Resultados demonstraram que ocorrem perdas mais significativas no IEEE 802.15.4 quando a distância entre as frequências centrais são menores do que 7 MHz.

O trabalho de (BERTOCCO, et al., 2008) apresenta um modelo de simulador para análise dos fenômenos de interferência entre os padrões IEEE 802.15.4 e IEEE 802.11. neste trabalho é utilizado a plataforma de simulação OMNet++. Ambos os padrões são implementados em módulos independentes e um terceiro módulo é utilizado e identificado como módulo interferente com a função de realizar o registro das colisões temporais. O ambiente simula uma rede IEEE 802.15.4 com cinco dispositivos e um ponto de acesso IEEE 802.11b dentro de um raio de dois metros, a estação receptora encontra-se afastada por uma distância aproximada de doze metros. Para o modelo de propagação livre foram medidas as perdas de pacote do IEEE 802.15.4 com variação do ciclo de trabalho e tamanho de pacotes (600 e 1112 bytes) da rede IEEE 802.11b. Os resultados demonstram perdas maiores do que 20% para ciclos de trabalho superiores a 75% e não demonstra diferenças significativas nas perdas para os diferentes tamanhos de pacotes utilizados.

No trabalho de (NOBRE, et al., 2011) é construído um módulo da camada física do WH utilizando o Simulador de Rede NS-3. No modelo é considerado as características do dispositivo de transmissão (potência de transmissão, detecção de sinal e mobilidade), assim como as características do acesso ao meio, tais como o uso dos 15 canais suportados pelo protocolo, o modelo de perda por propagação e erro. Considerando o modelo de propagação livre a taxa de perda de pacotes foi mensurada para pacotes de 6, 9, 18, 90 e 133 bytes, sendo aproximadamente de 1,3%, 1,4%, 1,6%, 2,4% e 3,2% respectivamente. A norma IEEE 802.15.4-2006 também apresenta simulações referente ao desempenho deste padrão em relação à interferência de outros padrões. Os resultados demonstram taxa de perda de pacotes em função da distância e do deslocamento de frequência, no pior caso apresentado deslocamento de 3 MHz, distância inferior à 10 metros, e resultando em uma perda de 1%.

Apesar dos modelos de simulação caracterizarem-se pela grande flexibilidade (número indeterminado de ensaios, fácil alteração de parâmetros das variáveis, etc.), ainda carecem de considerações reais, tais como os efeitos de propagação das ondas de rádio frequência as quais são normalmente simplificadas, no entanto, ainda é o meio mais utilizado para estimar o comportamento e desempenho dos protocolos de comunicação.

### **4.3 ANÁLISE EXPERIMENTAL**

Na terceira situação, os resultados obtidos através de medições experimentais são considerados os mais precisos, porém podem ser muito específicos para a aplicação testada. Experimentos reais podem ser muito informativos contendo todas variáveis de uma aplicação real. Uma dificuldade normalmente encontrada é a falta de acesso aos detalhes de implementação geralmente restritos pelos fabricantes levando a impossibilidade de variação de parâmetros e coleta de dados confiáveis.

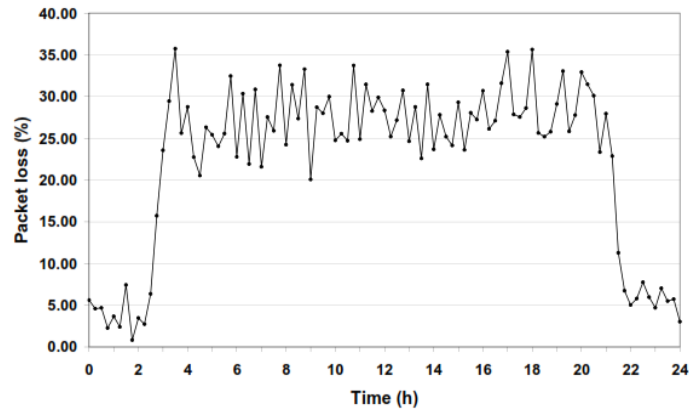
No trabalho de (ANGRISANI, et al., 2008) é apresentado um estudo experimental para identificar problemas relacionados a coexistência entre redes do tipo IEEE 802.11b e IEEE 802.15.4. Os experimentos são baseados na taxa de perda de pacotes, tratando os casos em que a rede WSN é a vítima da rede WLAN e o contrário. O cenário utilizou sobreposição dos canais, sendo utilizados canal 11 e o 22 para IEEE 802.11 e IEEE 802.15.4 respectivamente. Resultados mostram que sob a presença de interferência a rede de sensores (IEEE 802.15.4) pode ter uma taxa de perda de pacotes superior a 50%. Outra conclusão significativa deste estudo refere-se ao efeito predominante da interferência ser de uma rede IEEE 802.11 sobre a rede de sensores sem fio IEEE 802.15.4 e a identificação dos parâmetros que mostraram ser mais significativos para a coexistência de ambos os protocolos, neste caso, a taxa de ocupação da banda e o tamanho do pacote do IEEE 802.11.

O trabalho (SUBBU, et al., 2007) apresenta uma análise da relação da taxa de erro de pacotes com o sinal de interferência e o efeito do deslocamento da frequência. O estudo foi baseado na avaliação de taxa de erros nos pacotes na transmissão do IEEE 802.15.4 com interferência de transmissão também com o IEEE 802.15.4. A coexistência entre dispositivos IEEE 802.15.4 foi avaliada através de estudos empíricos para estimar o PER sob diferentes condições de operação. Entre as condições de operação estão incluídas variação da relação de sinal de interferência (SIR) e a frequência de deslocamento (*offset*) entre o sinal desejado e a frequência do sinal de interferência. Um aspecto interessante deste trabalho deve-se ao fato do cenário de teste possuir o meio controlado através de cabos e atenuadores de potência permitindo uma avaliação do desempenho da rede sem variação descontrolada dos fenômenos de propagação de RF. Resultados demonstram que a partir de um deslocamento de frequência de 15 MHz não há mudanças substanciais na relação sinal interferência (SIR). Ainda outro dado importante refere-se ao tamanho do pacote transmitido, à medida que o tamanho dos pacotes desejados é reduzido (123, 66 e 9 bytes), o SIR necessário para manter o mesmo PER

diminui, ou seja, um aumento da potência de interferência é necessário. Menos bits dentro de um pacote diminui a probabilidade deste ser corrompido por um pacote interferente.

Em (PETERSEN et al., 2007), experimentos foram realizados em um laboratório de pesquisa de uma empresa do ramo de óleo e gás (Statoil ASA, Noruega), onde havia réplicas de equipamentos em tamanho real usuais em plantas industriais, tais como motores, vasos e tanques de aço. Neste cenário foram realizados experimentos para testar o desempenho de uma rede de nós sensores de dois fabricantes distintos utilizando o IEEE 802.15.4 contra uma rede IEEE 802.11b com os canais 1, 6 e 11 sendo utilizados e uma ocupação da banda de frequência em 50%. O gateway e o ponto de acesso foram colocados em uma área com raio de 1 metro. As estatísticas da rede demonstraram que a interferência do IEEE 802.11b aumentou a latência da rede em 20 % para o pior caso registrado, forçando retransmissões e diminuindo a estabilidade, mas mantendo o nível de confiabilidade em 100%.

No trabalho de (PETERSEN, et al., 2009) uma rede WH foi testada utilizando 9 nodos e 1 gateway sob condição de coexistência com o padrão IEEE 802.11. Neste trabalho três canais foram utilizados simultaneamente (1,6 e 11), deixando apenas 3 canais WH livres de interferência. No pior caso, foram observados uma média de perda de pacotes de 27% aproximadamente dentro do período que foi inserido interferência na rede WH, ver Figura 14, na condição de um ciclo de trabalho de 4%. Outra situação empregada foi a geração de interferência por meio de um *chirp jamming* com uma distância inferior à 1 metro do gateway WH, transmitindo ruído em períodos de 10 ms. Neste cenário a rede WH apresentou total degradação, não havendo nenhuma recepção de dados no gateway e resultando em uma confiabilidade de 0%. Este último cenário é improvável dentro de um cenário real, concorrendo com outro padrão, no entanto este resultado é importante para uso contra ataques maliciosos. Este é o único trabalho encontrado utilizando avaliação de desempenho de uma rede WH real até o fim do período desta pesquisa.



**Figura 14** Perda de pacotes de uma rede WH sob interferência IEEE 802.11 entre 3 e 22 horas.

A literatura apresenta muitas pesquisas e resultados envolvendo a análise de alguns parâmetros relacionados ao desempenho de redes IEEE 802.15.4 em relação a outros padrões que operam na mesma faixa de frequência. Os resultados de desempenho são variados, isso se deve principalmente à dificuldade de caracterizar nos modelos de testes utilizados todos os parâmetros envolvidos em um sistema de comunicação sem fio. Até o presente momento apenas poucos trabalhos relacionados especificamente com o protocolo WH foram encontrados. No estudo do protocolo WH ainda são poucos os trabalhos consistentes que realizam análise de coexistência dentro da proposta de cenários reais e apesar do protocolo WH ter sua camada física baseada no IEEE 802.15.4 existem diferenças significativas que influenciam no desempenho da rede e carecem de estudo. A Tabela 2 apresenta um resumo de experimentos realizados avaliando o desempenho de protocolo baseados no IEEE 802.15.4 contra outros protocolos que utilizam a mesma faixa do espectro de frequência.

**Tabela 2** Trabalhos relacionados

Cenário	Ambiente	Conclusões	Referência
IEEE 802.15.4 x IEEE 802.11b	Modelo de coexistência utilizando sobreposição de canais IEEE 802.15.4 (0 dBm), IEEE 802.11b (14 dBm)	1) IEEE 802.11b reduz a capacidade do IEEE 802.15.4; 2) Mecanismos de seleção de canais reduz a vulnerabilidade do IEEE 802.15.4; 3) Interferência do IEEE 802.11b diminui proporcionalmente com o aumento do deslocamento de frequência.	HAN, et al., 2007

Cenário	Ambiente	Conclusões	Referencia
(WH, IEEE 802.15.4) x IEEE 802.11b	WH 0-1,8 dBm IEEE 802.15.4 0 dBm WLAN 15 dBm operação: 40 - 100% Distancia entre os nodos: raio de 2 m	1) Perda de pacotes é menor no WH do que no IEEE 802.15.4 2) Diferença de desempenho atribuída ao salto de canais do WH.	DOMINICS, et al., 2009
IEEE 802.15.4 x IEEE 802.11b	32 m de distância entre transmissor e receptor, pacotes de 20, 40, 80 e 127 bytes. Taxa de 20 pacotes/s	1) IEEE 802.11 não tem influencia negativa sob IEEE 802.15.4, desde que tenha um deslocamento de frequência superior a 7 MHz; 2) IEEE 802.15.4 tem mais perdas do que o IEEE 802.11	PETROVA, et al. 2006
IEEE 802.15.4 x IEEE 802.11b	OMNET++; 5 dispositivos IEEE 802.15.4 com elemento interferente IEEE 802.11 em um raio de 2 m.	1) IEEE 802.15.4 apresenta uma taxa de perda de pacotes superior a 20% para ciclos de trabalho do IEEE 802.11 acima de 75 %	BERTOCCO, et al. 2008
IEEE 802.15.4 x IEEE 802.11b	Sobreposição de canais, CH 11 (WLAN) e CH 22 (WSN). Ambas as redes em CCA1	1) Importância do tamanho dos pacotes e da ocupação da banda do IEEE 802.11b 2) IEEE 802.15.4 sofre grande degradação sob interferência do IEEE 802.11	ANGRISANI, et al. 2008
IEEE 802.15.4 x IEEE 802.11b	Réplica de uma típica instalação de óleo e gás. 10 nodos IEEE 802.15.4. Ponto interferente e gateway em área de 1 m.	1) Ocorre aumento na perda de pacotes, latência da rede e instabilidade; 2) Confiabilidade mantém em 100%	PETERSEN, et al., 2007
IEEE 802.11 e IEEE 802.15.4	Distância da interferência < 2 m; CCA com limiar em -76dBm; Offset do canal em 2 MHz; Sobreposição canal 22 e 11	PLR é dependente do SIR. Três importantes limiares: 1)baixo -13dB, o menor valor que permite 802.11 operar; 2)alto -7dB, valor grande suficiente para não influenciar no PLR; 3)Inflexão em -11dB.	ANGRISANI, et al. 2008
IEEE 802.15.4 x IEEE 802.15.4	Três dispositivos: transmissor, receptor e elemento interferente; Potência do sinal controlado, meio físico cabos. Pacotes de 22 bytes	1) Significativa diferença de PLR para um offset de frequência de 5 MHz; 2) Não ocorrem mudanças significativas a partir de um deslocamento de frequência maior que 15 MHz; 3) Tamanho dos pacotes relacionado ao SIR requerido para sucesso na transmissão.	SUBBU, et al., 2007
WH x IEEE 802.11	Nove sensores WH distribuídos em um laboratório e três pontos de acesso (IEEE 802.11b/g)	1) WH sem interferência perda de pacotes < 1 %, latência ~ 2 s; 2) IEEE 802.11 causa perda de pacotes WH e aumento de latência da rede.	PETERSEN, et al., 2009
WH x Chirp jamming	Dispositivo interferente < 1 m do gateway WH	1) Degradação completa da rede WH, nenhum pacote entregue.	PETERSEN, et al., 2009

## **5 ANÁLISE DE COEXISTÊNCIA EM REDES WIRELESSHART**

Uma característica importante das redes sem fio é sua típica suscetibilidade por interferência de rádio e o fato que estes dispositivos são geralmente colocados em áreas onde já existe poluição de distúrbios de rádio frequência, gerado por operação de equipamentos elétricos e eletrônicos e ou também por outros padrões de comunicação sem fio.

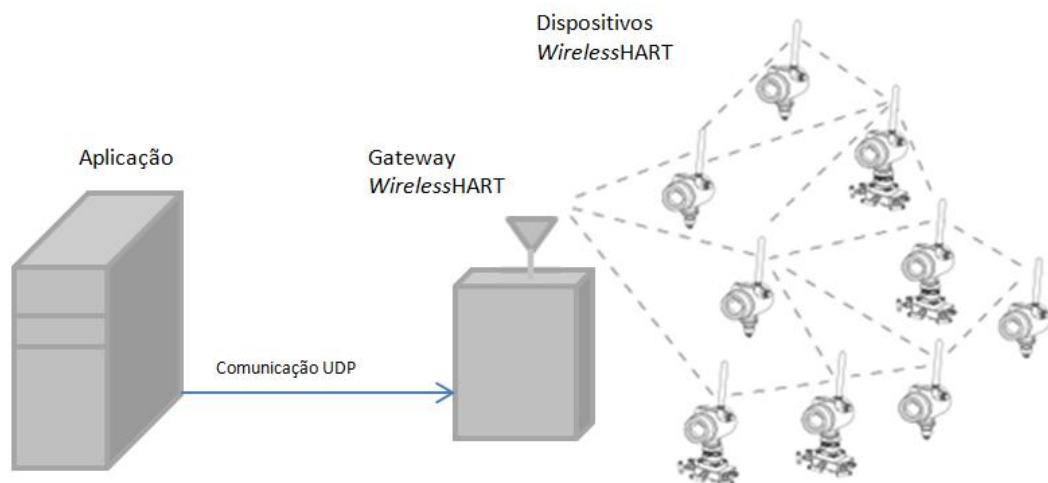
Existem diferentes condições de coexistência. Muitos dispositivos de comunicação sem fio são ditos terem a capacidade de coexistir se não causam impacto significativo no desempenho de outros dispositivos. Outra definição apresentada refere-se à habilidade de um sistema desempenhar uma tarefa em um ambiente compartilhado com outros sistemas que utilizam ou não o mesmo conjunto de regras de operação. O objetivo de uma rede sem fio é transmitir dados com certa qualidade de serviço (QoS). Os parâmetros primários de QoS são perda de pacotes e atraso de transmissão. Em seguida estão os parâmetros como jitter, disponibilidade e segurança conforme detalhado em (SIKORA & GROZA, 2005).

### **5.1 MÉTODOS E MÉTRICAS UTILIZADAS**

Baseado nos critérios primários da qualidade de serviço, foram desenvolvidas ferramentas exclusivas para análise do desempenho de uma rede WH sob circunstâncias de interferência. As métricas utilizadas referentes à camada de transporte são as mesmas utilizadas pela rede WH para determinar as conexões e o roteamento de mensagens entre os dispositivos vizinhos, o que inclui estatísticas referentes ao número de pacotes transmitidos e recebidos para um determinado dispositivo. As métricas utilizadas são descritas abaixo.

### 5.1.1 Latência e Jitter

Para obter dados temporais da rede WH foi implementada uma ferramenta que permite obter dados dos dispositivos de campo através de mecanismos que realizam a requisição de dados por intermédio do gateway. Através de uma comunicação Ethernet, o aplicativo utiliza o protocolo UDP para realizar a comunicação com o Gateway WH, aqui denominado Hart sobre UDP. O Gateway por sua vez comunica-se com os dispositivos na rede, ver Figura 15.



**Figura 15. Comunicação da aplicação com os dispositivos de campo.**

Este software identifica os dispositivos conectados na rede WH e envia uma requisição periódica de dados, neste caso, foi implementado a requisição do comando 780 (HCF, 2008). Além dos dados dos dispositivos da rede, o software registra o tempo de resposta para cada comando enviado. (WINTER, et al., 2011) descreve outras aplicações baseadas nesta ferramenta de análise. Os componentes envolvidos no processo e os tempos medidos são apresentados na Figura 164.



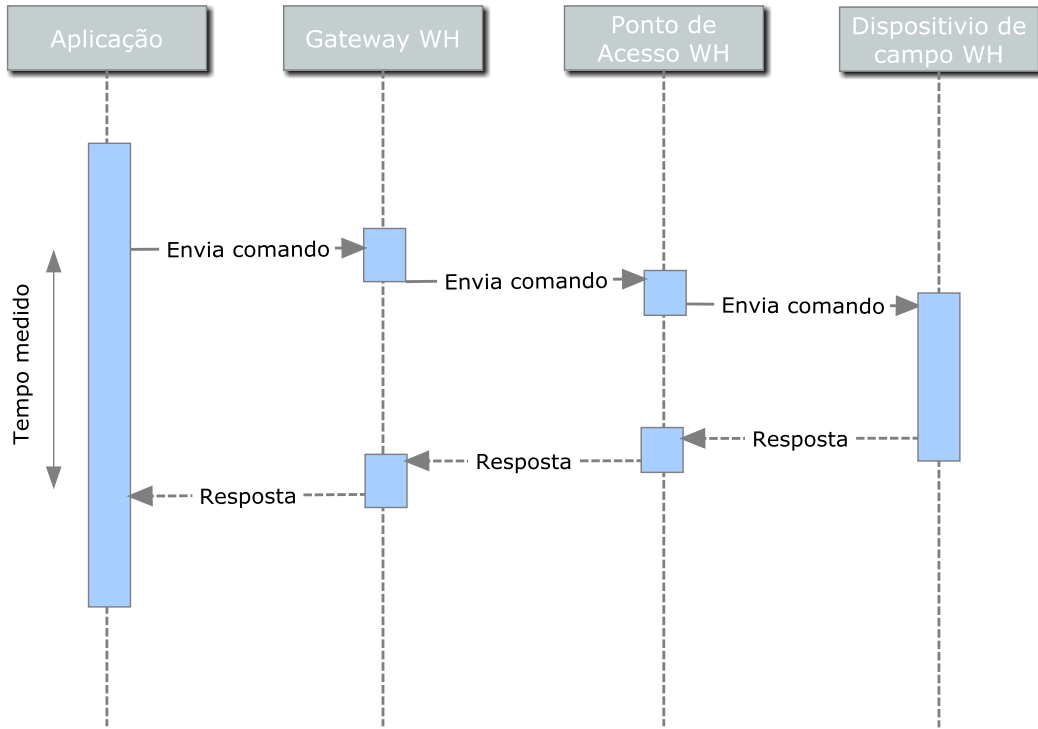


Figura 16 Diagrama de seqüência da aplicação HART sobre UDP

Os dados obtidos são apresentados na interface do software, vide Figura 17, e ainda registrado em um documento para posterior análise.

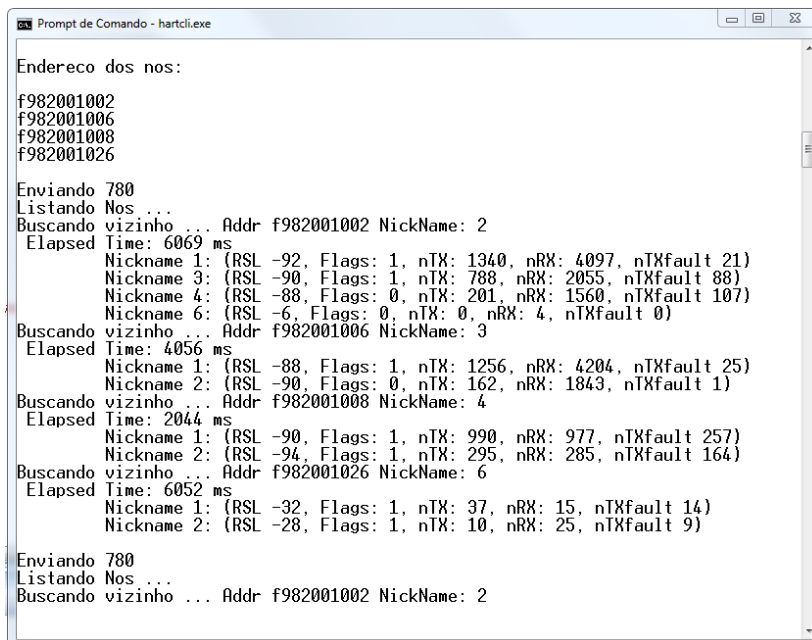


Figura 17. Dados obtidos na interface da aplicação.

Primeiramente são identificados os dispositivos que estão na rede através do comando 814 (HCF, 2008), sendo obtidos a identificação única de cada dispositivo (no exemplo, são lidos 4 dispositivos: F982001002, F982001006, F982001008 e F982001026). Na sequência, para cada dispositivo na rede é enviado um comando WH. O tempo de envio e retorno é preenchido no campo *Elapsed Time* e, neste caso, o conteúdo de retorno indica a lista de dispositivos vizinhos identificados através do endereço curto (apelido) com os dados de intensidade de sinal entre o dispositivo requisitado e seu respectivo vizinho (RSL), a indicação se o dispositivo vizinho é uma referência para ajuste de tempo (*Flags*), número de pacotes transmitidos, recebidos e pacotes que apresentaram falha na transmissão com o dispositivo vizinho, respectivamente (nTx, nRx e nTxFault).

### 5.1.2 Taxa de Pacotes Perdidos

A norma WH determina que os dispositivos de campo devem ser capazes de suportar comandos através da porta de manutenção, de forma a permitir o comissionamento dos dispositivos da rede. A partir destas considerações uma segunda ferramenta foi utilizada para obter dados referentes ao desempenho do protocolo diretamente no dispositivo de interesse. Utilizando a porta de manutenção para requisição de dados, o aplicativo no dispositivo servidor realiza a comunicação através de um conversor USB - RS485, vide Figura 18. O trabalho de (LIMA, et al., 2012) apresenta mais detalhes sobre a comunicação entre o dispositivo WH e a aplicação.

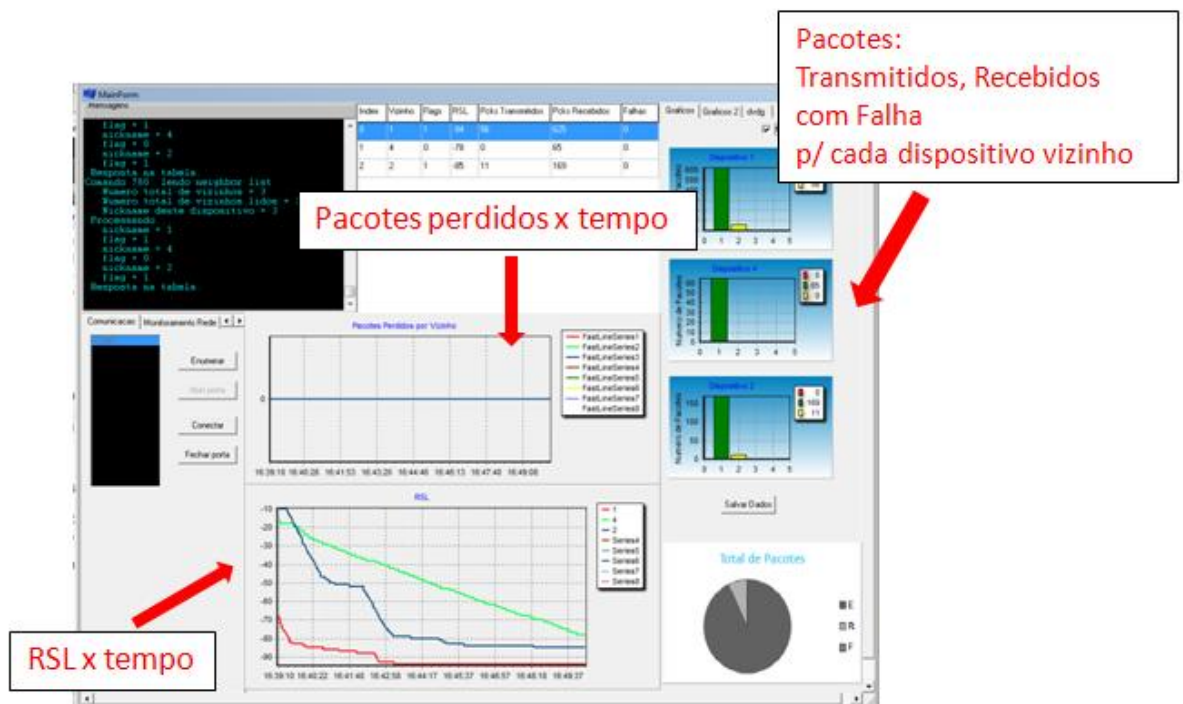


**Figura 18. Comunicação da aplicação diretamente com dispositivo WH.**

Através desta aplicação são coletados periodicamente os seguintes dados:

- Número de dispositivos vizinhos (dispositivos com conexão com o dispositivo alvo);
- Número de pacotes de dados transmitidos para cada dispositivo vizinho;
- Número de pacotes recebidos de cada dispositivo vizinho;
- Número de pacotes que falharam, foram transmitidos e não receberam confirmação de recebimento;
- Intensidade de sinal entre cada dispositivo vizinho.

Na interface do aplicativo, Figura 19, pode-se verificar os dados mensurados de cada dispositivo conectado com o dispositivo em análise.



**Figura 19 Interface de aplicação para acesso a porta de manutenção do dispositivo WH**

A taxa de relação de perda de pacotes é obtida a partir da relação dos pacotes transmitidos e dos pacotes os quais não houve confirmação de recebimento.

No protocolo WH, a confirmação do recebimento da mensagem é enviada imediatamente inclusive no mesmo quadro de tempo. Uma falha na transmissão é considerada quando um reconhecimento de recebimento de mensagem (ACK) é esperado e não chega. Quando uma mensagem é recebida com falha, o ACK não é transmitido. De acordo com a norma o dispositivo deve possuir uma lista de pacotes que podem ser transmitidos para um ou mais vizinhos. Quando ocorrer um quadro de tempo com um pacote pendente, o dispositivo deve tentar propagar a mensagem para um vizinho. Essas tentativas resultam em transmissão com sucesso ou falha:

- Sucesso na propagação de um pacote com o endereço da DLPDU sendo o endereço de *broadcast*, ocorre assim que o pacote é transmitido. O buffer do pacote pode ser liberado imediatamente depois de finalizada a transmissão da DLPDU;
- Sucesso na propagação de um pacote com um endereço de DLPDU que não é *broadcast*, ocorre quando um ACK é recebido. O buffer do pacote pode ser liberado;
- Mensagens com erros nos bits transmitidos são detectadas pelo mecanismo de CRC (*Cyclic Redundancy Check*), neste caso a DLPDU é descartada e não há resposta de recebimento de mensagem;
- Outro erro pode ocorrer em função de uma falha na autenticação, após confirmado pelo CRC, o MIC é calculado e comparado com o MIC da DLPDU em caso de divergência a mensagem é descartada e da mesma forma a confirmação do recebimento não é enviada.

### 5.1.3 Detecção de Energia

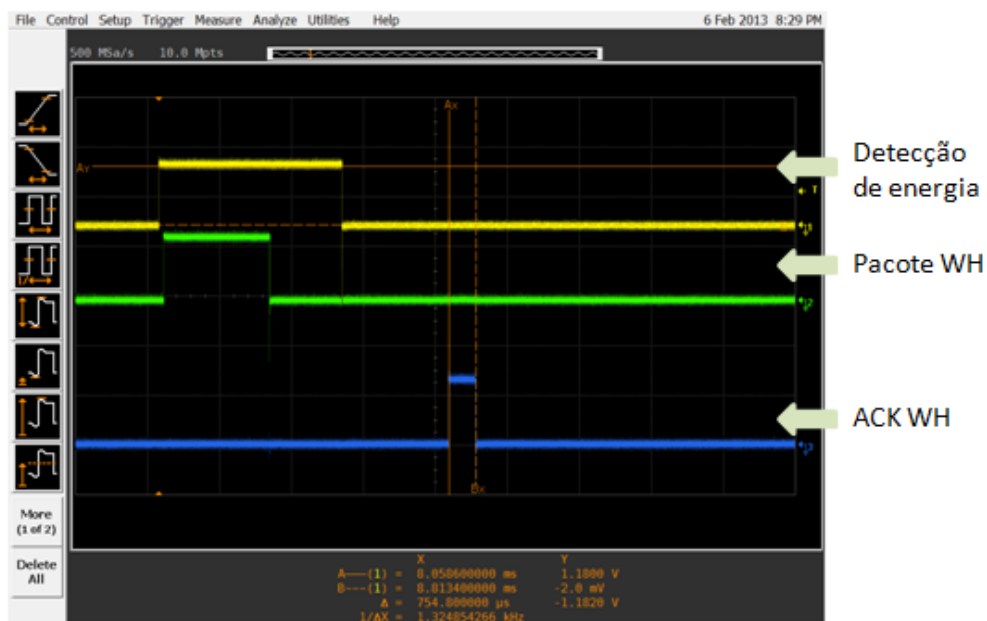
Ainda outra métrica utilizada para análise refere-se à medição do nível de energia durante o tráfego de dados dos dispositivos WH. Uma das dificuldades para monitorar o meio físico utilizado pelo WH está relacionada ao número de canais utilizados (15 canais), sendo tradicionalmente necessários 15 rádios para monitorar cada faixa de frequência. Nesta etapa propõem-se o uso de uma ferramenta que monitore apenas o canal utilizado no instante da comunicação para o quadro de tempo designado para o dispositivo alvo de análise, no entanto, o canal a ser utilizado é somente conhecido pelos elementos que compõem a rede WH uma vez que este é baseado por i) deslocamento do canal; ii) mapa de canais e iii) no ASN, conforme visto na equação 7.

A camada física do IEEE 802.15.4 possui duas funções de medidas para indicar o nível de interferência dentro de um canal. A medida de energia no receptor RSSI (*Receive Signal Strength Indication*) é uma estimativa da potência do sinal recebido em um determinado canal e permite utilizá-lo como parte de algoritmos para seleção de canais na camada de rede, utilizado no padrão ZigBee, por exemplo. A outra métrica refere-se ao indicador da qualidade da conexão ou LQI (*Link Quality Indicator*) que caracteriza a intensidade e ou a qualidade do pacote recebido. De acordo com (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEER, 2006), esta métrica de medida pode utilizar a detecção de energia, o SNR ou a combinação destes dois métodos no dispositivo utilizado.

Para a detecção de energia ocorrer no tempo e na frequência correta foi implementado uma ferramenta que utiliza apenas um único rádio com comunicação com o dispositivo de campo WH. A pilha do WH foi alterada de forma a fornecer as informações relacionadas ao canal utilizado pelo dispositivo em análise. Além do canal também são enviados para o

dispositivo que monitora a energia no canal utilizado o ASN, o tipo da DLPDU, tamanho do pacote enviado e recebido e a confirmação ou não da entrega e do envio do pacote.

Nesta ferramenta restrições temporais foram relevantes para o dispositivo atender adequadamente a leitura de energia do canal correto utilizado pelo dispositivo de campo WH. Na Figura 20 são apresentados os tempos do acionamento da detecção de energia e o tempo de transmissão ou recepção do dispositivo WH. Os tempos foram medidos diretamente nos hardwares utilizados, obtidos através de um osciloscópio com medidas em pinos de GPIO que indicam os intervalos de transmissão e recepção de dados. Verifica se que a janela de tempo é atendida durante o tráfego do pacote WH, a primeira linha representa o momento em que o dispositivo detector de energia coloca o modem em modo de recepção para medir o nível de energia. A segunda linha representa o tempo de transmissão do pacote WH e a terceira linha representa a janela de tempo da transação do ACK. Optou-se por não mensurar a energia no momento da operação do ACK, uma vez que em um canal utilizado para recepção, por exemplo, o valor medido seria alterado significativamente pela intensidade de sinal de uma operação de transmissão (valor alto dado à proximidade dos dispositivos).

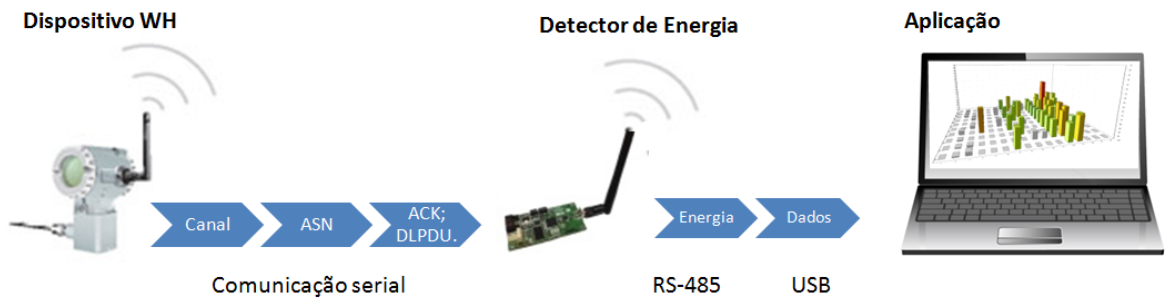


**Figura 20** Imagem dos tempos de envio de mensagem do dispositivo WH e do chaveamento do modem para detecção de energia.

A duração do quadro de tempo é de 10 ms, baseado em sua ocupação máxima, sendo:

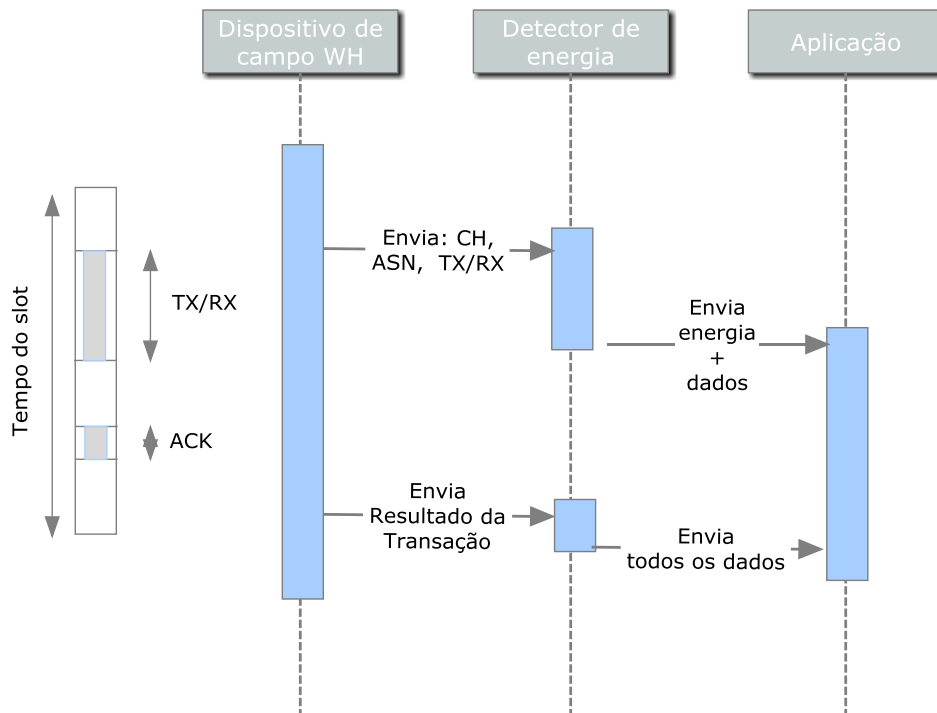
- 133 bytes de dados com uma taxa de 250kbps resultando em 4,256 ms;
- 26 bytes de ACK com uma taxa de 250kbps resultando em 832 us.

A arquitetura utilizada para esta ferramenta pode ser vista na Figura 21.



**Figura 21. Comunicação entre os dispositivos e a aplicação para detecção de energia.**

A Figura 22 ilustra em etapas o funcionamento do dispositivo para detecção de energia de acordo com os tempos do *slot* de tempo WH.



**Figura 22 Diagrama de sequência da detecção de energia**

#### 5.1.4 Confiabilidade

Para os experimentos realizados utilizamos um gateway WH comercial. Apesar de diversas limitações quanto aos dados de gerenciamento da rede, é possível obter algumas informações relacionadas ao desempenho da rede. O protocolo WH permite configurar dados que podem ser publicados periodicamente dentro de um valor limite de tempo. As mensagens podem ser originadas assincronamente por um dispositivo HART sem a mensagem ser explicitamente requisitada por outro dispositivo. Este tipo cíclico de publicação é denominado pelo padrão como modo *Burst* de envio de mensagens e é normalmente configurado de acordo com os requisitos da planta e do processo. Através deste modo é possível garantir *slots* de tempo e *links* redundantes para a transmissão das variáveis de processo dentro dos requisitos temporais ajustados.

Nesta condição a publicação do valor da variável de processo dentro do limite temporal dos dispositivos utilizados, foi monitorada e definida como métrica de confiabilidade. A confiabilidade não contabiliza retransmissões e redundâncias inerentes da topologia.

## 5.2 ESTUDO DE CASO

A expressão “pior caso” é utilizada por (POLLIN, et al., 2008) indica uma condição de severa coexistência. Quatro parâmetros são apontados para formar este cenário de pior caso sendo: i) sobreposição de canais; ii) alta taxa de utilização da rede; iii) distância curta entre os dispositivos concorrentes e iv) o sistema interferente com uma alta potência de transmissão. A literatura apresenta uma série de estudos relatando degradação de redes do tipo IEEE 802.15.4 em ambientes aplicados ao pior caso, conforme abordado no capítulo 4.

Para o estudo de caso, são propostos experimentos em cenários reais com fontes interferentes que também operam na banda de 2.4 GHz. Os experimentos são promovidos de



forma a testar o desempenho da rede WH sob a interferência dos seguintes padrões IEEE 802.11g, IEEE 802.15.1 e o próprio IEEE 802.15.4.

Um dos principais propósitos desta análise é mensurar níveis de desempenho do protocolo WH de forma que se possam determinar níveis de confiabilidade. Nos cenários apresentados o impacto é observado sempre de forma unidirecional, ou seja, é monitorada a rede WH como vítima de interferência.

### 5.2.1 Parâmetros da Rede *Wireless*HART

No cenário utilizado para o estudo de caso foram utilizados nodos WH desenvolvidos no GCAR, vide Figura 23, (MULLER, 2010), formando uma rede com 5 dispositivos e o gateway da rede. Segue abaixo os parâmetros utilizados no cenário de estudo:

- Os dispositivos foram distribuídos em uma área com um raio de aproximadamente 6 metros;
- A potência de transmissão dos dispositivos foi ajustada para 10 dBm;
- O tempo de publicação da variável de processo associada aos dispositivos de campo foi ajustado para 60 segundos;
- O mecanismo de CCA da rede WH manteve-se na configuração padrão, ou seja, não habilitado.



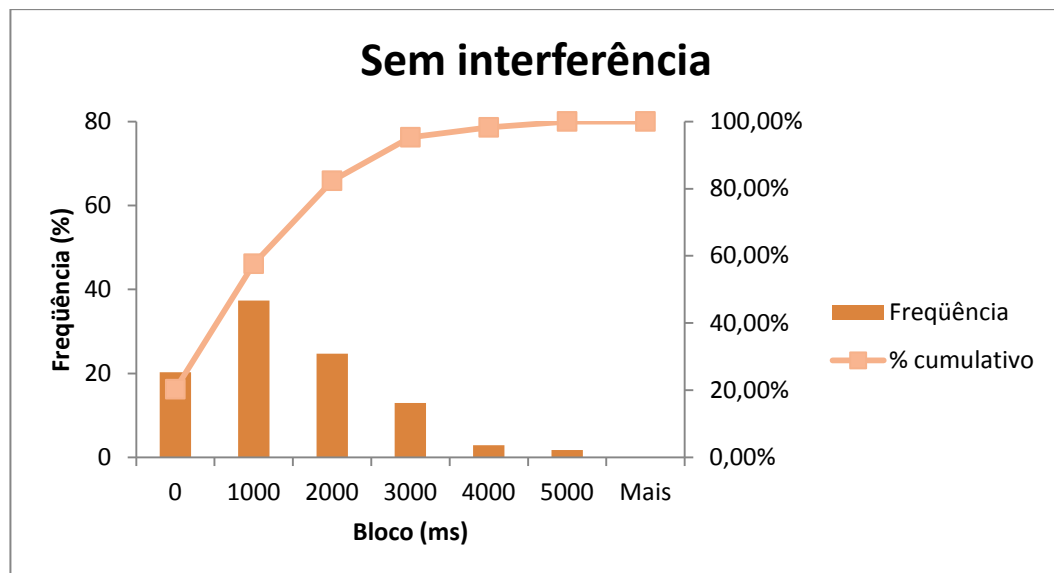
**Figura 23 Dispositivos WH.**

Utilizando a aplicação WH sobre UDP foi requisitado um tráfego maior de dados com pedidos de mensagens para os dispositivos de campo, com o objetivo de aumentar o fluxo de

dados da rede. Através das ferramentas já apresentadas em capítulos anteriores foram obtidos os seguintes resultados.

### 5.2.2 Desempenho da Rede *Wireless*HART sem Interferência

Inicialmente a rede foi monitorada em um ambiente livre de interferência de forma a obter uma medida de desempenho para poder distinguir as possíveis perdas do protocolo em relação a circunstâncias mais hostis. A Figura 24 apresenta o jitter da rede WH operando em condições livres de interferência.



**Figura 24 Jitter da rede WH em condições livre de interferência**

O histograma da Figura 24 mostra que aproximadamente 20% dos pacotes não apresentaram jitter, 40% apresentaram jitter de até 1 segundo e 98% das mensagens sofreram jitter inferior a 4 segundos. Sem interferência por outro padrão a rede WH apresentou um bom desempenho, mantendo a confiabilidade em 100% e com uma taxa de perda de pacotes quase nula como visto na Figura 25, (Desempenho do protocolo WH para diferentes condições de interferência).

### 5.2.3 Rede WirelessHART sob Interferência do IEEE 802.11

O protocolo IEEE 802.11 popularmente conhecido como WiFi é provavelmente a tecnologia de comunicação sem fio mais utilizada atualmente no mundo (HOWLADER, et al., 2007) . O IEEE 802.11 apresenta uma banda larga em relação ao WH assim como uma potência de transmissão alta (20 dBm). Sendo um protocolo de interesse para os experimentos.

No trabalho de (GOLMIE, 2002) foram analisados os ciclos de trabalhos para aplicações comuns de uma rede WiFi, neste estudo para uma rede com uma taxa de transferência de até 54 Mbps, foram obtidos os valores apresentados na Tabela 3.

**Tabela 3 Média de ciclo de trabalho IEEE 802.11g para diferentes atividades.**

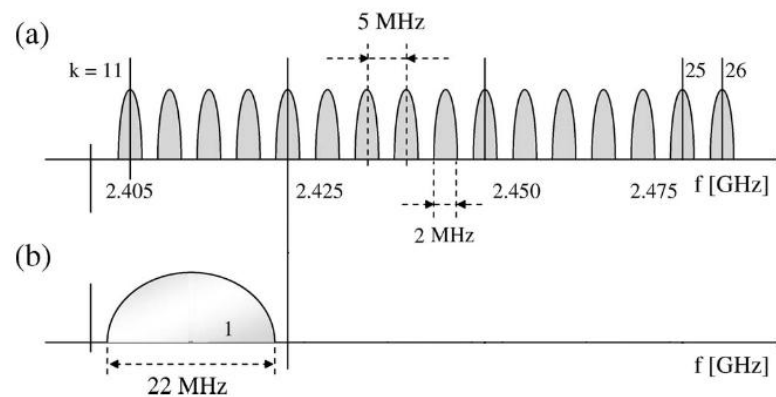
<b>Aplicação</b>	<b>Média (%)</b>	<b>Desvio padrão (%)</b>
Navegando em páginas	0,25	1,15
Voz Skype	0,8	0,47
Vídeo Skype	1,08	0,78
Áudio	0,13	0,58
Vídeo Youtube 306p	2,35	11,55
Vídeo Youtube 1080p	10,69	22,22
Transferência de arquivos	46,18	15,97

Interferência do tipo de banda larga, como o IEEE 802.11b/g, deve aparecer como ruído branco para um receptor IEEE 802.15.4. A resposta do detector, neste caso, é semelhante à resposta para sinal de ruído, mas a exigência da relação sinal interferência, SIR, é de 9 dB a 10 dB menor, pois apenas uma fração da potência do sinal do padrão IEEE 802.11b ou IEEE 802.11.g cai dentro da largura de banda do receptor IEEE 802.15.4.

#### 5.2.3.1 Sobreposição Parcial de Canais

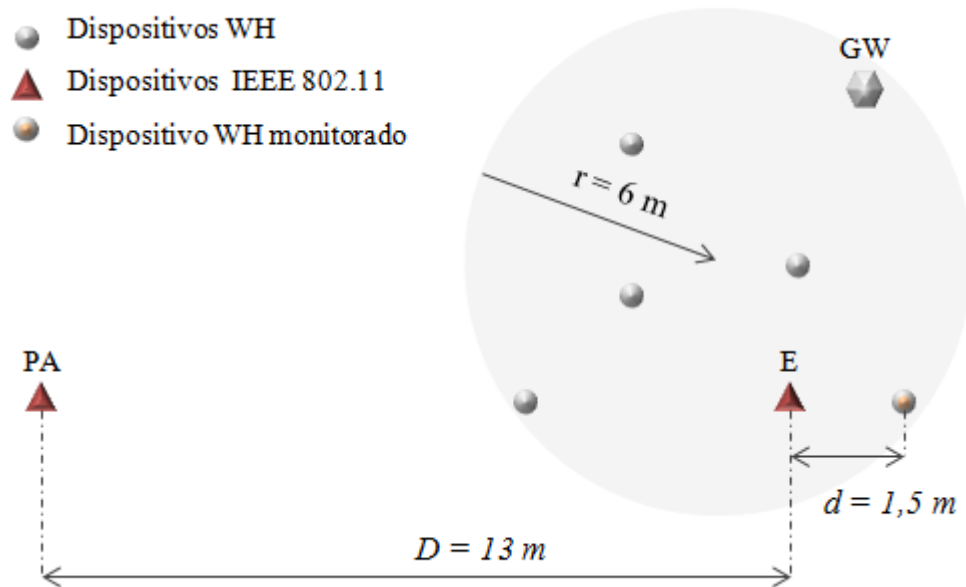
Neste cenário a rede WH opera com os 15 canais enquanto a rede IEEE 802.11 opera com o canal 1 com sobreposição em 4 dos 15 canais do WH, Figura 25. Os experimentos foram realizados seguindo o esquema demonstrado na Figura 264, apresentando uma rede

com 5 dispositivos WH, enquanto para a rede WLAN foram utilizadas duas estações, sendo um computador do tipo móvel (E), e um ponto de acesso (PA) conectado com um computador via cabo. Apesar de o ensaio ter sido limitado em apenas dois terminais, a configuração pode ser considerada em geral e representativa para situações com mais do que dois terminais WLAN.



**Figura 25. Frequências utilizadas (a) WH e (b) IEEE 802.11. (Adaptado de ANGRISANI, 2008)**

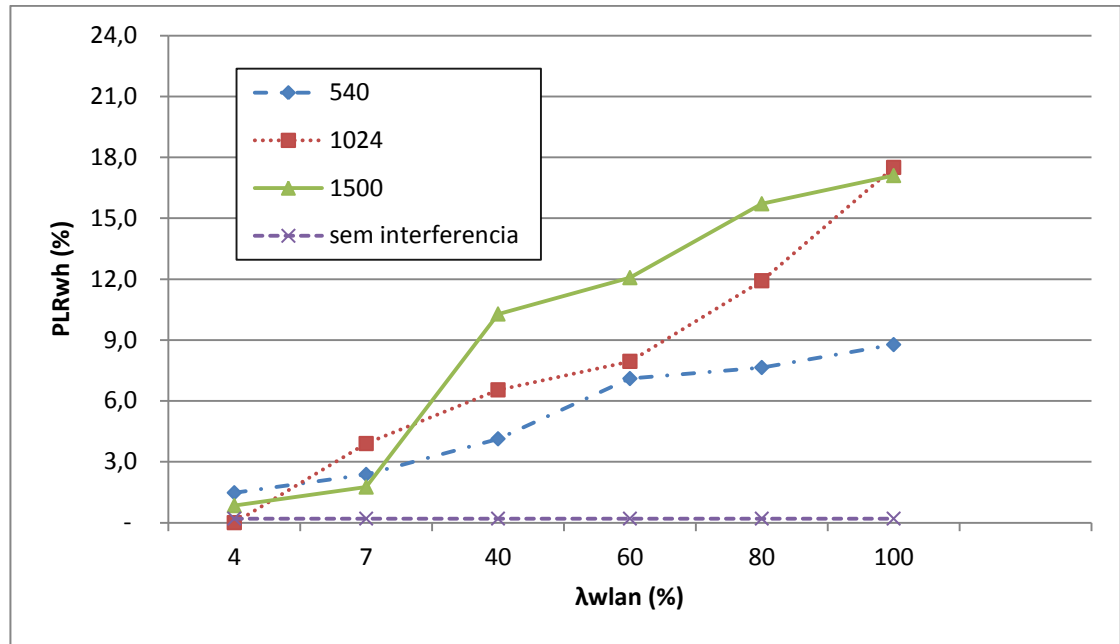
Para garantir e controlar o tráfego de dados na fonte interferente, no cenário de análise, foi utilizado a ferramenta *Distributed Internet Traffic Generator (D-ITG)* (BOTTA, et al. 2012). A aplicação permite o ajuste do protocolo da camada de transporte em TCP, UDP, ICMP e também funcionalidades da camada de aplicação como, DNS, Telnet, Voz ou modo padrão. A aplicação em modo padrão permite determinar a taxa de pacotes transmitidos, tamanhos dos pacotes e a distribuição estatística do tempo entre o envio de mensagens.



**Figura 26** Cenário utilizado para a rede WH

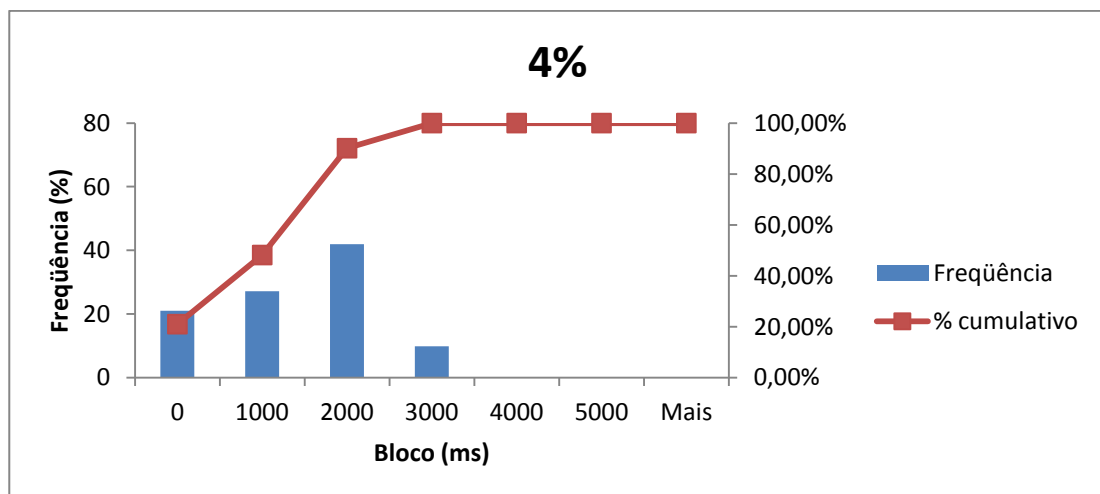
Os experimentos foram conduzidos de forma a verificar o desempenho da rede WH em condições de coexistência com a rede WLAN. A estação E (localizada próxima à rede WH) recebe pacotes do PA (afastado da rede WH). Esta configuração de cenário emula uma situação típica no qual o transmissor da rede WLAN tem uma sensibilidade baixa do sinal da rede WH através do limiar do mecanismo de CSMA/CA, ou seja, desta forma o canal de comunicação do PA para a estação E está sempre livre podendo transmitir continuamente. Sendo  $D$  igual a 13 metros e  $d$  igual a 1,5 metro aproximadamente.

Nos experimentos que seguem a rede WH operou com os 15 canais enquanto a rede IEEE 802.11 utilizou o canal 1 com sobreposição em 4 dos 15 canais do WH. Essa configuração permite a ocorrência de dois tipos de interferência, uma por sobreposição direta de canais e a outra por canais adjacentes. Neste cenário, a rede WLAN operou com diferentes ciclos de trabalho,  $\lambda_{wlan}$ , e também com diferentes tamanhos de pacote, 540, 1024 e 1500 bytes, com uma carga de dados de 512, 996 e 1472 bytes respectivamente. Quanto à taxa de perda de pacotes obtemos os resultados apresentados na Figura 27.



**Figura 27 Desempenho do protocolo WH para diferentes condições de interferência**

O gráfico da Figura 28 ilustra que as perdas de pacotes são superiores a 10% para um  $\lambda_{wlan}$  maior que 75% e pacotes maiores que 1024 bytes. Para pacotes de 540 bytes as perdas não ultrapassam os 10% para a pior condição de ciclo de trabalho da rede interferente. Embora não apresentado no gráfico, o nível de confiabilidade manteve-se em 100% durante os diferentes parâmetros testados, ou seja, as mensagens esperadas foram entregues e atenderam o requisito temporal proposto. Os gráficos a seguir, Figura 30-46, apresentam o jitter obtido da rede WH quando configurado os testes acima.



**Figura 28 Jitter para um ciclo de trabalho de 4% e pacotes de 540 bytes da WLAN**

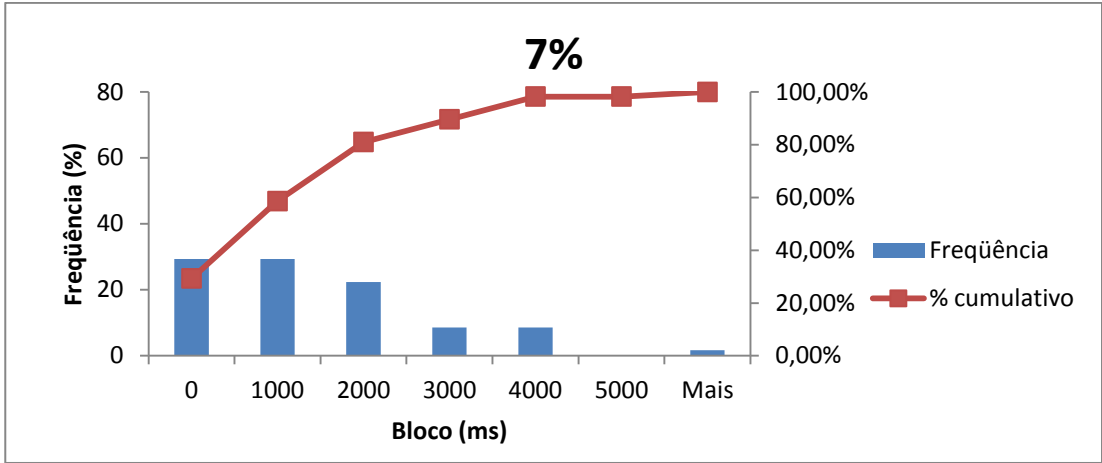


Figura 29 Jitter para um ciclo de trabalho de 7% e pacotes de 540 bytes da WLAN

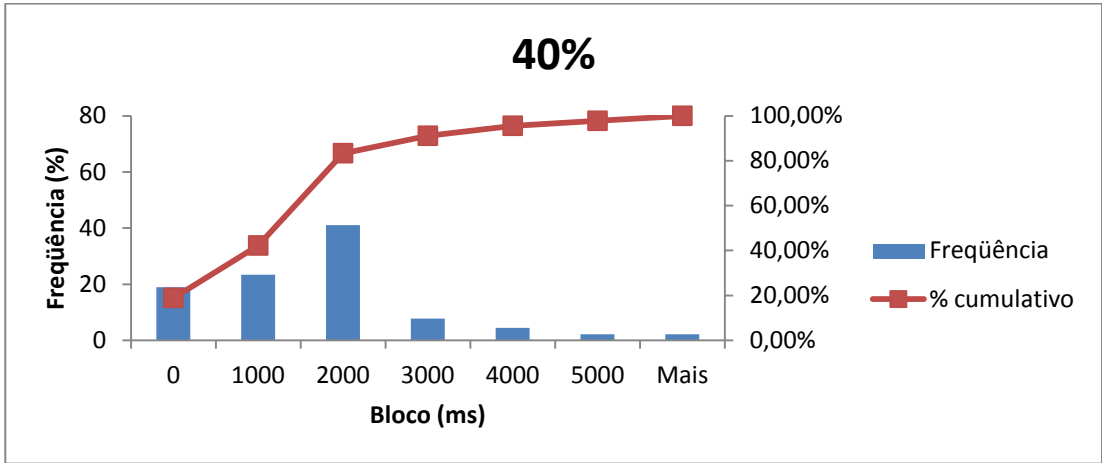


Figura 30 Jitter para um ciclo de trabalho de 40% e pacotes de 540 bytes da WLAN

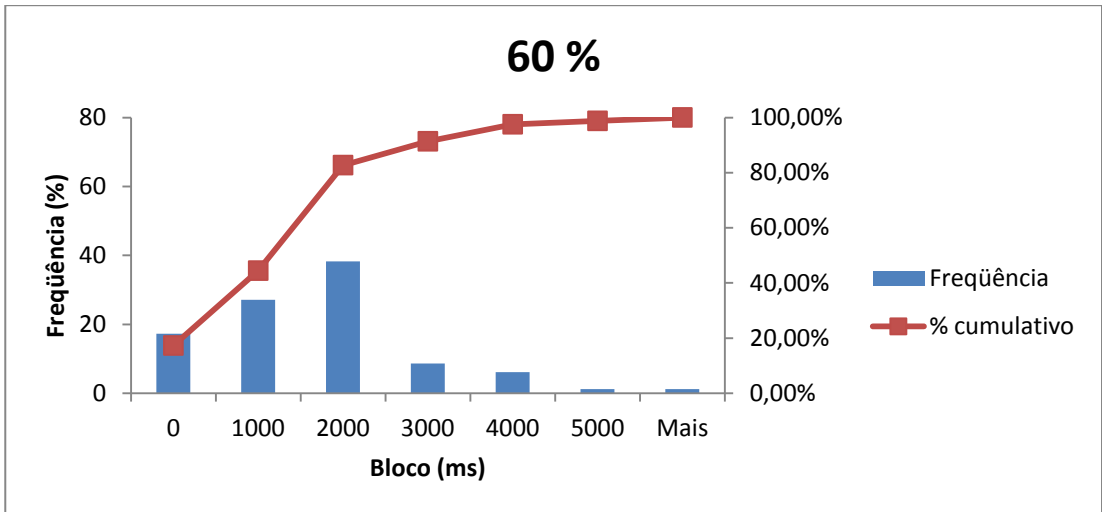


Figura 31 Jitter para um ciclo de trabalho de 60% e pacotes de 540 bytes da WLAN

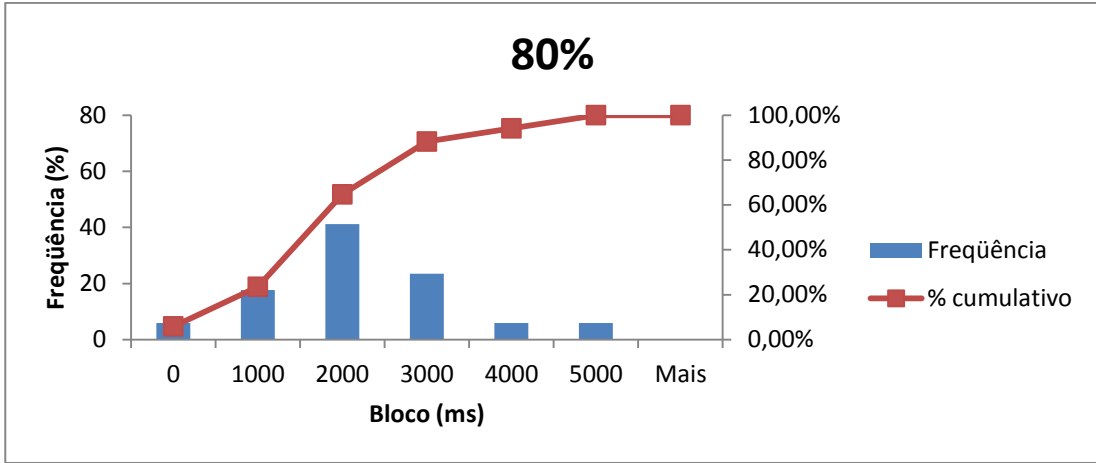


Figura 32 Jitter para um ciclo de trabalho de 80% e pacotes de 540 bytes da WLAN

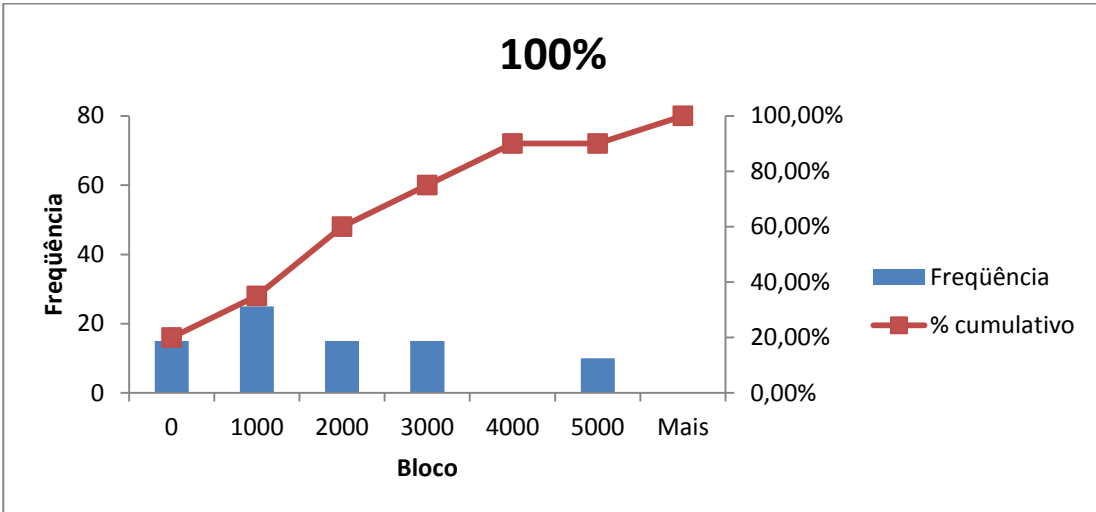


Figura 33 Jitter para um ciclo de trabalho de 100% e pacotes de 540 bytes da WLAN

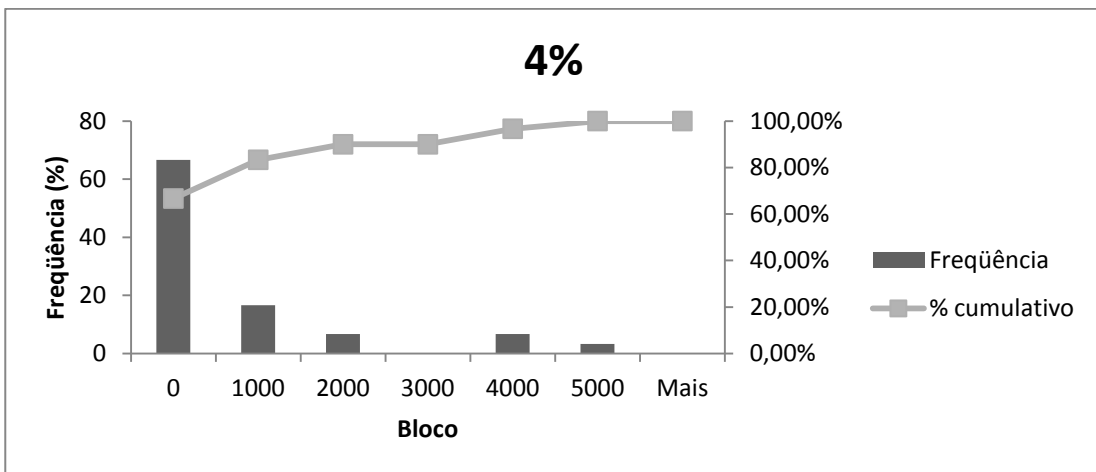


Figura 34 Jitter para um ciclo de trabalho de 4% e pacotes de 1024 bytes da WLAN



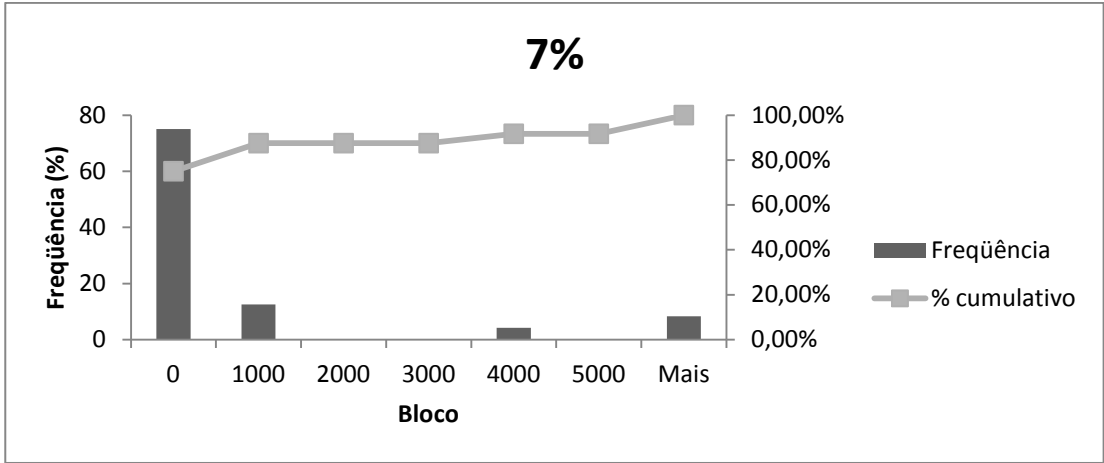


Figura 35 Jitter para um ciclo de trabalho de 7% e pacotes de 1024 bytes da WLAN

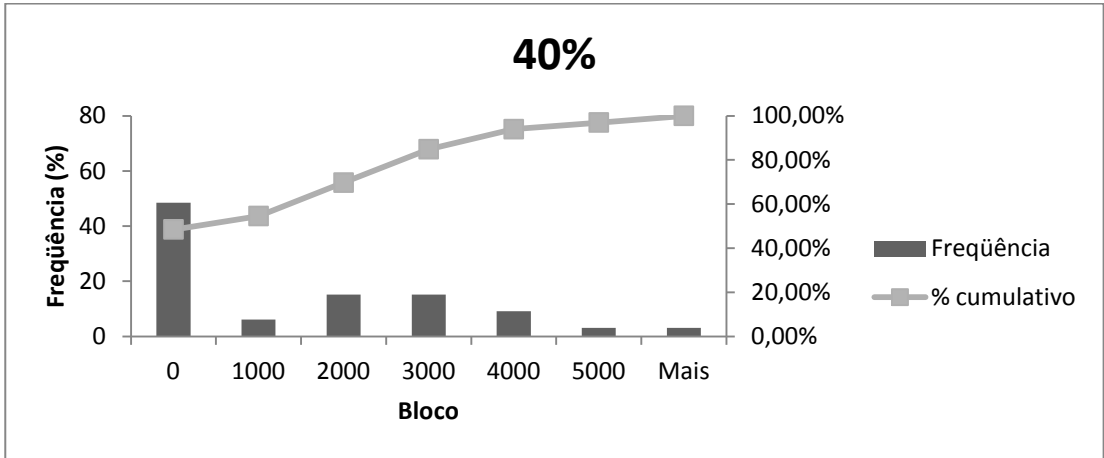


Figura 36 Jitter para um ciclo de trabalho de 40% e pacotes de 1024 bytes da WLAN

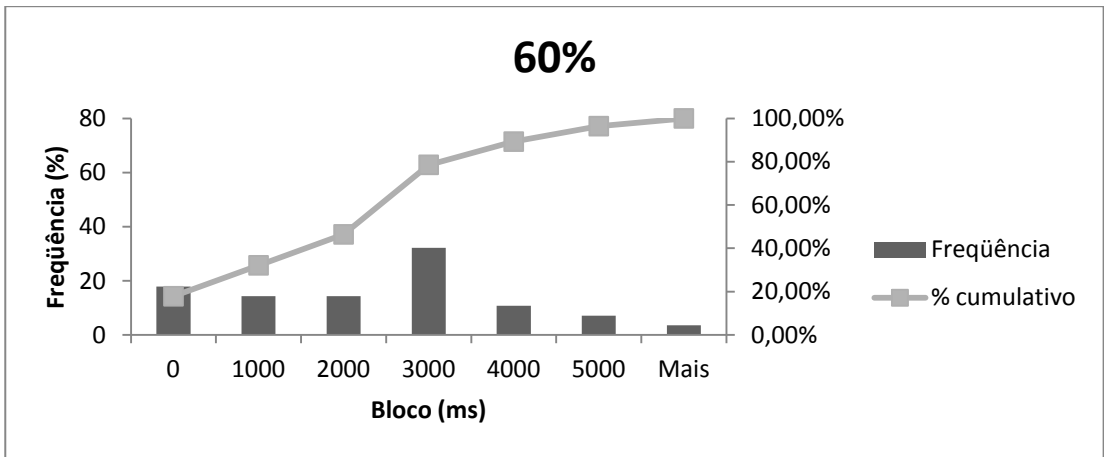
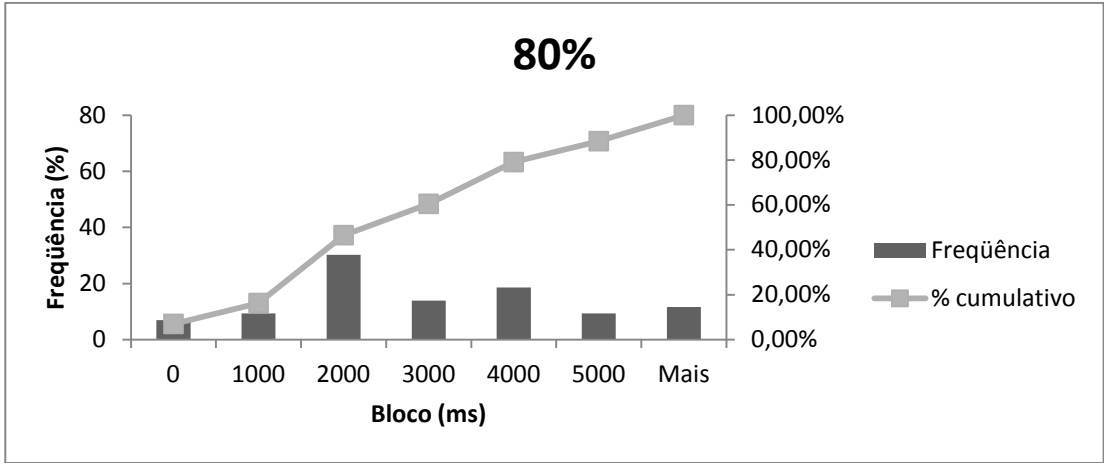
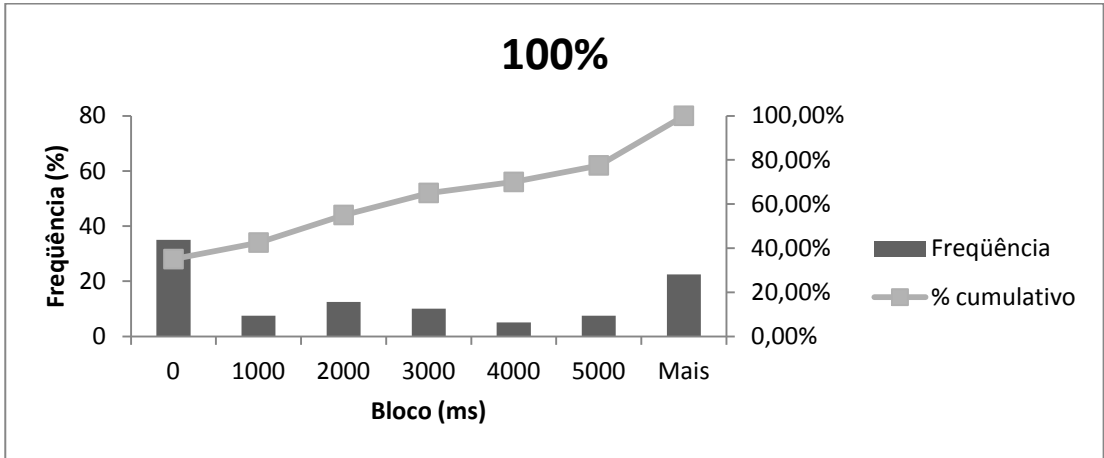


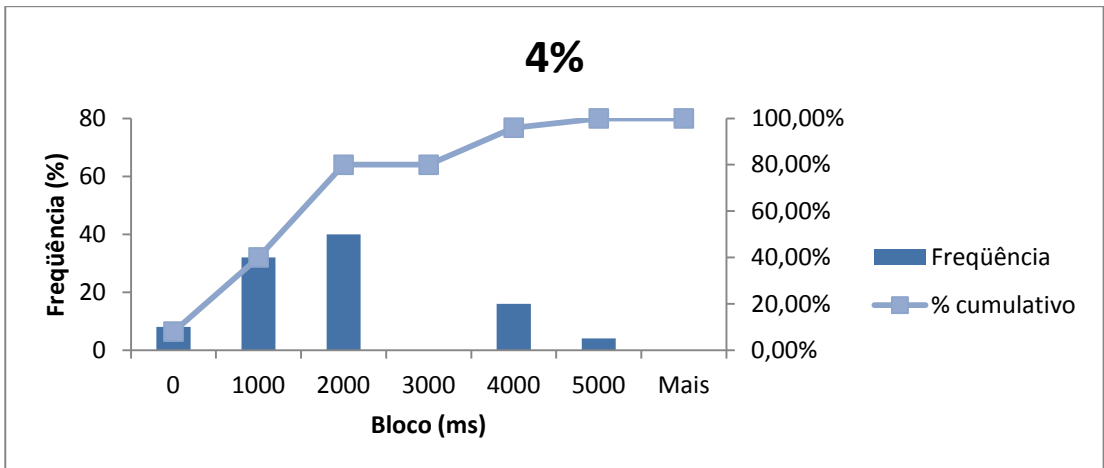
Figura 37 Jitter para um ciclo de trabalho de 60% e pacotes de 1024 bytes da WLAN



**Figura 38 Jitter para um ciclo de trabalho de 80% e pacotes de 1024 bytes da WLAN**



**Figura 39 Jitter para um ciclo de trabalho de 100% e pacotes de 1024 bytes da WLAN**



**Figura 40 Jitter para um ciclo de trabalho de 4% e pacotes de 1500 bytes da WLAN**

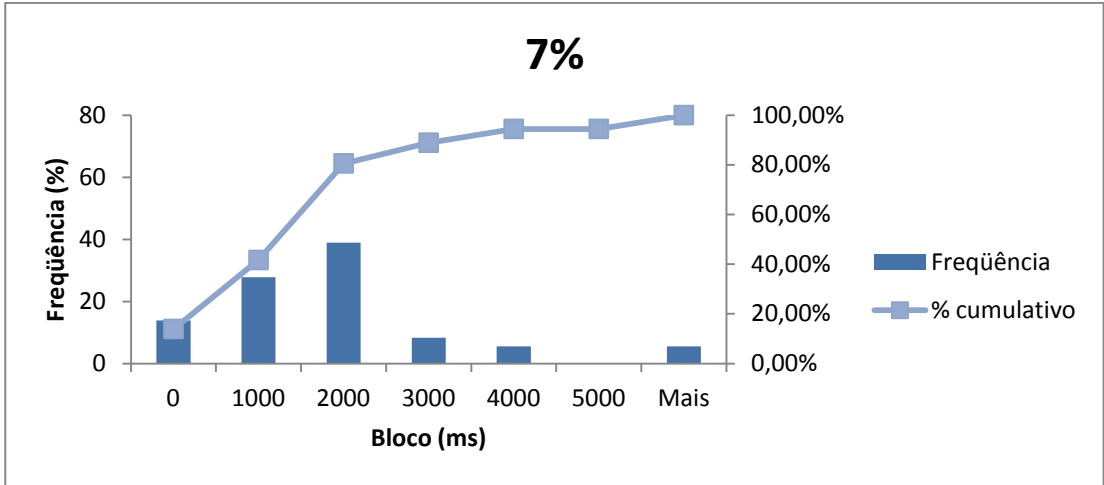


Figura 41 Jitter para um ciclo de trabalho de 7% e pacotes de 1500 bytes da WLAN

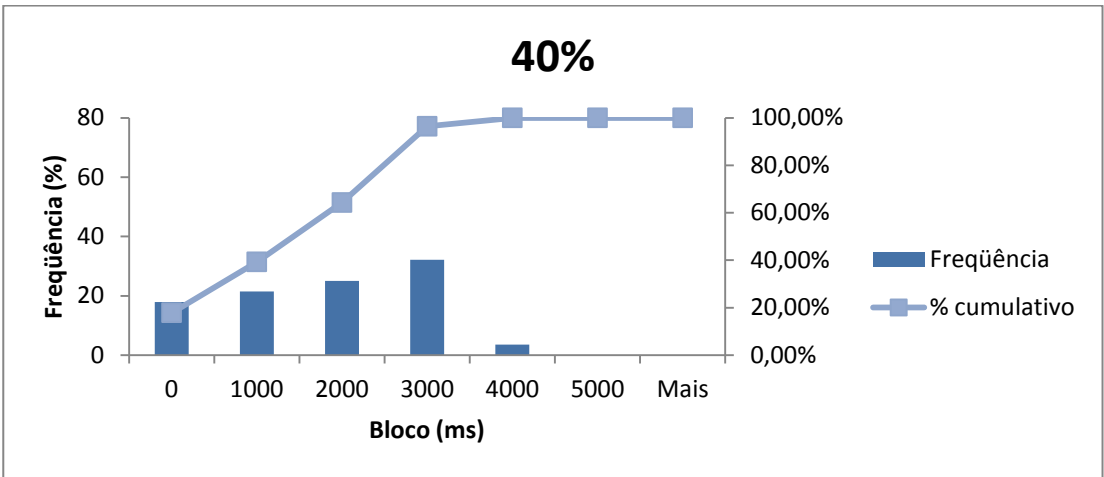


Figura 42 Jitter para um ciclo de trabalho de 40% e pacotes de 1500 bytes da WLAN

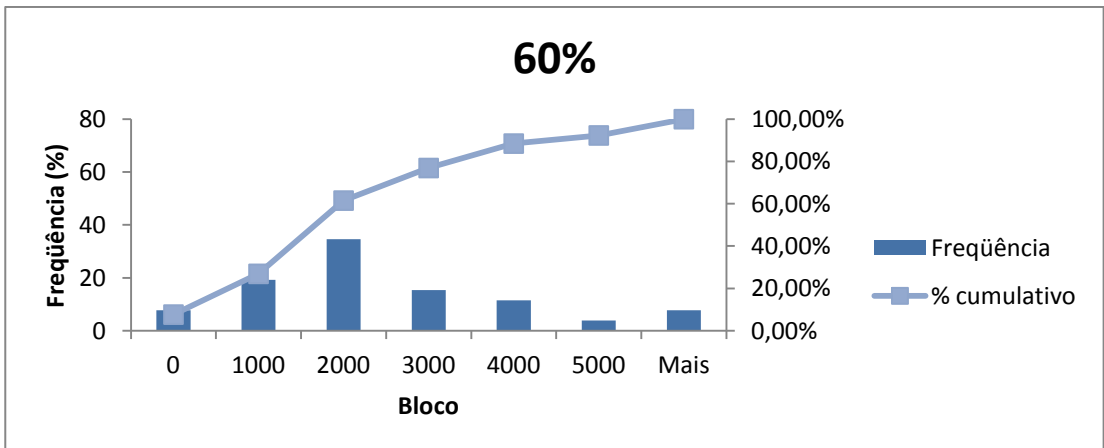
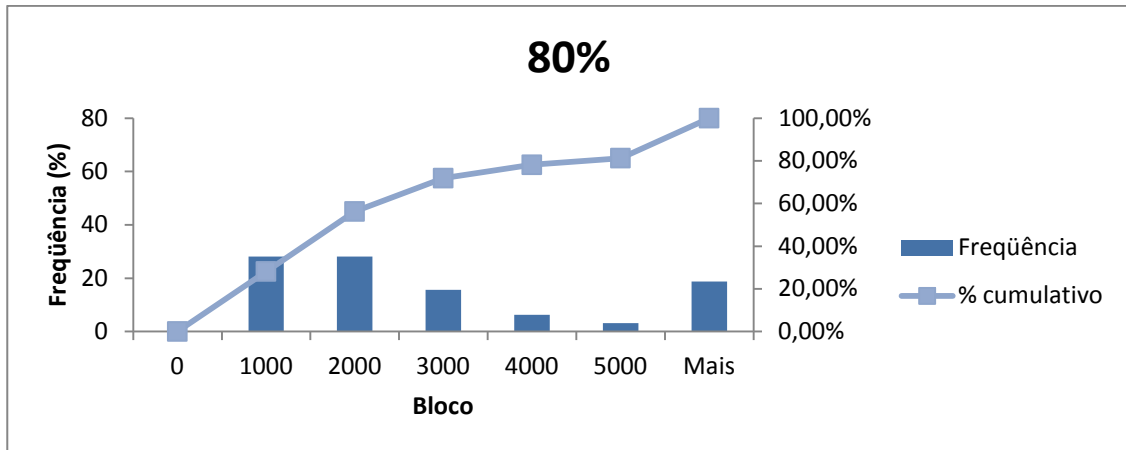
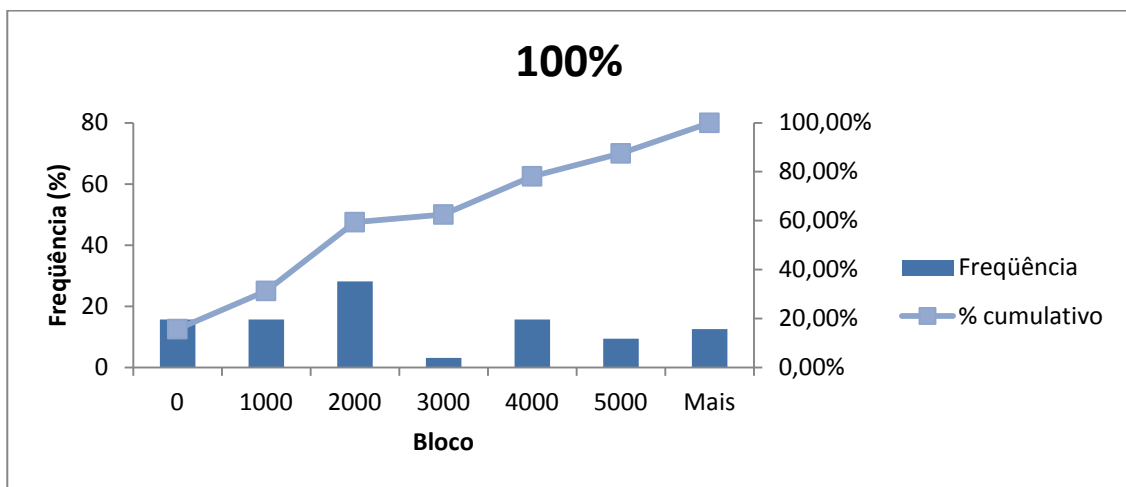


Figura 43 Jitter para um ciclo de trabalho de 60% e pacotes de 1500 bytes da WLAN



**Figura 44 Jitter para um ciclo de trabalho de 80% e pacotes de 1500 bytes da WLAN**



**Figura 45 Jitter para um ciclo de trabalho de 100% e pacotes de 1500 bytes da WLAN**

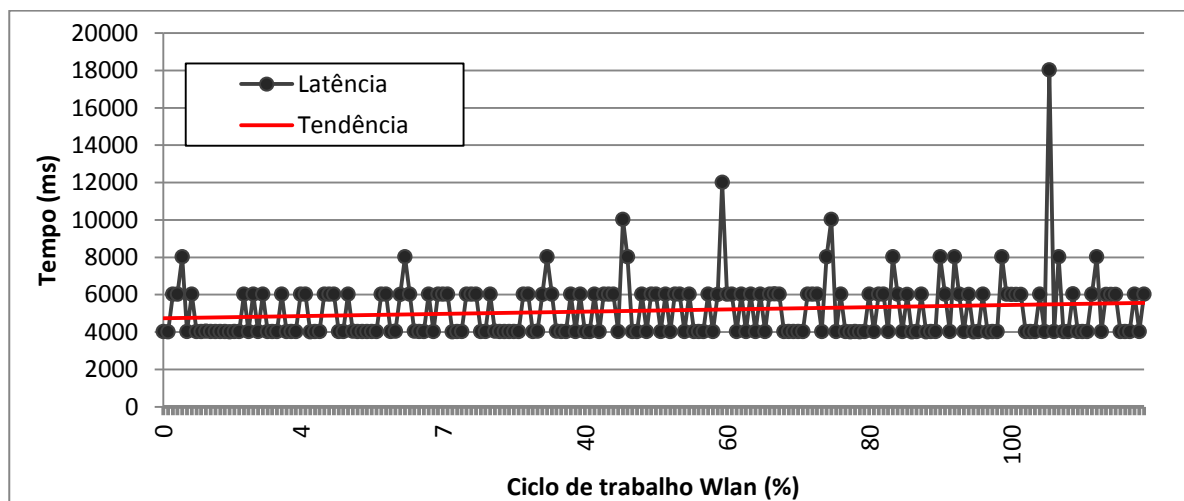
Os resultados demonstram que o jitter da rede aumenta conforme o aumento da ocupação da banda pelo protocolo interferente. Na Tabela 4 são apresentadas as médias e o desvio padrão obtido para alguns casos. Percebe-se que os maiores níveis de desvio padrão estão concentrados para os maiores percentuais de ciclos de trabalho, representando à rede certa instabilidade.

**Tabela 4 Média e o desvio padrão do jitter da rede WH sobre diferentes condições de operação da rede IEEE 802.11**

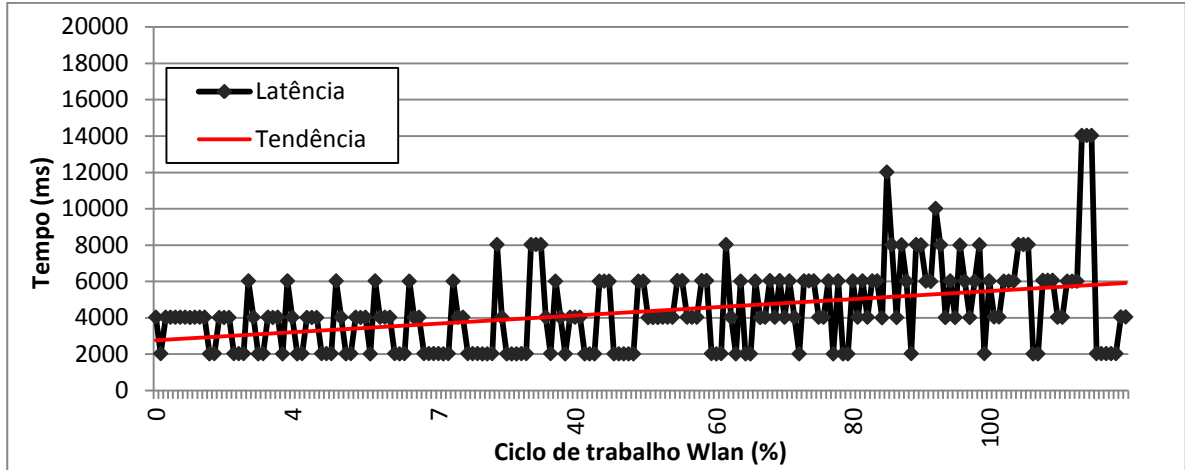
Ciclo de Trabalho (%)	Tamanho do pacote (bytes)					
	500		1024		1500	
	M	DP	M	DP	M	DP
0	945,8	1170,9	945,8	1170,9	945,8	1170,9
4	1038,2	1003,7	1136,5	1355,2	1600,4	1523,3
7	1370,1	1254,7	1465,8	1891,8	1562	1802,5
40	1385,7	1477,6	1305,8	1649,7	1290,3	1115,1
60	1309,5	1344,9	1934,8	1651,9	2081,3	1737,5
80	1766,9	1197,6	3071,8	3210,1	2817,3	3206,5
100	2799,3	4073,1	2930,9	3730,2	2498,2	2378,6

M: média (ms); DP: desvio padrão (ms)

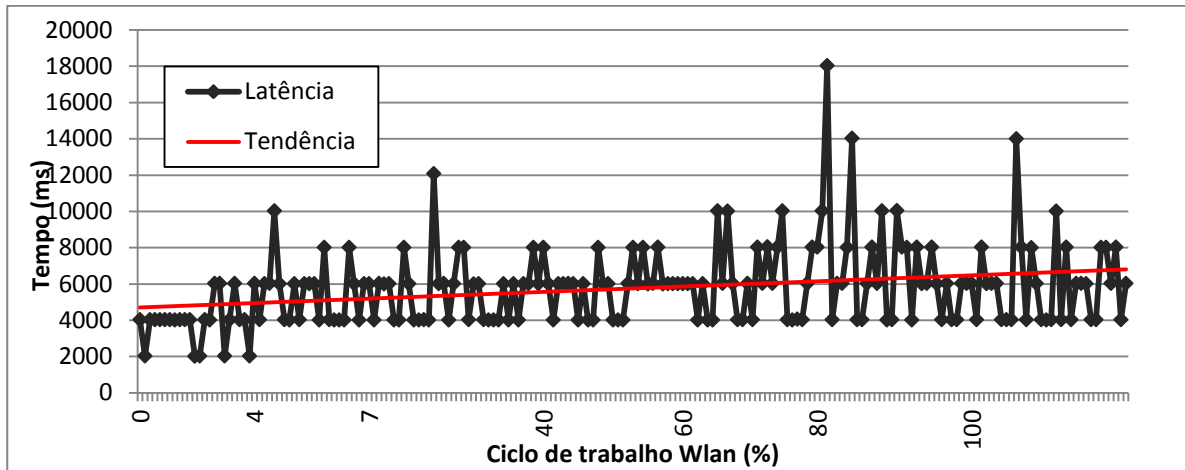
Nas Figuras 46, 47 e 48 são apresentadas amostras da variação da latência da rede em relação à requisição de dados por intermédio da ferramenta WH sobre UDP. Os três casos (540, 1024 e 1500 bytes) são mostrados.



**Figura 46 Latência da rede WH para uma rede interferente com mensagens de 540 bytes**



**Figura 47** Latência da rede WH para uma rede interferente com mensagens de 1024 bytes

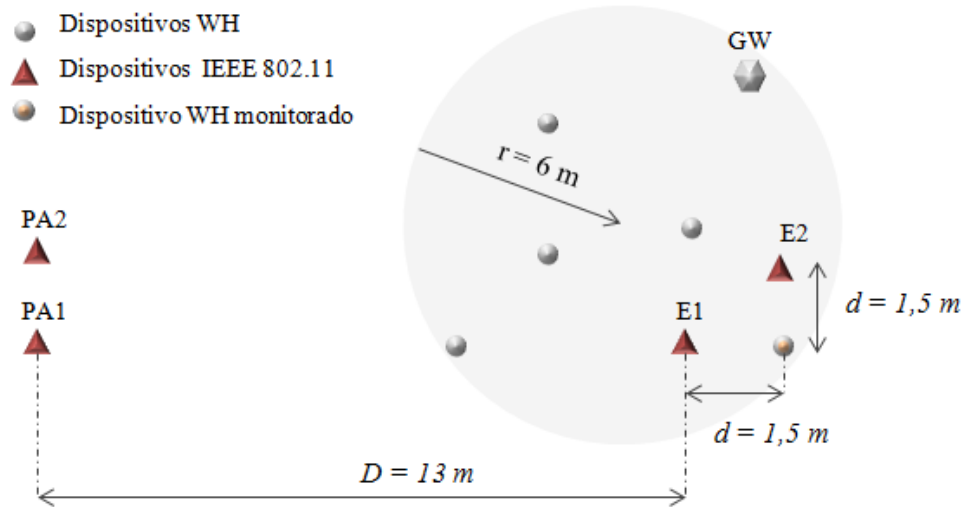


**Figura 48** Latência da rede WH para uma rede interferente com mensagens de 1500 bytes

Observa-se que existe um aumento na latência em função da taxa de ocupação da rede interferente e ainda que amplitudes maiores na latência ocorrem com mais frequência nas interferências com os pacotes maiores (1024 e 1500 bytes).

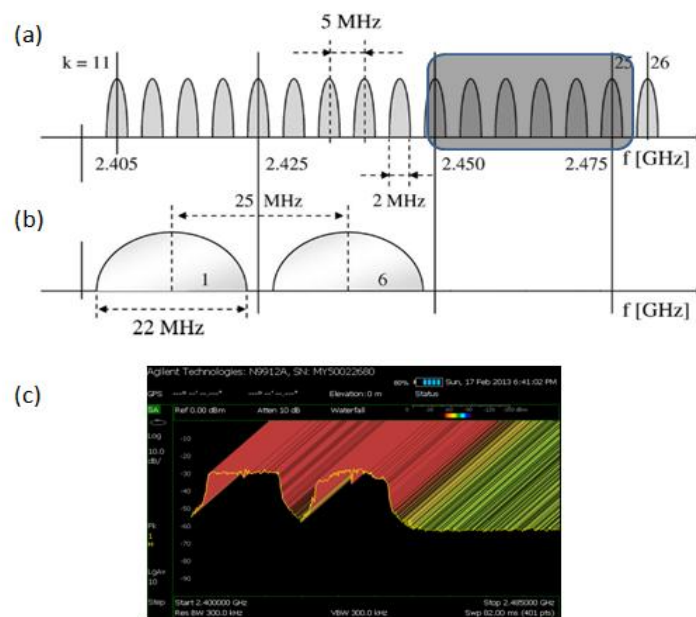
### 5.2.3.2 Sobreposição Total de Canais

Na sequência são realizados ensaios com maior ocupação do espectro pelo elemento interferente. Agora o novo cenário possui duas estações transmissoras e duas estações receptoras, conforme Figura 49.



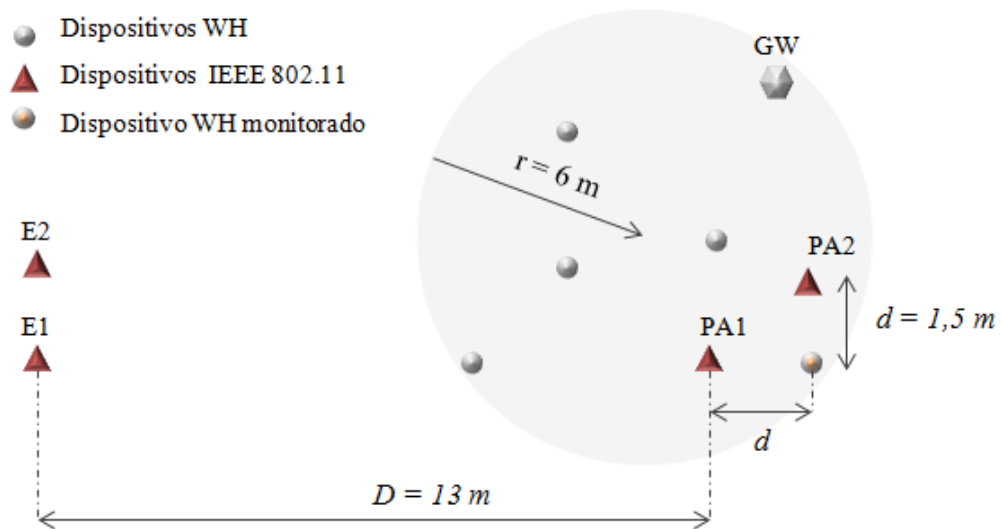
**Figura 49 Segundo cenário utilizado – interferência or downlink**

Os canais 1 e 6 da rede WLAN são utilizados e os canais 20 ao 25 do WH são colocados na lista proibida, de forma a deixar a ocupação do espectro conforme Figura 50, com o objetivo de obtermos a maior ocupação possível do mesmo espectro de frequência utilizado pela rede WH. Neste cenário, com exceção do canal 15, os canais 11 ao 19 sofrem interferência por co-canal.



**Figura 50. Canais utilizados: a) WH; b) rede WLAN e c) imagem real do espectro de frequência utilizado.**

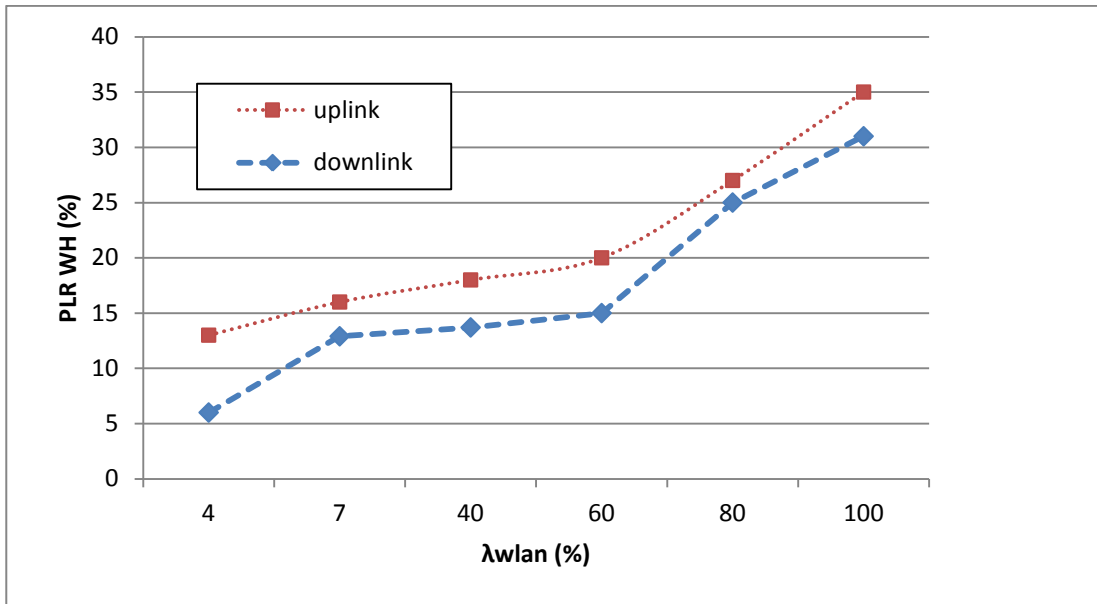
O trabalho de (SHUAIB et al., 2006), relata duas diferentes situações denominadas interferência por *downlink* e por *uplink*. É demonstrado por resultados experimentais que na ocasião em que o dispositivo com o padrão IEEE 802.15.4 é colocado próximo à fonte transmissora de dados, a interferência apresenta uma influência mais forte sobre a rede IEEE 802.15.4 do que se estivesse próximo do terminal receptor. A possível causa deve-se ao fato da fonte transmissora possuir uma potência de saída maior do que a receptora, neste caso um fenômeno fácil de entender, no entanto, ainda não deve ser esquecido a complexidade da coexistência de padrões sem fio (efeitos de propagação e reflexões), como comentado no trabalho de (YANG, et al., 2011). O seguinte ensaio teve o cenário modificado de forma que as fontes transmissoras estão mais próximas dos dispositivos WH, conforme Figura 51.



**Figura 51 Terceiro cenário utilizado - interferência por *uplink***

A Figura 52 apresenta os resultados, pode-se observar que apesar de um aumento nas taxas de perdas de pacote em relação ao experimento anterior o nível de confiabilidade manteve-se em 100% durante todo o experimento.





**Figura 52** Perda de pacotes do WH para condições de interferência por *uplink* e *downlink*

Para um ciclo de operação maior que 60%, no caso da situação de *downlink*, as perdas são superiores a 15%. No caso da interferência na situação de *uplink* as perdas são superiores a 15% a partir de uma interferência com ciclo de operação de 7% da rede WLAN. Chegando a perdas superiores a 30% na condição mais severa de interferência.

A través da ferramenta WH de detecção de energia foram registrados diversos dados referente ao tamanho do pacote, LQI detectado no dispositivo WH e nível de energia detectado no momento da recepção. As Figuras 53 e 55 demonstram respectivamente um cenário ausente de interferência e outro com interferência. No caso, são demonstrados resultados referentes a pacotes de 44 bytes no canal de recepção do dispositivo WH monitorado.

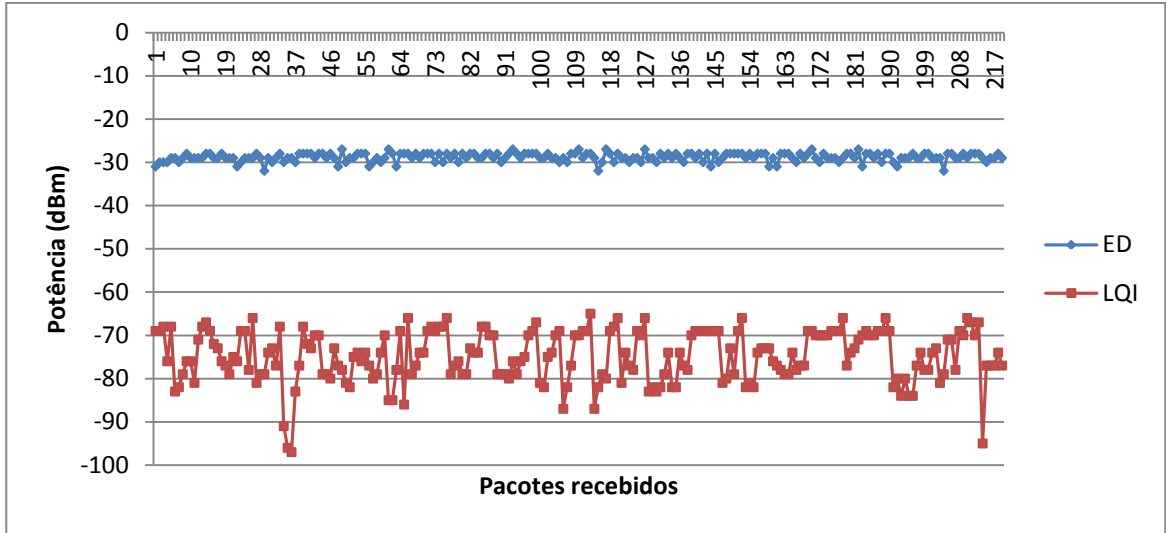


Figura 53 Níveis de energia e LQI medidos sem interferência.

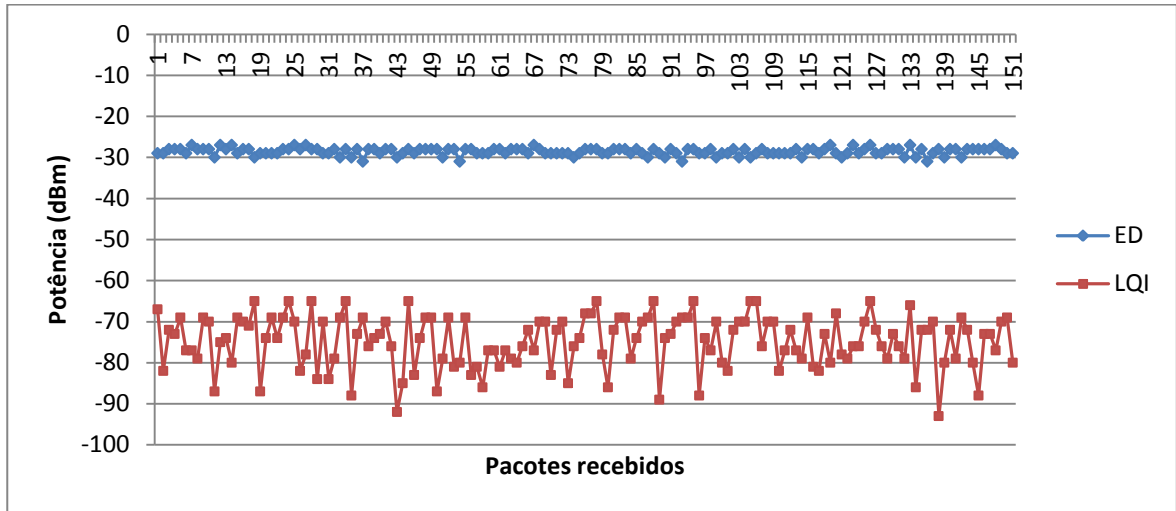
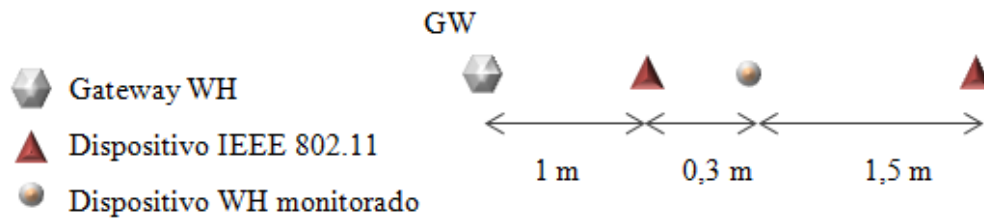


Figura 54 Níveis de energia e LQI medidos com interferência

### 5.2.3.3 CCA E IEEE 802.11g

Outro cenário proposto coloca o dispositivo WH em uma condição severa de coexistência com uma distância inferior a 0,5 metros do elemento interferente e com um ajuste de potência de saída inferior a 0 dBm. A Figura 55 ilustra a distribuição e os componentes envolvidos neste experimento.



**Figura 55 Distribuição dos dispositivos para análise de desempenho do CCA.**

O objetivo deste experimento é avaliar a eficácia do mecanismo CCA, uma vez que trata-se de uma técnica opcional dentro do protocolo. Abaixo são listadas as condições desta análise:

- Somente um dispositivo WH comunicando-se com o Gateway;
- Potência do rádio WH ajustado em -2 dBm;
- Rede WH limitada em 5 canais (16, 17, 18, 19 e 20) com sobreposição no canal 6 da rede IEEE 802.11g;
- Tamanho do pacote utilizado no IEEE 802.11g de 1500 bytes;
- Três situações foram propostas e estão descritas abaixo:
- Sem interferência;
- Com interferência e CCA desabilitado;
- Com interferência e CCA habilitado.

A Tabela 5 apresenta os resultados, pode-se verificar que sem interferência a rede WH manteve-se com 100% de confiabilidade, os pacotes foram entregues atendendo o requisito temporal. Sob condições de coexistência e com o mecanismo de CCA desligado, a rede WH apresentou apenas 11% de confiabilidade. Sob as mesmas condições de interferência utilizadas no teste anterior, mas com o CCA habilitado a rede WH teve uma confiabilidade de 21%.

Tabela 5 Desempenho WH com CCA

Modo	Publicação com sucesso	Publicação com falha	Confiabilidade
Sem interferência	60	0	100%
CCA desabilitado	7	56	11%
CCA habilitado	10	37	21%

A partir da análise dos resultados, as seguintes conclusões podem ser extraídas:

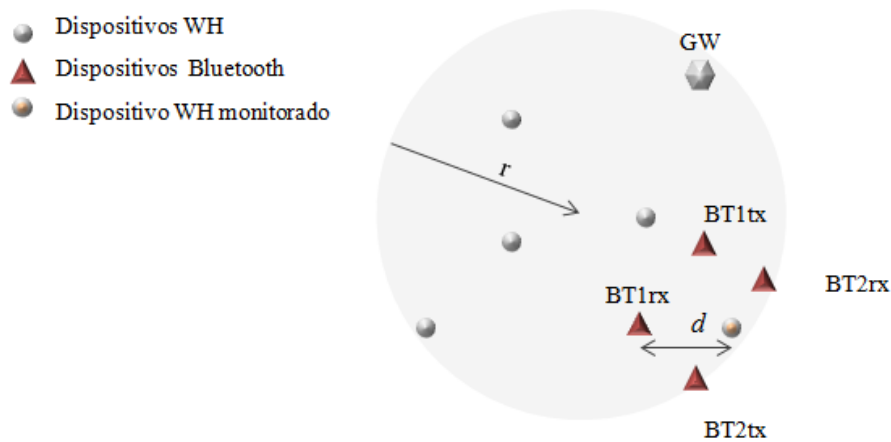
- Na ausência de interferência a rede WH teve um desempenho com perdas não significativas, as perdas praticamente nulas podem ser negligenciadas e causas podem estar relacionadas a interferência da própria rede WH quanto as questões de propagação, efeitos de reflexão, etc.
- As perdas de pacotes WH aumentam proporcionalmente com o aumento do ciclo de trabalho da rede WLAN;
- Quanto maior o pacote WLAN maior o número de perdas de pacote na rede WH;
- Apesar das perdas sob interferência o protocolo WH manteve sempre 100% de confiabilidade, ou seja, não houve atraso na entrega da variável primária do dispositivo, dentro do requisito temporal proposto.
- Quando o espectro do WH é limitado a apenas um canal livre de sobreposição de interferência, a taxa de perda de pacotes é maior, como esperado. Chegando no pior caso a perdas de até 35 %;
- Apesar de a rede interferente ter uma ocupação de apenas 20 % dos canais do WH, no cenário 1, deve se considerar os efeitos de interferência adjacentes a banda utilizada. Em uma análise do próprio dispositivo utilizado percebe-se que ainda existe potência residual em até 6 canais de deslocamento, vide Figura 59;
- A condição de interferência por *uplink* resultou em maior perda de pacotes da rede WH em aproximadamente 5% em relação a condição de *downlink*. Para um ciclo

de trabalho da rede WLAN superior a 80% as perdas ultrapassam os 25% em ambos os casos;

- Para os cenários com aproximações mais reais (distribuição de dispositivos, distância, potências usuais, canais disponíveis e taxa de ocupação) o nível de confiabilidade da rede manteve-se em 100%;
- A utilização do CCA melhora o desempenho da rede WH em condições de coexistência.

#### 5.2.4 Interferência do IEEE 802.15.1

Nesta etapa foi realizado um ensaio utilizando o padrão IEEE 802.15.1 como elemento interferente em uma rede WH. O cenário de teste é apresentado na Figura 56.



**Figura 56. Distribuição dos dispositivos Bluetooth na rede WH**

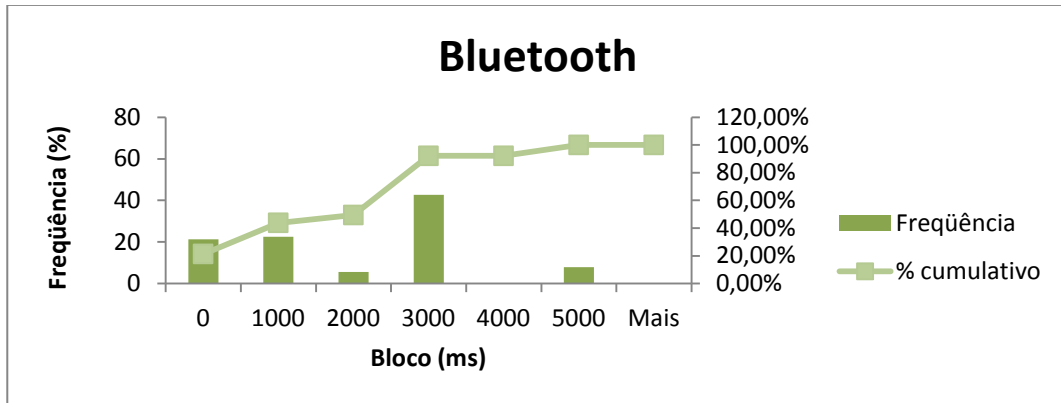
Foram utilizadas 4 estações Bluetooth para transmissão de dados. Para este experimento a transmissão de dados foi baseada em uma aplicação para transmissão de áudio, os parâmetros utilizados são apresentados na Tabela 6.

**Tabela 6 Tempo e tamanho dos pacotes utilizados no ensaio com Bluetooth**

MP3	Distribuição	Valor
Tamanho do pacote (bytes)	Constante	462
Tempo entre pacotes (s)	Constante	0,026

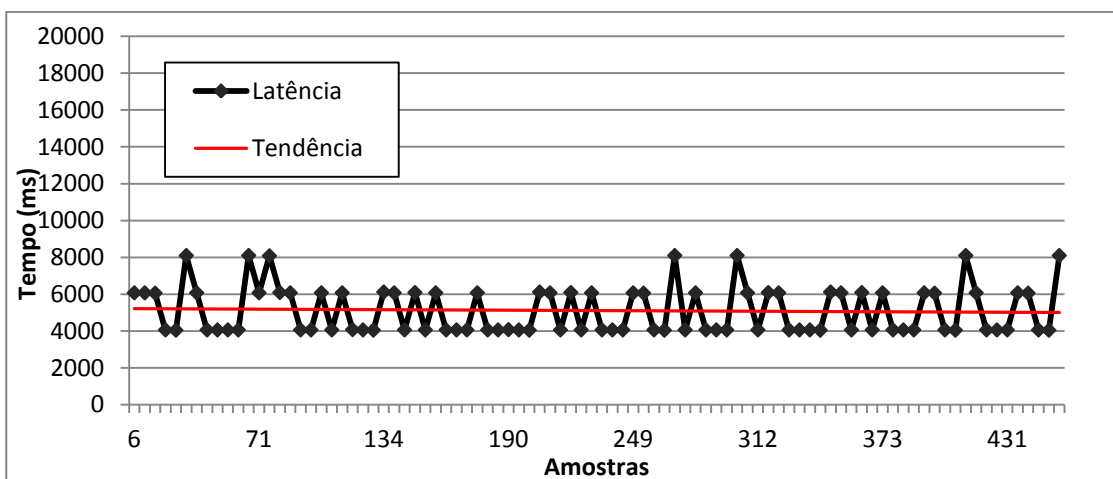
Para o ensaio realizado foram obtidos os seguintes resultados:

O jitter da rede WH é apresentado na Figura 57. Com o maior número de variações concentradas no bloco dos 3 segundos, mas não com muitos valores acima deste limiar. A taxa de pacotes perdidos registrada foi de 5,5 % e o nível de confiabilidade da rede manteve-se em 100%.



**Figura 57 Jitter da rede WH sob interferência do IEEE 802.15.1**

No caso da interferência com os dispositivos Bluetooth 21% das mensagens amostradas não apresentaram jitter, 22% apresentaram jitter de até 1 segundo e 92% das mensagens apresentaram jitter inferior a 3 segundos. A Figura 58 apresenta a latência da rede quando coexistindo com o IEEE 802.15.1.



**Figura 58 Latência da rede WH sob interferência do IEEE 802.15.1**

A interferência proveniente do IEEE 802.15.1 foi muito baixa mesmo em um cenário real proposto com interferências mais agravantes em relação ao número de dispositivos e a

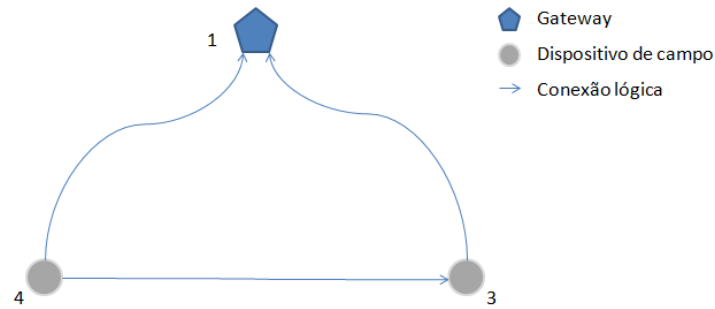
distância entre eles. Uma das razões desta baixa influência deve-se ao fato da banda do Bluetooth ser muito estreita (1 MHz) em relação ao WH, além dos mecanismos do Bluetooth para evitar colisões. Conforme (CHEN, et al., 2010) a interferência entre dispositivos Bluetooth e WH podem ser considerados ruídos e assim negligenciado.

### **5.2.5 *Wireless*HART x *Wireless*HART**

O próximo experimento realizado teve o objetivo de investigar o desempenho de uma rede WH coexistindo com outra rede WH. Como já descrito em capítulos anteriores o padrão WH utiliza o TDMA para realizar o acesso ao meio, ou seja, isto implica em uma divisão ordenada no tempo para cada rádio transmitir ou receber um determinado pacote de dados. Uma interferência proveniente de outra rede baseada no mesmo tipo representa um dos casos de pior desempenho, no entanto o protocolo WH permite a coexistência com outra rede WH desde que as redes diferenciem-se na identificação da rede (*Network ID*). De acordo com (CHEN, et al., 2010), se duas redes transmitirem ao mesmo tempo no mesmo canal, ambas devem falhar. Uma maneira de realizar uma análise da coexistência entre redes WH é através de um cenário com redes distintas, este cenário deve conter pelo menos dois grupos de dispositivos associados a diferentes gerenciadores de rede. No entanto, para obtenção de dados significativos tal análise deve se estender por um tempo demasiado longo, uma vez que possíveis colisões de pacotes ficam intrinsecamente condicionados a coincidências no tempo e na frequência, como já discutido no capítulo 3. Para uma análise de coexistência mais eficaz entre redes WH, este trabalho propõem a manipulação das conexões existentes entre os dispositivos de uma única rede de forma que seja possível gerar e controlar colisões de forma determinística entre os pacotes de diferentes dispositivos.

O cenário proposto é composto por dois dispositivos de campo WH e um gateway comercial, os equipamentos foram distribuídos conforme Figura 59. A primeira etapa do

experimento consiste em analisar a formação da rede WH: topologia lógica e conexões. A partir da inicialização da rede, e sua concreta formação, um mapa das conexões foi obtido a partir da ferramenta de dados com acesso pela porta de manutenção dos dispositivos.



**Figura 59 Distribuição e conexão dos dispositivos WH**

A leitura das conexões utilizados pelo dispositivo 3 e 4 é apresentada nas Tabelas 7 e 8 respectivamente.

**Tabela 7 Conexões do dispositivo 3**

Link Index	Superframe ID	Time Slot	CH Offset	Nickname	Option	Type
0	1	212	2	65535	RX	Broad
1	0	986	1	1	TX	Normal
2	0	1	0	1	TX/RX	Discovery
3	4	115	7	65535	TX	Broad
4	0	218	5	1	TX	Normal
5	1	230	1	63872	TX	Join
6	1	242	3	65535	RX	Broad
7	0	367	3	63872	RX	Join
8	0	474	5	1	TX	Normal
9	0	730	3	1	TX	Normal
10	0	346	2	1	TX	Normal

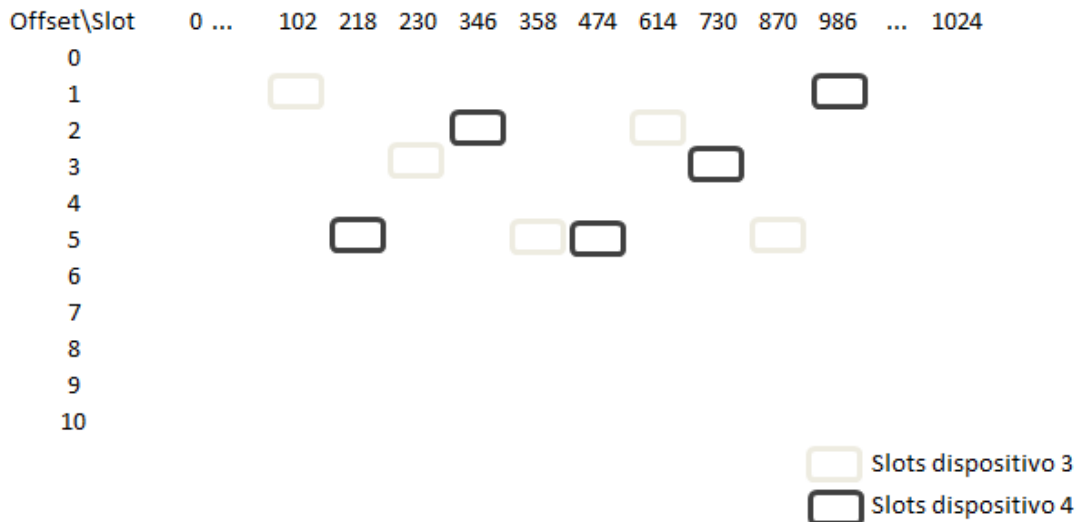


**Tabela 8 Conexões do dispositivo 4**

Link Index	Superframe ID	Time Slot	CH Offset	Nickname	Option	Type
0	1	212	2	65535	RX	Broad
1	0	870	5	1	TX	Normal
2	0	1	0	1	RX/TX	Discovery
3	0	102	1	1	TX	Normal
4	4	103	7	65535	TX	Broad
5	1	226	4	63872	TX	Join
6	1	227	4	65535	RX	Broad
7	0	358	5	1	TX	Normal
8	0	614	2	1	TX	Normal
9	0	630	4	63872	RX	Join
10	0	230	3	1	TX	Normal

As linhas sombreadas representam as conexões utilizadas para o envio e recebimento de DLPDUs do tipo comando e dados.

Nesta rede pode ser observado que o gerenciador de rede está utilizando pelo menos 3 superframes. Neste caso o superframe de interesse é o cuja identificação é 0, ou seja, onde os dados do tipo comando são enviados e recebidos. A Figura 60 ilustra os quadros de tempo do tipo Normal direcionados para a comunicação com o gateway em seus respectivos deslocamentos de frequência para ambos os dispositivos.



**Figura 60 Quadros de tempo dos dispositivos 3 e 4 dentro do superframe 0**

Na estratégia de análise os dispositivos receberam os mesmos requisitos temporais para a publicação da variável de processo. Ambos os dispositivos publicam a variável de processo a cada 4 segundos. O superframe 0 tem o tamanho de 1024 quadros de tempo o que corresponde a 10,24 segundos.

Através da análise da rede podemos destacar:

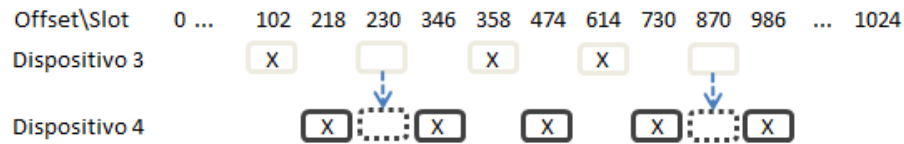
- Os dispositivos possuem 5 *slots* de tempo disponíveis para a transmissão da variável primária, com espaçamento mínimo de 640 ms e máximo de 1280 ms. Representando pelo menos 3 oportunidades para o envio do valor da variável primária, de maneira a garantir o determinismo da rede;
- Observa-se que a política de gerenciamento adotada pelo gerenciador de rede, distribui conexões alternativas que antecedem o limiar do requisito temporal, sendo que cada conexão utiliza um canal de frequência diferente. Caso ocorra uma colisão em uma das transmissões, ainda há a possibilidade de outras tentativas diversificando no tempo e na frequência.

#### **5.2.5.1 Interferência de uma rede *WirelessHART***

Como já comentado anteriormente, uma dificuldade para um ensaio de duas redes WH concorrentes é provocar a colisão de pacotes, uma vez que ambas as redes realizam o salto de canal para cada transmissão. Para obtermos um ambiente determinístico quanto à colisão de pacotes WH esta segunda etapa da análise consiste em manipular as conexões dos dispositivos presentes na rede para gerar a sobreposição de mensagens WH. Neste cenário o dispositivo 3 foi denominado como dispositivo interferente e o dispositivo número 4 denominado como dispositivo vítima e ambos tiveram seus mapas de conexões reescritos.

No dispositivo 3 foram excluídos 3 das 5 conexões, sendo mantido apenas duas conexões para que a transmissão da mensagem possa ocorrer dentro do requisito temporal, ou seja, uma conexão disponível dentro de um intervalo de 4 segundos. Enquanto no dispositivo

4 foram excluídos todos as conexões e adicionado duas novas conexões clonadas do dispositivo 3, vide Figura 61.



**Figura 61 Alteração das conexões dos dispositivos da rede WH**

A estratégia utilizada força uma colisão de pacotes sempre que ocorre uma transmissão do dispositivo 4, ou seja, sempre que ocorre uma transmissão do dispositivo 3 também.

No experimento manteve-se uma simetria entre as distâncias dos dispositivos (interferente e vítima) em relação ao gateway da rede com o objetivo de manter uma relação de potência semelhante para todos os dispositivos. É importante destacar que este experimento foi realizado em laboratório, ambiente interno, com potencial ocorrência dos fenômenos de propagação de rádio frequência tais como reflexões, multi caminhos e atenuação. A potência de ambos dispositivos foi variada, sempre com um dispositivo apresentando uma potência de saída maior que o dispositivo concorrente. Inicialmente esperava-se que os dois dispositivos tivessem seus pacotes corrompidos, no entanto, os resultados demonstraram no cenário utilizado que o dispositivo com maior potência foi capaz de entregar o pacote enquanto o de menor potência apresentou falha. Observa-se também neste experimento que, mesmo o dispositivo que recebeu as conexões designadas para outro dispositivo, quando ajustado com uma potência maior que seu concorrente ou mais próximo do gateway teve seu pacote aceito pelo ponto de acesso WH.

O experimento acima utiliza um processo de teste de colisão determinístico e demonstra a grande robustez do protocolo WH, uma vez que mesmo sob circunstâncias bem severas (colisão com o próprio protocolo), ainda foi possível realizar a entrega do pacote. Através da análise das conexões pode-se afirmar que:

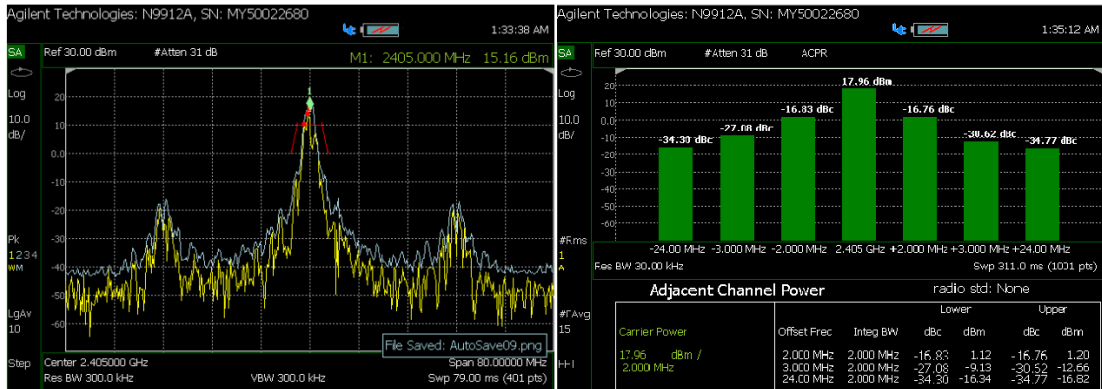
Quanto maior o número de nodos vizinhos, maior o número de possibilidades de caminhos livres de interferência resultando em maior robustez;

Quanto maior o requisito temporal para a entrega de um determinado dado, maior o número de conexões disponíveis e as chances de uma entrega bem sucedida.

### **5.2.6 Interferência por Canal Adjacente**

Interferências por canais adjacentes ocorrem por meio de transmissões de dispositivos que operam próximos ao mesmo canal de RF utilizado por outro receptor. É tipicamente uma das interferências mais comuns às quais os receptores ficam expostos, uma vez que podem ser provenientes da própria rede utilizada.

A interferência por canal adjacente, mesmo quando relativamente fraca, pode afetar diretamente a relação sinal ruído de um receptor. Normalmente mais transmissores na vizinhança significa mais interferência e, no caso do WH, o controle do enlace é do tipo TDMA, sendo que há apenas um dispositivo por vez transmitindo dados. No entanto, ressalta-se a sobreposição de canais de outros padrões (além dos canais utilizados) e da possibilidade de utilização de mais de uma rede WH para uma determinada área. Neste âmbito, a quantidade de potência de um dispositivo com camada física padrão IEEE 802.15.4 pode estender sua transmissão para canais adjacentes. A Figura 62-a apresenta o sinal de potência de saída modulado para o canal 11, utilizado no WH (centro em 2405 MHz).

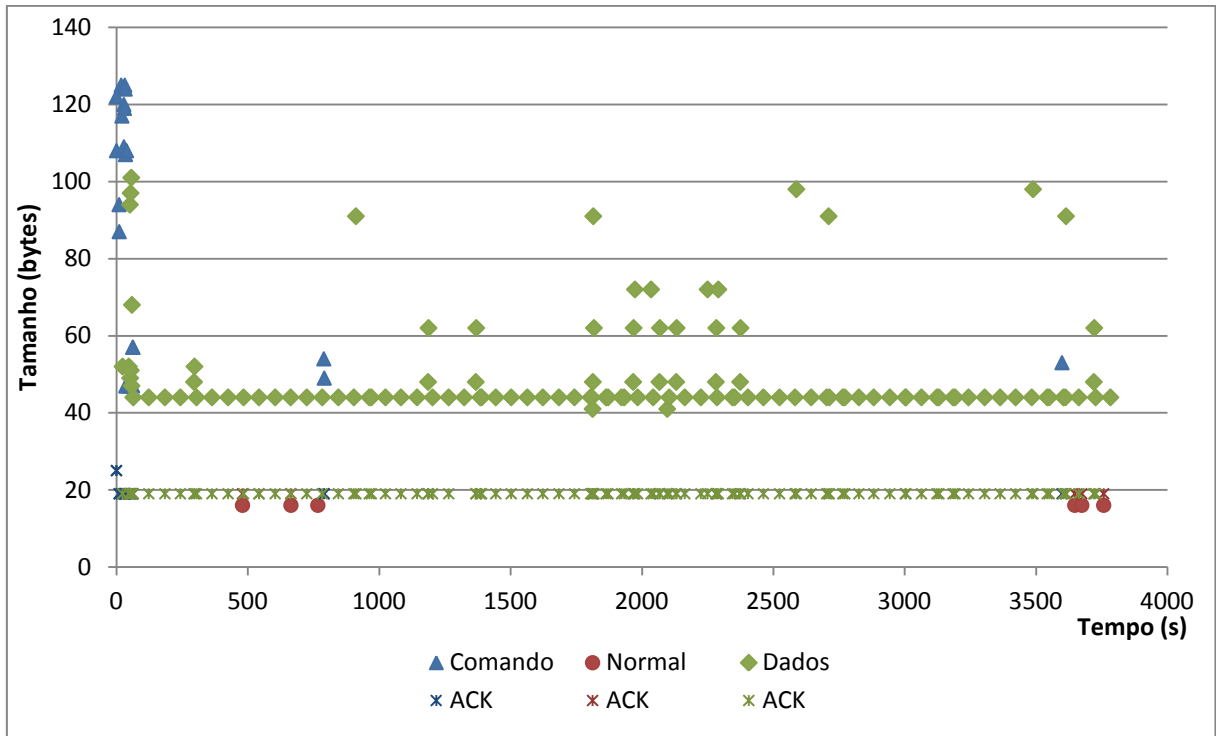


**Figura 62 a) Sinal de potência modulado. Em b, as relações de intensidades com canais adjacentes.**

Pode-se verificar que há espúrios além do centro da banda do canal desejado, chegando com uma intensidade de até  $-34,77$  dBc para um deslocamento de frequência de quase cinco canais  $802.15.4$  (canal 16 –  $2430$  MHz), vide Figura 62-b. Estes espúrios são imagens do sinal modulado, e podem se estender por várias frequências harmônicas do sinal original. Os efeitos podem ser reduzidos a partir de uma configuração adequada da potência de saída do dispositivo, observável em experimentos de laboratório.

### 5.2.7 Tamanho e Tráfego de Pacotes de uma Rede WH

Como apresentado no trabalho de (HAN et al., 2007) e (NOBRE, et al., 2011) a taxa de erro de pacotes cresce com o aumento do tamanho do pacote, sendo estimado nas simulações um PER variando de 1,5% até 3,2% do menor até o maior pacote possível a ser transmitido. Nesta etapa é levantado o fluxo de mensagens que ocorre em uma rede WH. A Figura 63 ilustra os dados da comunicação de um dispositivo durante aproximadamente 70 minutos, as mensagens são classificadas por prioridade e tamanho. As mensagens de maior prioridade são as DLPDUs do tipo Comando, seguindo de Dados e Normal.



**Figura 63 Fluxo de pacotes de uma rede WH**

Pode-se observar que o período mais crítico da rede quanto a uma probabilidade de colisão relacionada ao tamanho do pacote ocorre nos primeiros 60 segundos a partir do momento que o dispositivo inicia o processo de associação à rede. Isto ocorre pela demanda dos diferentes comandos contendo informações das tabelas, mapa de canais, superframes, etc. necessários para o dispositivo ingressar à rede. A norma WH permite a associação de comandos em um único pacote dependendo da estratégia utilizada pelo gerenciador de rede, o que implica na ocorrência de pacotes com maior quantidade de bytes. Para a rede apresentada, durante o decorrer das comunicações, em uma situação normal de operação, são mais frequentes pacotes com tamanho de 44 bytes referentes a publicação das variáveis do processo.

## 6 CONCLUSÃO

Neste trabalho, foi proposto uma avaliação do desempenho do protocolo de comunicação *WirelessHART* em condições de coexistência com outros padrões que utilizam a mesma faixa de frequência do espectro. Os resultados demonstram que a rede WH é prejudicada sob certas condições de coexistência variando a intensidade da degradação em função do tamanho dos pacotes e do nível de ocupação dos elementos interferentes.

Diferentes ensaios foram realizados com os padrões IEEE 802.11g, IEEE 802.15.1 e como próprio padrão WH. Para a pior condição de coexistência com o IEEE 802.11g houve uma perda de pacotes em torno de 35 %, já no caso de coexistência com o IEEE 802.15.1 as perdas de pacotes não ultrapassaram 6 % no pior caso. Dependendo da demanda das redes concorrentes utilizadas observa-se diferentes variações nos tempos de entrega das mensagens implicando em certa instabilidade. No entanto, nos cenários propostos com aplicações mais reais quanto à distribuição de dispositivos, níveis de potência, taxas de transmissão e canais utilizados, apesar das perdas registradas o nível de confiabilidade do protocolo manteve-se em 100%, ou seja, garantiu a entrega de dados dentro dos requisitos temporais propostos. As análises também demonstram que, quanto menor o requisito temporal, menor o número de conexões disponíveis e maior as chances de não atendimento do período determinado para a entrega das mensagens, uma importante consideração que deve ser avaliada em função dos requisitos de controle de um determinado processo. Também foi mensurada a eficácia do mecanismo de CCA do WH para coexistência com o IEEE 802.11g. No caso observado, foi constatado que os dispositivos com o modo CCA habilitado apresentam um nível de confiabilidade maior em relação a situação a qual o CCA estava desabilitado. Uma questão relevante, uma vez que a utilização do CCA é opcional no protocolo e deve aumentar o consumo de energia do dispositivo.

Apesar dos resultados obtidos, ainda ficam lacunas para medições dos limites de suscetibilidade do protocolo quanto aos níveis de intensidade de potência interferente e deslocamento de frequência máximo permitido entre outras variáveis. Medições mais adequadas devem ser efetuadas em ambientes com o meio controlado através de equipamentos adequados. No capítulo de trabalhos futuros é apresentado um método para tal estudo com equipamentos que permitem o controle de propagação e atenuação dos dispositivos da rede.

Atualmente, para ambientes industriais mais críticos como, por exemplo, a indústria de óleo e gás as áreas são classificadas e muitas vezes locais onde os processos ocorrem são isentos de interferência por outros padrões, tal como o IEEE 802.11. No entanto, os benefícios que os sistemas de comunicação sem fio apresentam movem esse campo da automação para a utilização de padrões internacionais de comunicação sem fio, ainda associado às perspectivas de uso de tais dispositivos existe uma grande tendência da integração de comunicação sem fio industrial com a aplicações da tecnologia da informação. Todas estas questões servem de base para a importância deste tipo de pesquisa assim como a continuidade deste trabalho de forma que se possa cada vez mais entender a complexidade destes sistemas e assim permitir uma busca para o desenvolvimento de tecnologias ainda mais confiáveis.



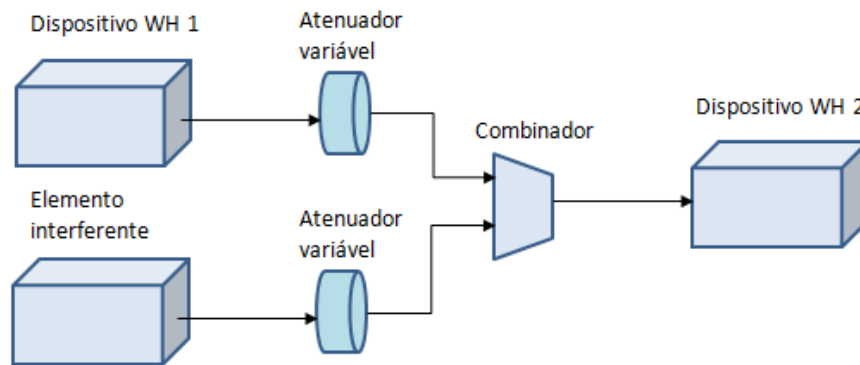
## **7 TRABALHOS FUTUROS**

Neste capítulo são introduzidos possíveis métodos para analisar o desempenho do protocolo WH, assim como propostas de mecanismos que podem trazer um desempenho mais confiável deste padrão em condições de interferência.

### **7.1 PROPOSTA DE ANÁLISE DE DESEMPENHO E LIMITES DE POTÊNCIA INTERFERENTE**

O sinal recebido é uma combinação dos diversos fenômenos de propagação envolvidos, os quais são dependentes de diversos fatores como tipos de materiais do ambiente, número de objetos, tamanho, forma, ruídos, interferência, etc. Torna-se uma tarefa complicada identificar os limiares de suscetibilidade da relação sinal ruído e interferência dentro de um enlace de comunicação, uma vez que é necessário um controle mais apurado do meio para as medições adequadas como, por exemplo, câmaras anecoicas que permitem realizar análise sem as influências externas que acabam alterando os resultados.

Para análises futuras é proposto uma arquitetura de dispositivos para avaliar com maior precisão os efeitos e limiares de potência das fontes interferentes e da fonte desejada, vide Figura 61. O cenário proposto é composto por um conjunto de atenuadores variáveis conectados respectivamente nos transceptores do dispositivo WH e do dispositivo interferente (IEEE 802.15.1, IEEE 802.11, WH e ZigBEE). O sinal desejado e o interferente são atenuados de forma independente e combinados através de um combinador de potência. Todos os dispositivos devem ser conectados utilizando cabos coaxiais de baixa perda de forma a confinar o ambiente de propagação com a menor perda possível.



**Figura 64 Cenário proposto para análise de interferência**

A partir deste cenário pode-se analisar a relação de perda de pacotes com a taxa de sinal e interferência e ainda os efeitos do deslocamento de frequência de diferentes padrões que operam na banda de 2.4 GHz.

## 7.2 PROPOSTA DE MECANISMOS ATIVOS DE COEXISTÊNCIA

A principal questão relacionada à coexistência é o compartilhamento adequado dos recursos disponíveis para os sistemas de comunicação, no caso, frequência, espaço e tempo. Os mecanismos avaliados e descritos neste trabalho referente ao protocolo WH operam de forma passiva, ou seja, independente de haver algum tipo de interferência coexistindo durante a comunicação. Aqui são descritos algumas possíveis propostas para implementar meios ativos de coexistência dentro do protocolo WH.

Na questão da frequência, o princípio básico refere-se ao uso de um canal livre de interferência para a comunicação. No protocolo WH é possível determinar uma lista de canais a serem bloqueados, desta maneira através da intervenção do planejador da rede pode-se mitigar ou evitar interferências permanentes de outras redes. Porém a partir do momento que a rede é iniciada o gerenciador de rede envia uma sequência rígida de canais previamente determinada para os dispositivos conforme sua associação. No caso do surgimento de uma fonte de interferência móvel ou uma fonte de interferência ter sido iniciada após o início da rede WH, a lista negra já não deve mais trazer a eficiência proposta. Uma possível solução

para estas situações pode ser a implementação de uma lista negra dinâmica de canais, no entanto, atualmente um dos grandes desafios é sincronizar um novo mapa de canais entre os dispositivos da rede e não perder o determinismo da rede durante a transição das configurações.

Quanto ao compartilhamento do espaço, soluções podem ser apresentadas através da modulação dinâmica da potência do dispositivo WH em relação à distância e a qualidade do enlace. O melhoramento da eficiência espectral e o aumento da capacidade implicam na minimização da interferência, que, por sua vez, está diretamente relacionada ao nível de potência transmitida de cada terminal. Para um controle dinâmico da potência de saída dos dispositivos WH deve se ter atenção ao fato da rede ser do tipo malha e haver parâmetros de diferentes dispositivos os quais devem ser mensurados de acordo de forma a manter o nível de qualidade da comunicação.

Talvez o maior desafio seja referente a soluções relacionadas à divisão de tempo, as quais são abordadas através da cooperação entre vítima e interferente, ou seja, a solução deve trabalhar simultaneamente com a vítima e o elemento interferente por meio de controle dos intervalos de tempo. Soluções relacionadas ao compartilhamento de tempo também são utilizadas através do controle de tráfego de dados. Intervalos de grandes pacotes podem reduzir a probabilidade de conflito de pacotes, porém a sincronização de diferentes protocolos envolvem grandes desafios iniciando pela conservação do determinismo da rede.

## REFERÊNCIAS

ANGRISANI, L. et al. Experimental Study of Coexistence Issues Between IEEE 802.11b and IEEE 802.15.4 Wireless Networks. **Journal in IEEE Transactions on Instrumentation and Measurement**, [S.l.], v. 57, p. 1514-1523, 2008.

BERTOCCO, M. et al. Investigating wireless networks coexistence issues through an interference aware simulator. In: EMERGING TECHNOLOGIES AND FACTORY AUTOMATION, 2008, Hamburg. **Proceedings...** New York: IEEE Press, 2008. p. 1153-156.

CHEN, D.; NIXON, M.; MOK, A. (Ed.). **WirelessHART: Real-Time Mesh Network for Industrial Automation**. New York: Springer, 2010.

BOTTA, A.; DAIANOTTI, A.; PESCAPÉ, A. A tool for the generation of realistic network workload for emerging networking scenarios. **Journal Computer Networks**, [S.l.], v. 56, p. 3531-3547, 2012.

DOMINICIS, C. M. et al. Investigating WirelessHART coexistence issues through a specifically designed Simulator. In: IEEE INTERNATIONAL INSTRUMENTATION AND MEASUREMENT TECHNOLOGY CONFERENCE, 2009, Singapore. **Proceedings...** New York: IEEE Press, 2009. p.1085-1090.

FERRARI, P. et al. Performance Assessment of a WirelessHART network in a real-world testbed. In: IEEE INSTRUMENTATION AND MEASUREMENT TECHNOLOGY CONFERENCE, 2012, Graz. **Proceedings...** New York: IEEE Press, 2012. p. 953 – 957.

FREESCALE, **MC1322X** : Advanced ZigBee – Compliant Soc Plataform for the 2.4 GHz IEEE 802.15.4 Standard Reference Manual, Rev. 1.6. 2012.

GOLMIE, N. (Ed.). **Coexistence in Wireless Networks: Challenges and System-Level Solutions in the Unlicensed Bands**. New York: Cambridge University Press, 2006.

GOLMIE, N. Performance Evaluation of a Bluetooth Channel Estimation Algorithm. In: IEEE INTERNACIONAL PERSONAL, INDOOR AND MOBILE RADIO COMMUNICATIONS, 2002, Lisboa. **Proceedings...** New York: IEEE Press, 2002. p. 156-160.

HAN, B.; SEUNGJOON, L. Efficient packet error rate estimation in wireless networks. In: IEEE INTERNATIONAL CONFERENCE ON TESTBEDS AND RESEARCH INFRASTRUCTURE FOR THE DEVELOPMENT OF NETWORKS AND COMMUNITIES, 2007, Lake Buena Vista. **Proceedings...** New York: IEEE Press, 2007. p 1-9.

HART COMMUNICATION FOUNDATION. **HCF\_SPEC-065, Rev. 1.0.** Austin: HCF, 2007. Parte da norma.

HART COMMUNICATION FOUNDATION. **HCF\_SPEC-075, Rev 1.1.** Austin: HCF, 2008. Parte da norma.

HART COMMUNICATION FOUNDATION. **HCF\_SPEC-085, Rev. 1.2.** Austin: HCF, 2009. Parte da norma

HART COMMUNICATION FOUNDATION. **HCF\_SPEC-155, Rev. 1.1.** Austin: HCF, 2008. Parte da norma.

HART COMMUNICATION FOUNDATION. **HCF\_SPEC-290, Rev. 1.1.** Austin: HCF, 2008. Parte da norma.

HAYKIN, S.; MOHER, M. (Ed.). **Sistemas Modernos de Comunicações Wireless.** Porto Alegre : Artmed Editora, 2008.

HOWLADER, M.; KIGER, C. J.; EWING, P. D. (Ed.). **Industrial Wireless Protocols in the Nuclear Facility Environment.** Washington, DC: Oak Ridge National Laboratory, 2007.

HUO, H. et al. Coexistence Issues of 2.4 GHz Sensor Networks with other RF devices at Home. In: INTERNATIONAL CONFERENCE ON SENSOR TECHNOLOGIES AND APPLICATIONS, 2009. Athens. **Proceedings...** New York: IEEE press, 2009. p. 200-205.

INTERNATIONAL ELECTROTHERNICAL COMMISSION. **IEC 62591, Rev. 1.0.** Massachusetts, 2010. Parte da norma.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEER. **Part 15.4,** Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). New York: IEEE Computer Society, 2006. Parte da norma.

LIMA, C. P. et al. Porta de Manutenção para Comissionamento e Análise Local de Redes WirelessHART. In: CONGRESSO BRASILEIRO DE AUTOMÁTICA, 19., 2012, Campina Grande. **Anais...** Campinas: SBA, 2012. v. 1. p. 4923-4929.

MOLISCH, A. F. (Ed.). **Wireless Communications.** Chennai: Laserwords, 2005.

MULLER, I.; NETTO, J.C.; PEREIRA, C.E. WirelessHART field devices. **Journal IEEE INSTRUMENTATION AND MEASUREMENT,** [S.l.], v.14, p.20 -25, 2011.

MULLER, I. et al. Development of WirelessHART Compatible Field Devices. In: IEEE INTERNATIONAL INSTRUMENTATION AND MEASUREMENT TECHNOLOGY CONFERENCE, 2010, Austin. **Proceedings...** New York: IEEE Press, 2010. p. 1430-1434.

NOBRE, M. H. R. **Análise de Desempenho Baseada em Simulação de Redes WirelessHART.** 2011. 73 p. Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal do Rio Grande do Norte, Natal, 2011.

PETERSEN, S. et al. Requirements, Drivers and Analysis of Wireless Sensor Network Solutions for the Oil and Gas Industry. In: IEEE CONFERENCE ON EMERGING

TECHNOLOGIES AND FACTORY AUTOMATION, 2007, Patras. **Proceedings...** New York: IEEE Press, 2007. p. 219-226.

PETERSEN, S.; CARLSEN, S. Performance Evaluation of WirelessHART for Factory Automation. In: IEEE CONFERENCE ON EMERGENT TECHNOLOGIES AND FACTORY AUTOMATION, 2009, Mallorca. **Proceedings...** New York: IEEE Press, 2009. p. 1-9.

PETROVA, M. et al. Performance Study of IEEE 802.15.4 Using Measurements and Simulations. In: IEEE WIRELESS COMMUNICATIONS AND NETWORKING CONFERENCE, 2006, Las Vegas. **Proceedings...** New York: IEEE Press, 2006. p. 487-492.

POOLIN, S. et al. Harmful coexistence between IEEE 802.15.4 and 802.11. In: INTERNATIONAL CONFERENCE ON COGNITIVE RADIO ORIENTED WIRELESS NETWORKS AND COMMUNICATIONS, 2008, Singapore. **Proceedings...** New York: IEEE Press, 2008. p. 1-9.

RAPPAPORT, T. S. (Ed.). **Wireless Communications** – Principles & Practice. New Jersey: Prentice Hall, 1996.

STALLINGS, W. (Ed.). **Data And Computer Communications**. New Jersey: Prentice Hall, 2007.

SHUAIB, K. et al. Coexistence of Zigbee and WLAN, a performance study. In: IEEE WIRELESS TELECOMMUNICATIONS SYMPOSIUM, 2006, Pomona. **Proceedings...** New York: IEEE Press. p. 1-6.

SIKORA, A.; GROZA, V. Coexistence of IEEE 802.15.4 with other Systems in the 2.4 GHz ISM Band. In: INSTRUMENTATION AND MEASUREMENT TECHNOLOGY CONFERENCE, 2005, Ottawa. **Proceedings...** New York: IEEE Press, 2005. p. 1786-1790.

SUBBU, K. P.; HOWITT, I. Empirical Study of IEEE 802.15.4 Mutual Interference Issues. In: IEEE CONFERENCE SOUTHEASTCON, 2007, Richmond. **Proceedings...** New York: IEEE Press, 2007. p. 191-195.

THOMESSE, J. P. Fieldbus Technology in Industrial Automation. **Journal in IEEE Proceedings**, [S.l.], v. 93, p. 1073-1101, 2005

TOVAR, E.; VASQUES, R. Real Time Fieldbus Communication using Profile Networks. **Journal Industrial Electronics**, [S.l.], v. 46, p. 1241-1251, 1999.

VERLOOCK, L. et al. Procedure for assessment of general public exposure from WLAN in offices and in wireless sensor network testbed. **Journal in Health Phys**, Belgium, v. 4, p. 628-638, 2010.

WENYUAN, X. et al. Jamming Sensor Networks: Attack and Defense Strategies. **Journal in IEEE Networks**, [S.l.], v. 20, p. 41-47, 2006.

WINTER, J.M. et al. WirelessHART Routing Analysis Software. In: BRAZILIAN SYMPOSIUM ON COMPUTING SYSTEM ENGINEERING, 2011, Florianópolis. **Anais...** Porto Alegre: SBC, 2011. p. 96-98.

YANG, D.; XU, Y.; GIDLUND, M. Wireless Coexistence between IEEE 802.11 and IEEE 802.15.4 – Based Networks: A Survey. **Journal of Distributed Sensor Networks**, [S. l.], v. 2011, p. 1-17, 2011.

YUAN, W. et al. A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g. In: IEEE SYMPOSIUM ON COMMUNICATIONS AND VEHICULAR TECHNOLOGY IN THE BENELUX, 2007, Delft. **Proceedings...** New York: IEEE Press, 2007. p. 1-5.