UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
CURSO DE ENGENHARIA DE CONTROLE E AUTOMAÇÃO

DYLAN MIELKE TIMM

FERRAMENTA PARA AVALIAÇÃO DE DESEMPENHO PONTO-A-PONTO DE REDES WIRELESSHART SOB INSTRUMENTAÇÃO PASSIVA

PORTO ALEGRE-RS
2018

DYLAN MIELKE TIMM

Ferramenta para Avaliação de Desempenho Ponto-a-ponto de Redes WirelessHART sob Instrumentação Passiva

Trabalho de Conclusão do Curso de Engenharia de Controle e Automação da Universidade Federal do Rio Grande do Sul, apresentado à Banca Julgadora como pré-requisito para aprovação na atividade.

Orientador: Ivan Müller

PORTO ALEGRE - RS

2018

DYLAN MIELKE TIMM

Ferramenta para Avaliação de Desempenho Ponto-a-ponto de Redes WirelessHART sob Instrumentação Passiva

Trabalho de Conclusão do Curso de Engenharia de Controle e Automação da Universidade Federal do Rio Grande do Sul, apresentado à Banca Julgadora como pré-requisito para aprovação na atividade.

PORTO ALEGRE, 26 DE JUNHO DE 2018

Banca Examinadora

_____

Prof. Marcelo Goetz

_____

Prof. Valner Brusamarello

_____

Prof. Renato Ventura

_____

Prof. Orientador Ivan Müller

AGRADECIMENTOS

À minha família, pelos constantes suporte, paciência e sustento.

Aos colegas da UFRGS, pelo companheirismo nessa jornada compartilhada.

Ao professor Ivan Müller, pela oportunidade de aprendizado, acompanhamento e tutoria.

Aos colegas do LASCAR, especialmente a Leomar Mateus Radke, pelo apoio nesse projeto e pela parceria nas tardes de estudo.

Aos demais professores e funcionários da UFRGS, pela responsabilidade, pelo senso de urgência e por todo o valor agregado à minha formação pessoal e profissional.

RESUMO

Este trabalho consiste no desenvolvimento e aplicação de uma ferramenta para análise de robustez de redes sem fio WirelessHart sob instrumentação passiva através da avaliação de performance ponto-a-ponto. Após a elaboração de um ambiente em Java com integração a um dispositivo passivo *sniffer*, é feita a avaliação do comportamento de uma rede WirelessHart quando sujeita a interferências de comunicação por co-canal do tipo coexistência, observando-se a dinâmica da comunicação ao longo do tempo em termos de taxa de pacotes perdidos e nível de sinal entre dispositivos vizinhos.

A partir da ferramenta, correlaciona-se a depreciação da comunicação com as interferências inseridas e avalia-se a extensão da capacidade de ajuste de uma rede WirelessHart para evitar o comprometimento das métricas de confiabilidade e robustez.

Palavras-chave: WirelessHART, confiabilidade, robustez, *sniffer*, coexistência, comunicação sem fio.

ABSTRACT

This paper presents the development and application of a tool for robustness analysis of WirelessHART networks under passive instrumentation through the evaluation of its peer-to-peer performance. After the elaboration of a Java ambient integrated to a *sniffer* passive device, an evaluation of a WirelessHART network when subjected to co-channel communication interferences such as coexistence is due, observing the dynamics of communication throughout time in terms of packet loss rate and signal level between neighbors.

The developed tool enables the correlation between the communication depreciation and the input interferences, evaluating the extension of a WirelessHART network responsiveness in avoiding the compromise of its criteria for reliability and robustness.

Key-words: WirelessHART, reliability, robustness, sniffer, coexistence, wireless communication.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACK – *Acknowledge*

ASN – *Absolute Slot Number*

CRC - *Cyclic Redundancy Check*

ED – *Energy Detection*

IEC - *International Electrotechnical Commission*

IEEE - Instituto de Engenheiros Eletricistas e Eletrônicos

ISM - *Industrial, Scientific and Medical*

ITU-R - *International Telecommunication Union – Radiocommunication*

LQI – *Link Quality Indicator*

OSI - *Open Systems Interconnection*

PER – *Packet Error Rate*

PDU – *Protocol Data Unit*

RSSI – *Received Signal Strength Indicator*

SNR – *Signal-Noise Ratio*

TDMA - *Time Division Multiple Access*

UFRGS – Universidade Federal do Rio Grande do Sul

SUMÁRIO

CAPÍTULO 1 - INTRODUÇÃO

A constante renovação da tecnologia de automação e o aumento da competição no fornecimento de soluções de engenharia impactam no cenário industrial de forma paralela. Os avanços em *software* e *hardware* direcionam desenvolvedores a questionarem continuamente o estado da arte e trazerem inovações que tragam redução de custos, visando crescente participação de mercado em seus segmentos.

Dentre as reduções de custo mais comuns ao longo da evolução da automação industrial está a redução de *hardware* – em especial, de cabeamento. Muito do sucesso de protocolos como o Foundation FieldBus, o ProfiBus e o HART vem do emprego de meios de comunicação do tipo barramento e a possibilidade de implementação de novas topologias de rede, que agregam confiabilidade na entrega da informação e eliminam custos em material e mão-de-obra para instalação.

Protocolos de comunicação *wireless* (sem fio) se destacam economicamente pelo ainda mais reduzido custo de instalação. Enquanto dispositivos cabeados requerem uma infraestrutura dedicada comparativamente maior, tanto para comunicação quanto para alimentação, dispositivos *wireless* inserem no meio industrial um conceito diferenciado do *plug and play* (ligar e usar), onde o impacto na infraestrutura é fracionado e se introduz maior flexibilidade para reestruturações e projetos tipo *retrofit* (ARAMPATZIS; LYGEROS; MANESIS, 2005). Considerando, ainda, a utilização de dispositivos alimentados à bateria, o impacto em infraestrutura é mínimo.

Além da vantagem em custo, protocolos *wireless* apresentam a característica de escalabilidade, onde a possibilidade de diversificação na elaboração de novas topologias se mostra comparativamente maior, frequentemente sem qualquer necessidade de alteração de *hardware* e, muitas vezes, de forma autônoma, visando otimizar a estratégia de roteamento

dos pacotes de informação (WANG; ZHANG; WANG, 2006). A possibilidade de otimização do tráfego de informação, alinhada à capacidade de instrumentação em ambientes anteriormente proibitivos ou de difícil acesso (como máquinas rotativas ou motorizadas), traz aos protocolos *wireless* uma vantagem técnica sobre protocolos cabeados, além da vantagem econômica.

Contudo, protocolos *wireless* apresentam dificuldades particulares de projeto que dispositivos cabeados já têm amenizados, devido ao maior tempo de mercado e consequente maior evolução. A confiabilidade no envio e entrega de dados se torna mais desafiadora na tecnologia sem fio, considerando-se que o meio pelo qual a informação trafega apresenta possibilidades de interferência mais acentuadas do que o meio cabeado, como o ruído e a coexistência (WANG; SEAH; KONG, 2007). Efeitos adversos de tráfego, especialmente os mais comuns em ambientes industriais, mostram-se empecilhos na tarefa de trazer protocolos de comunicação *wireless* ao nível de competição comercial de protocolos cabeados já bem estabelecidos no mercado. Segundo Dominics *et al* (2009), os padrões *wireless* atuais não tratam com considerável enfoque o problema de possível coexistência com outros protocolos, não apresentando mecanismos que permitam coexistir de forma efetiva com outros padrões.

O protocolo WirelessHART, certificado pela IEC (*International Electrotechnical Commission*) como o primeiro protocolo de comunicação sem fio para controle de processo industrial (IEC, 2010), é um protocolo *wireless* baseado em topologias do tipo *mesh*, onde todos os dispositivos são capazes de rotear mensagens (CHEN; NIXON; MOK, 2010). Como outros padrões *wireless*, este protocolo sofre dos desafios de robustez sob interferência. Não seria incomum um cenário industrial apresentar vários protocolos *wireless* competindo pela mesma faixa do espectro de frequência, como o WirelessHART com o WiFi, o ZigBee ou o Bluetooth. Nesse cenário, a possibilidade de antecipação das perdas de qualidade de comunicação (como nível de sinal e taxa de pacotes transmitidos) permitiria otimizar a quantidade de dispositivos roteadores durante o projeto da instalação física, enquanto que futuramente possibilita a elaboração da estratégia de roteamento em malha fechada.

Com isso, o objetivo deste trabalho é elaborar uma ferramenta que permita a análise de performance ponto-a-ponto de comunicação de redes sem fio – particularmente, do WirelessHART – de forma gráfica ao longo do tempo e que seja capaz de elaborar bancos de dados para futuras aplicações. Utilizando essa ferramenta, é possível instrumentar situações de ruído e coexistência em uma rede WirelessHART prototipada para avaliação de robustez

enquanto se determina o impacto de cada tipo de interferência em análise cruzada com a inserção dos efeitos adversos. A ferramenta permitirá a coleta de dados referentes à qualidade de comunicação para posteriores trabalhos acadêmicos e se mostra relevante para pesquisa e desenvolvimento de protocolos quando no intuito de parametrizar as limitações de projeto físico e de roteamento. As transmissões entre dispositivos WirelessHART serão coletados através de um dispositivo passivo (que não interfere nos eventos de comunicação), o *sniffer*, e o processamento será efetuado em um ambiente Java baseado em um *software* acadêmico de avaliação de estratégias de roteamento.

CAPÍTULO 2 - REVISÃO BIBLIOGRÁFICA

Neste capítulo, serão apresentados os conceitos aplicados no decorrer do trabalho para parametrizar e mensurar robustez e confiabilidade do protocolo WirelessHART ante interferências controladas. Primeiramente, introduz-se o protocolo, com suas principais características (seção 2.1.1), dispositivos (seção 2.1.3) e detalhamento das camadas física, de enlace e de rede (seção 2.1.2). Posteriormente, define-se os conceitos de interferência (seção 2.1.4) e as definições de confiabilidade, robustez e coexistência (seção 2.1.5). Por fim, revisa-se o que existe atualmente referente ao estado da arte da análise de robustez de redes sem fio (seção 2.2).

2.1. FUNDAMENTOS TEÓRICOS

2.1.1. PROTOCOLO WIRELESSHART

O WirelessHART é o primeiro padrão de comunicação sem fio a ser certificado pela *International Electrotechnical Commission* (IEC) para monitoramento e controle de processos (IEC, 2010). É implementado como uma extensão do homônimo cabeado HART, de forma a permitir compatibilidade, visando disponibilizar um padrão já bem estabelecido no mercado em um novo formato (MULLER, I., NETTO, J.C., PEREIRA, C.E, 2011).

O protocolo opera sobre a banda de rádio 2,4 GHz ISM (*Industrial, Scientific and Medical*), reservada para uso em fins científicos, médicos, domésticos e similares, como definido pelo órgão ITU-R (*International Telecommunication Union – Radiocommunication*). Além do WirelessHART, diversos protocolos utilizam essa banda, como o Bluetooth, o ZigBee e o WiFi (WINTER, 2013), todos amplamente abrangidos no mercado, o que incita a relevância do estudo de confiabilidade e robustez da comunicação sujeita a coexistência.

2.1.2. MODELO OSI

O WirelessHART, visando compatibilidade com sua versão cabeada, apresenta o mesmo modelo OSI (*Open Systems Interconnection*) do HART, com exceção às camadas física, de enlace e de rede. Ilustra-se, na Figura 1, a definição de cada camada OSI com sua respectiva aplicação nos protocolos em questão. Tanto no HART quanto no WirelessHART, as camadas de rede, transporte e sessão são tratadas como uma única camada – responsável pelas funções de roteamento de rede e entrega de dados; enquanto o mesmo pode ser dito das camadas de apresentação e aplicação – uma única camada responsável pelo gerenciamento dos comandos utilizados (HCF, 2007).

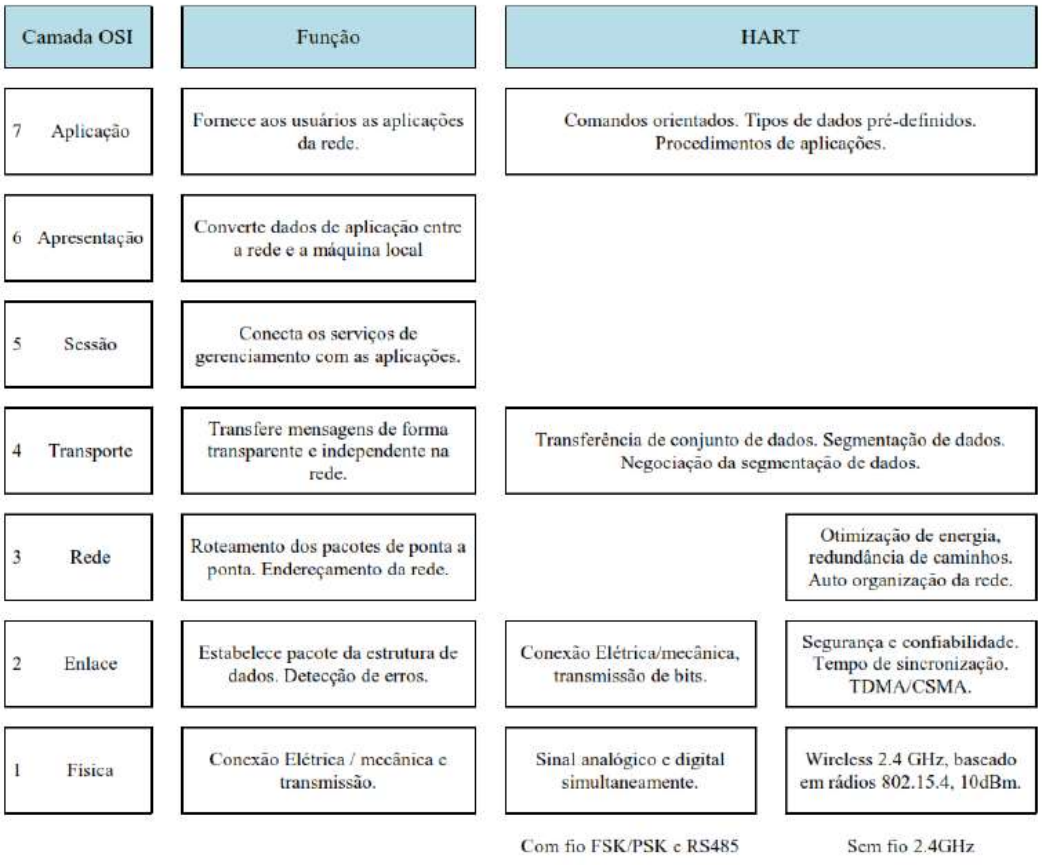


Figura 1: Modelo OSI e padrão WirelessHART (CHIEN, 2010).

A camada física do protocolo é baseada no padrão IEEE (Instituto de Engenheiros Eletricistas e Eletrônicos) 802.15.4, utilizando a banda 2,4 GHz ISM. Sua potência de transmissão pode ser programada de -10 dBm a 10 dBm. Com taxa de dados de até 250 kbits/s, apresenta 16 canais de frequência aptos para transmissão de comunicação, enumerados de 11 a 26 (intervalos de 5 MHz entre canais adjacentes). A Figura 2 ilustra as

faixas de frequência e os respectivos canais empregados. O canal 26 é reservado, como definido pelo padrão (CHIEN, 2010).

Índice	Canal 802.15.4	Frequência (MHz)
0	11	2405
1	12	2410
2	13	2415
3	14	2420
4	15	2425
5	16	2430
6	17	2435
7	18	2440
8	19	2445
9	20	2450
10	21	2455
11	22	2460
12	23	2465
13	24	2470
14	25	2475
15	26	Não usado

Figura 2: Canais de comunicação do WirelessHART (HCF, 2007).

À camada de enlace, cabe a detecção e correção de erros inerentes ao nível físico. Através da técnica de *Time Division Multiple Access* (TDMA), garante-se o determinismo e se evita colisões. A técnica consiste na limitação de acesso ao meio físico a dois dispositivos por vez (um envia o sinal, o outro confirma recebimento através de um comando denominado ACK) a cada espaço de tempo de 10 milissegundos, definido como *timeslot*. Cada unidade de tempo do *timeslot* é contabilizado em um parâmetro denominado ASN (*Absolute Slot Number*) e um conjunto de *timeslots* é definido como *superframe*.

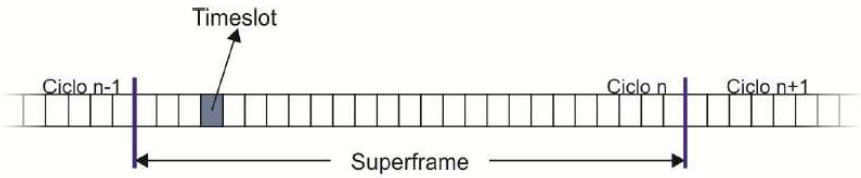


Figura 3: Representação de *timeslot* e *superframe* (KUNZEL, 2012).

2.1.3. DISPOSITIVOS DE UMA REDE WIRELESSHART

O WirelessHART apresenta cinco tipos principais de dispositivos: dispositivos de campo, adaptadores, *gateway,* gerenciadores de rede (ou *Network Managers*) e pontos de acesso (*access points*) (MULLER, I., NETTO, J.C., PEREIRA, C.E, 2011). A Figura 4 mostra um esquema de dispositivos em uma rede WirelessHART genérica.

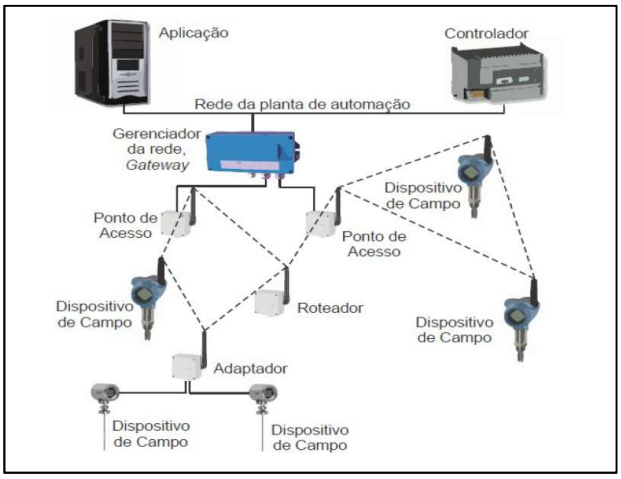


Figura 4: Dispositivos de uma rede WirelessHART (KUNZEL, 2012).

Os dispositivos de campo são os atuadores e sensores que efetivamente se relacionam com o meio que se deseja controlar ou medir. De forma a expandir o potencial de conectividade da rede, cada dispositivo sem fio é capaz de agir também como um roteador. Em regiões de baixa intensidade de sinal ou com variáveis de processo críticas, pode-se recorrer a *access points*, dispositivos que provêm pontos de acesso adicionais à rede de forma a aumentar a confiabilidade e promover maior vazão de fluxo de dados.

Adaptadores são responsáveis pela compatibilidade de dispositivos HART cabeados com a rede sem fio. Estruturalmente, são dispositivos de campo sem fio que, ao invés atuarem diretamente no meio, o fazem por meio dos dispositivos cabeados HART a que estão conectados.

A tarefa de gerir as aplicações da planta e prover o acesso aos dados dos dispositivos cabe ao *gateway*. Este dispositivo serve de fonte do relógio de sincronização, item crucial para o determinismo devido ao funcionamento segundo o TDMA, e possui conexão física com o gerenciador de rede. Este, por sua vez, realiza as ações de criar, controlar, gerenciar e otimizar a rede, computando informações como dispositivos ativos, *links* estabelecidos, *superframes* configurados, entre outros.

2.1.4. INTERFERÊNCIA E RUÍDO

Em redes industriais, interferências e ruídos podem constituir um sério agravante para a confiabilidade do sistema. Diferentemente de redes cabeadas, onde o meio físico de propagação do sinal apresenta barreiras e isoladores para proteção da informação, redes sem

fio estão expostas a distúrbios inerentes da instabilidade de seu meio físico, o ar (no caso de redes por rádio frequência, como o WirelessHART).

Pode-se definir interferência como “qualquer sinal indesejado de uma fonte externa, o qual pode perturbar ou mascarar o sinal desejado” (WINTER, 2013). Dessa forma, diferentemente de ruído, que pode ser oriundo tanto de fontes externas quanto internas e em geral apresenta características aleatórias, interferências estão relacionadas a interposição de sinais, disputando acesso ao mesmo meio físico e alterando um ao outro.

Em geral, interferências podem ser classificadas em dois tipos: interferência por co-canal, onde a fonte interferente irradia no mesmo transceptor ou em uma frequência sobreposta; ou por canal adjacente, onde sinais de energia de uma fonte atuando em uma frequência vizinha à da rede acaba por interferir na transmissão dos dados.

2.1.5. ROBUSTEZ, CONFIABILIDADE E COEXISTÊNCIA

Segundo a definição de Sikora e Groza (2005), redes são capazes de coexistir caso não sejam significantemente impactadas pela existência de outras fontes de sinal nas mesmas faixas de frequência. Pela definição de interferência da seção 2.1.4, coexistência pode ser classificada como uma interferência por co-canal.

Em IEEE (1990), define-se os conceitos de robustez (*robustness*) e confiabilidade (*reliability*). Redes podem ser avaliadas segundo sua robustez quando se leva em consideração sua capacidade de lidar com erros ou demais condições não-ideais durante seu funcionamento e, ainda assim, garantir transmissão de dados. Dessa forma, trata-se de uma medida de tolerância a erros. Confiabilidade, por outro lado, é a habilidade de um sistema realizar suas tarefas sem perder parâmetros pré-estabelecidos durante um período determinado de tempo. Portanto, é uma medida de qualidade de performance em regime nominal.

Para este trabalho, ambos os conceitos de robustez e confiabilidade são empregadas para avaliar a capacidade de coexistência de redes WirelessHART. Todo sistema robusto é um sistema com confiabilidade, mas nem todo sistema com confiabilidade é robusto. Enquanto confiabilidade é um parâmetro próprio definido no protocolo como a taxa de entrega efetiva de informações ao seu destinatário final (independente da rota ou da quantidade de tentativas necessárias), o conceito de robustez é empregado como a capacidade da rede de manter sua confiabilidade em situações adversas, como, no caso em questão, de coexistência forçada.

2.2. ESTADO DA ARTE

Os estudos de Golmie (2006) e de Winter (2013) citam três principais classificações de estudos de coexistência: modelagem matemática, simulações e experimentação.

Estudos de coexistência baseados em modelagem analisam, através de modelos matemáticos, a probabilidade de colisão de pacotes com base em uma rede hipotética. O trabalho de Han e Seungjoon (2007), por exemplo, modela um cenário para coexistência dos padrões IEEE 802.15.4 e IEEE 802.11b utilizando probabilidade de erro de pacote, concluindo que a confiabilidade do sistema é inversamente proporcional ao deslocamento de frequência ocupada entre os dois padrões e que um algoritmo de seleção de canais poderia reduzir significantemente o impacto das interferências (o WirelessHART não apresenta um sistema do gênero, com exceção da mecânica de *channel hopping*, onde canais com demasiada interferência são listados como desfavoráveis e se preferencia a transmissão de pacotes por outros canais – vide Figura 2).

Estudos de simulação, segundo Winter (2013), são os mais empregados atualmente e os que mais facilmente permitem análise sob cenários diferenciados. O trabalho de simulação de Dominics *et al* (2009) modelou as camadas físicas e de enlace para avaliar as principais diferenças entre uma rede WirelessHART e outras redes IEEE 802.15.4 e IEEE 802.11b quando sujeitas a interferências. Definindo uma colisão como cada coincidência temporal de utilização do mesmo canal de frequências, o estudo mostrou que o WirelessHART apresenta desempenho melhor em coexistência que os demais protocolos empregados. O estudo, contudo, cita a necessidade de se incluir modelagens dos efeitos de interferência por canais adjacentes.

Estudos de coexistência sob experimentação tendem a ser os mais confiáveis e precisos, contudo, limitados pela situação implementada. O estudo de Subbu e Howitt (2007) avalia a coexistência entre dispositivos IEEE 802.14.5 estimando a taxa de perda de pacotes sob diferentes situações, variando parâmetros como sinal de interferência e frequência de deslocamento. O estudo concluiu, dentre os demais resultados, que a partir de 15 MHz de frequência, a taxa de variação do sinal de interferência é atenuada e que o tamanho do pacote é proporcional à probabilidade de corrupção de dados, considerando-se uma potência de interferência constante.

CAPÍTULO 3 - METODOLOGIA

A confiabilidade da rede, conforme descrito na seção 2.1.5, reflete a capacidade de entrega de informação de um dispositivo transmissor ao seu destinatário final. Muitas vezes, devido a interferências e ruídos, pacotes de dados se corrompem, incapacitando sua interpretação por parte do dispositivo receptor, sendo este o destinatário final ou não. Contudo, a perda de um pacote não acarreta a perda definitiva da informação, pois caso o nivel de criticidade da informação for devidamente alto, o emissor tentará novamente o envio em uma próxima janela de oportunidade. A confiabilidade, dessa forma, é um parâmetro de rede e está intrinsicamente relacionada ao gerenciador de rede (seção 2.1.3). Dessa forma, para este estudo, a métrica de confiabilidade foi obtida conforme o reportado pela interface homem-máquina do gerenciador de rede.

Robustez, por outro lado, sendo definida como a capacidade de uma rede manter sua confiabilidade perante situações adversas, precisa levar em consideração parâmetros de campo. Este capítulo descreve o princípio de funcionamento da ferramenta de análise de robustez desenvolvida, detalhando as métricas de campo avaliadas (seção 3.1), o *hardware* necessário para a aplicação da ferramenta (seção 3.2) e a lógica para aquisição dos parâmetros propostos (seção 3.3). Posteriormente, descreve-se a metodologia empregada nos estudos de caso realizados para validação da ferramenta (seção 3.4).

3.1. MÉTRICAS

3.1.1. PER

O PER, ou *Packet Error Rate*, é a principal métrica de robustez empregada neste trabalho. Definido como a taxa percentual de pacotes com erro, o PER pode ser estimado empiricamente como a razão entre o total de transmissões consideradas com falha (*Failed*

Packets) sobre o total de transmissões de dados (*Packets Transmited*), como ilustra a Equação (1).

$$PER = \frac{Failed\ Packets}{Packets\ Transmited} * 100\% \quad \textbf{(1)}$$

Como forma de garantir entrega de dados, o protocolo WirelessHART emprega mensagens de ACK (*acknowledge*) após certas transmissões: toda vez que um dispositivo destinatário recebe uma mensagem e esta passa no teste de validação do conteúdo (no caso do WirelessHART, chamado *Cyclic Redundancy Check,* ou CRC), uma mensagem de confirmação de entrega (ACK) é encaminhada ao dispositivo emissor na mesma janela de tempo (*timeslot*). Somente após receber o ACK, o emissor pode ter certeza que seu dado foi corretamente recebido e interpretado, assim, não precisando organizar o reenvio dos dados na próxima janela de oportunidade (que varia com o grau de criticidade da informação). Dessa forma, mesmo que o dado tenha sido entregue ao receptor, o fato de o ACK não ter sido recebido pelo emissor força o reenvio da mensagem e impacta no desempenho da rede.

A variável de comunicações com falha, *Failed Packets*, é definida como a soma das transmissões cujo emissor não recebeu o reporte de ACK do devido receptor. Como o envio do ACK depende tanto da entrega quanto da validação dos dados no CRC, o PER se torna um parâmetro de avaliação do grau de transmissão de informações. Considerando uma grande quantidade de dados para o cálculo da taxa, o PER pode ser tratado estatisticamente como a probabilidade de um pacote de informações ser perdido.

Para este trabalho, emprega-se o PER em análise ponto-a-ponto, ou seja, avalia-se a taxa de perda de pacotes a cada par de dispositivos vizinhos. Dessa forma, o PER se torna a principal métrica de robustez da rede, possibilitando avaliação de perda de performance dos pares de dispositivos ante interferência. Ressalta-se, contudo, que aumento do PER e conseguinte pior performance entre pares de dispositivos não indica necessariamente perda de confiabilidade da rede. Por mais que pacotes sejam perdidos por quaisquer fatores, a informação neles contida pode ser reenviada em posteriores *timeslots* e, assim, assegura-se que não houve impacto em confiabilidade.

3.1.2. RSSI

O *Received Signal Strenght Indicator*, ou RSSI, é um parâmetro medido em decibel-miliwatt (dBm) que indica o nível de sinal recebido pelo dispositivo receptor no canal de comunicação avaliado. É definido como o nível de potência em decibéis em relação ao nível de referência de um miliwatt (1 mW equivalente a 0 dBm). Com isso, quanto maior o valor absoluto de RSSI, maior a intensidade do sinal esperado.

Diferentemente do PER, que mede diretamente as falhas de comunicação da rede, o RSSI mede somente intensidade de sinal. Não necessariamente um *link* entre dispositivos com RSSI alto apresentará maior taxa de entregas que um *link* com RSSI menor, apesar de ser consideravelmente mais provável. Contudo, em normativas (específicas a cada aplicação), os limiares de confiabilidade estão intrinsicamente atrelados ao nível de RSSI entre os dispositivos. Por exemplo, pode-se esperar que, em determinada aplicação, para RSSI maiores de -70 dBm, a confiabilidade não seja menor que o limiar de 95%, e que cada faixa de RSSI subsequente apresente limiares diferenciados.

O RSSI pode ser impactado por interferências e ruídos na rede, tanto de corpos físicos quanto eletromagnéticos ou térmicos, mas é principalmente função da distância entre dispositivos. Uma vez estabelecidos os valores médios de RSSI entre dispositivos estáticos em um ambiente controlado, pode-se correlacionar os desvios mais significativos a interferências pontuais.

3.2. HARDWARE

O método empregado para captura dos sinais de comunicação da rede WirelessHART para posterior análise é o método passivo, no qual se utiliza instrumentos que não interferem diretamente nos dispositivos ou nos sinais da rede. O instrumento em questão para este estudo é o *sniffer* Wi-Analys (Figura 5), um dispositivo receptor especializado que captura as transmissões WirelessHART dentro de seu raio de alcance e salva *logs* (“registros”) de cada mensagem com uma estampa temporal, que pode ser posteriormente relacionada ao ASN (*Absolute Slot Number*).

Figura 5: Wi-Analys Network Analyzer, o *sniffer* do WirelessHART.

A vantagem da instrumentação passiva é que não se interfere com o sistema, de modo que não se prejudica o nível de sinal entre vizinhos ou a taxa de pacotes perdidos de qualquer dispositivo. Dessa forma, o *sniffer* se mostra um instrumento adequado para a aplicação de mensurar a robustez da rede. O *sniffer*, contudo, apresenta limitação de alcance, não sendo capaz de capturar todas as mensagens da rede caso a disposição dos dispositivos esteja além de seu raio de atuação. Contudo, como para esta aplicação se está interessado somente nos dados de processo enviados ao *Network Manager* (seção 3.3), a alocação do *sniffer* próximo ao *access point* do *gateway* atende à captura de todas as transmissões de interesse.

Um exemplo de *log* de captura do Wi-Analys é mostrado na Figura 6. Inicia-se com as identificações de *network ID* (“identificação de rede”) e *join key* (“chave de acesso”), códigos característicos da rede instrumentada. Em seguida, cada linha corresponde a uma transmissão de dados capturada pelo *sniffer*. Inicialmente, tem-se informações referentes à natureza da transmissão, como o padrão IEEE empregado, a data, a hora e a estampa de tempo. Em seguida, segue a informação da transmissão, criptografada e em formato de *bytes*, hexadecimal.

```
;netid  0001
;joinkey  12345678000000000000000000000000
119021, 802.15.4-DATA, 1, 2018-04-30 09:09:39.977, 1357515.507, -26, 0x0000, 23, 10 41 88 68 01 00 05 00 03 00 1A 7B 4B 2B
119021, 802.15.4-DATA, 2, 2018-04-30 09:09:39.977, 1357515.508, -80, 0x0001, 25, 10 41 88 68 01 00 05 00 03 00 1A 7B 4B 2B
119021, 802.15.4-DATA, 3, 2018-04-30 09:09:39.977, 1357517.233, -46, 0x0000, 23, 13 41 88 68 01 00 03 00 05 00 18 00 00 07
119021, 802.15.4-DATA, 4, 2018-04-30 09:09:40.727, 1358265.487, -46, 0x0000, 16, 3A 41 88 B3 01 00 01 00 05 00 2F 00 1E 58
119021, 802.15.4-DATA, 5, 2018-04-30 09:09:42.258, 1359805.440, -60, 0x0000, 13, 3A 41 88 4D 01 00 04 00 02 00 2F 00 20 6B
119021, 802.15.4-DATA, 6, 2018-04-30 09:09:42.258, 1359808.511, -55, 0x0000, 13, 13 41 88 4D 01 00 02 00 04 00 28 00 00 57
119021, 802.15.4-DATA, 7, 2018-04-30 09:09:42.523, 1360075.502, -56, 0x0000, 14, 3A 41 88 68 01 00 05 00 04 00 2F 00 1F 6B
119021, 802.15.4-DATA, 8, 2018-04-30 09:09:42.539, 1360078.570, -43, 0x0000, 14, 13 41 88 68 01 00 04 00 05 00 28 00 00 0B
119021, 802.15.4-DATA, 9, 2018-04-30 09:09:43.273, 1360825.484, -36, 0x0000, 11, 3A 41 88 B3 01 00 01 00 05 00 2F 00 1E 6B
```

Figura 6: Exemplo de *log* do Wi-Analys.

3.3. SOFTWARE

Para se obter as métricas de robustez estabelecidas na seção 3.1, é necessário determinar quais transmissões emitidas pelos dispositivos disponibilizam tais dados. A estrutura de pacote do WirelessHART (PDU, ou *Protocol Data Unit*) pode ser visualizada na Figura 7.

Segundo a estrutura do PDU, o comando da transmissão é interpretado na camada de aplicação (*application layer*), onde se obtém qual tipo de mensagem a transmissão está enviando. Dessa forma, a ferramenta deve:

- capturar a mensagem na camada física;
- validar a identidade de rede (*network ID*) e os destinatários na camada de enlace de dados;
- decriptar os dados na camada de segurança;
- interpretar os comandos de cada transmissão na camada de aplicação;
- filtrar os comandos que transmitem os dados usados para o cálculo do PER e do RSSI.

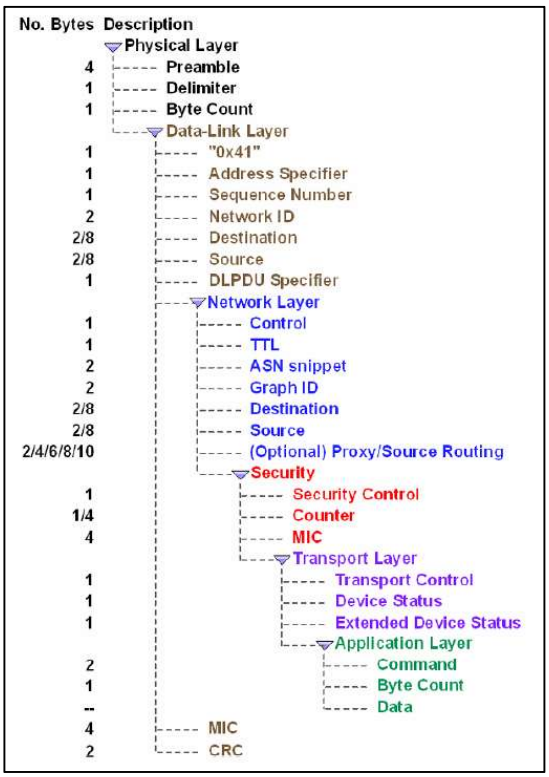


Figura 7: Estrutura do PDU WirelessHART (HCF, 2007).

Para a mensuração do RSSI e do PER, foram utilizados dois comandos específicos do WirelessHART: o comando 780 – *Report Neighbor Health List* (“Relatório de Lista de

Qualidade de Sinal entre Vizinhos") e o comando 787 – *Report Neighbor Signal Levels* ("Relatório de Níveis de Sinais entre Vizinhos"). Ambos os comandos, classificados como ordem de prioridade "dado de processo", são requisitados periodicamente pelo *Network Manager* (gerenciador de rede) para alimentar algoritmos internos de otimização de rotas – os dispositivos que apresentam maior nivel de sinal e menores taxas de erros são os candidatos mais favoráveis para transmissão de informações. Ambos os comandos são do tipo *downlink*, ou seja, são originados do *Network Manager* como uma requisição (*request*) e devem ser respondidos pelo dispositivo de campo (*response*).

O comando 780 - *Report Neighbor Health List* requisita do dispositivo uma série de informações referentes às conexões com vizinhos *conectados* com ele, enquanto o 787 - *Report Neighbor Signal Levels* requer somente a informação dos vizinhos atualmente *descobertos*. A distinção é importante, visto que o 780 é um reporte de status de conexões atuais e o 787 é um reporte de histórico de conexão, levando em conta até os pares já desconectados ou nunca conectados. Dessa forma, cada comando apresenta aplicações diferenciadas.

Dentre as informações relevantes encaminhadas pelos comandos, estão:

- o RSSI médio (em dBm) conforme reportado entre cada par de dispositivos;
- número de pacotes enviados para cada vizinho pareado (*Packets Transmitted*);
- números de pacotes falhados (sem ACK recebido quando esperado) com o vizinho pareado (*Failed Packets*);
- número de pacotes recebidos com sucesso do vizinho pareado.

Através dessas informações, é possível calcular as métricas conforme definidas na seção 3.1. O ambiente em Java elaborado é baseado no projeto de Kunzel (2012). Nele, uma classe denominada *Monitor* cria instâncias das classes *JFrameCapturaTopologia*, responsável pela interface gráfica e interação com o usuário, e *Network*, que gere os objetos da rede em si, como os objetos *Devices* (dispositivos), *Neighbors* (vizinhos), *superframes*, entre outros, além de ser responsável por variáveis da própria rede como ASN e o *NetworkID*.

Para o objetivo deste trabalho, criou-se novas classes, denominadas *command780* e *command787*. Cada classe representa uma abstraçãodos comandos *Report Neighbor Health List* e *Report Neighbor Signal Levels*, respectivamente. Interpreta-se que cada comando, por

ser uma transmissão encaminhada de um único dispositivo ao gerenciador de rede, pode ser modelado por um objeto que possui uma instância de um objeto *Device* (o dispositivo emissor) e este, por sua vez, possui um *array* de objetos *Neighbor*. Cada objeto *Neighbor* é uma abstração das variáveis pelas quais cada dispositivo interage com seus vizinhos, sendo responsável por calcular e guardar os dados de pacotes enviados, recebidos e perdidos com o *Device* correspondente.

Dessa forma, toda vez que o objeto *Network* tem sua operação *interpretCommandDevice* (“interpretar comando de dispositivo”) chamada (o que ocorre toda vez que uma nova linha do *log* do *sniffer* deve ser lida), o ambiente filtra o tipo de comando na camada de aplicação do dado transmitido. Sendo um comando 780 ou 787, uma nova instância da classe *command780* ou *command787* é criada, tendo como parâmetros de entrada: um objeto *Device* (com seus recém-atualizados atributos *discoveredNeighborList* ou *linkedNeighborList*) e o *array* de *Neighbor* representando os vizinhos do dispositivo em questão. O diagrama de classe resumido do ambiente é mostrado na Figura 8.

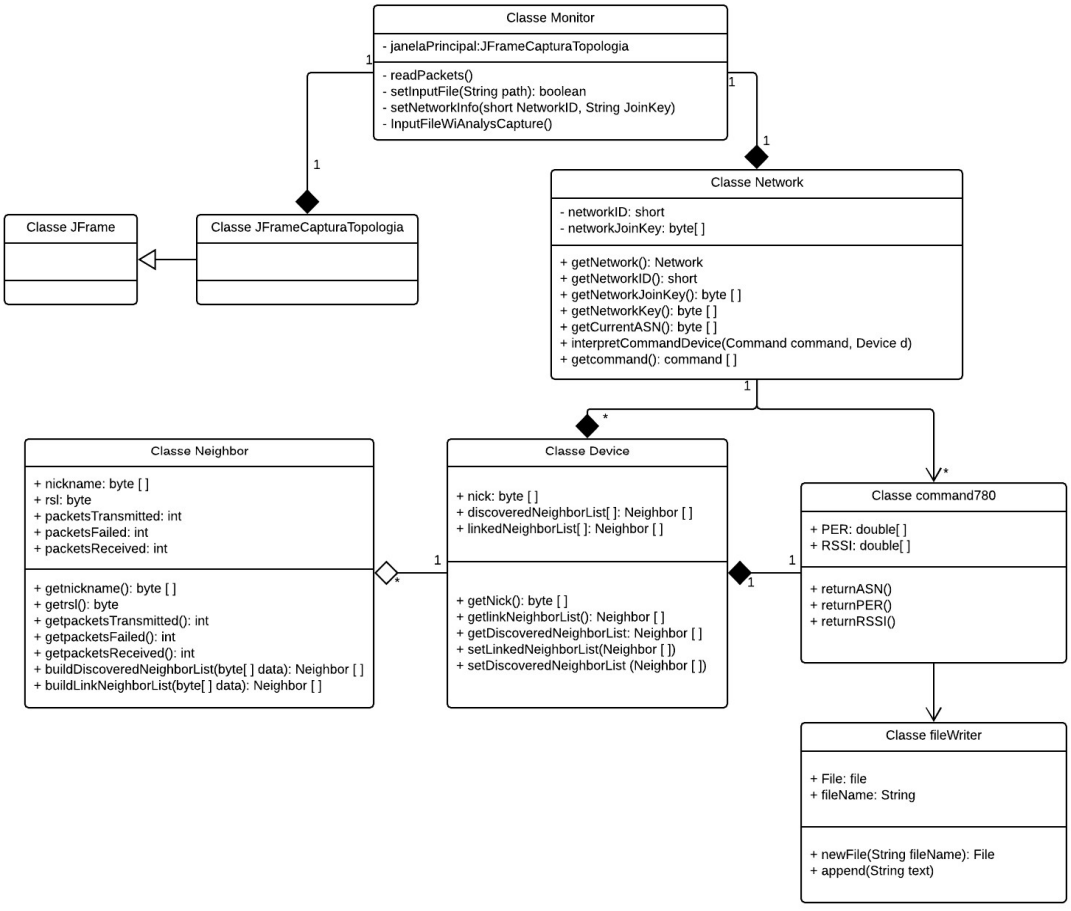


Figura 8: Diagrama de classes da ferramenta em *software* desenvolvida.

3.4. ESTUDOS DE CASO

Esta seção descreve como se validou a ferramenta implementada através de estudos de caso direcionados, realizados nos ambientes do LASCAR, o Laboratório de Automação, Controle e Robótica da UFRGS (Universidade Federal do Rio Grande do Sul). Após a descrição dos dispositivos utilizados (seção 3.4.1), descreve-se os dois regimes de experimento empregados em cada estudo (seção 3.4.2): um regime normal, onde os dispositivos operam normalmente, sujeitos apenas a interferências externas; e um regime interferido, onde propositalmente se inserem interferências para avaliação comparativa da robustez da rede.

3.4.1. DISPOSITIVOS EMPREGADOS

Para a elaboração do estudo de caso, são necessários os dispositivos citados na seção 2.1.3, assim como o *sniffer* descrito na seção 3.2.

Como *Network Manager*, *gateway* e *access point*, foi empregado o dispositivo comercial Emerson Wireless 1420A Gateway (EMERSON ELECTRIC CO., 2018), com capacidade de conexão para com até 100 dispositivos, configuração automática de rede WirelessHART com rotas otimizadas e garantia de confiabilidade de 99% (Figura 9). O dispositivo também apresenta uma interface homem-máquina de onde se obteve a avaliação de confiabilidade (*reliability*) da rede ao longo do tempo, mostrada na Figura 9.

Figura 9: Emerson Wireless 1420A Gateway (EMERSON ELECTRIC CO., 2018).

HART Tag	Node state	Active neighbors	Neighbors	Service denied	Reliability	Missed updates	Path stability
TAG 1005	●	wihartgw TAG 1011 TAG 1015	3	●	93.9 %	10	99.1 %
TAG 1008	●	wihartgw	1	●		0	
TAG 1011	●	wihartgw TAG 1005 TAG 1022	3	●	93.9 %	10	95.8 %
TAG 1015	●	wihartgw TAG 1005	2	●	93.3 %	11	95.3 %
TAG 1022	●	wihartgw TAG 1011 TAG 1025	3	●	90.4 %	16	97.2 %
TAG 1025	●	wihartgw TAG 1022	2	●	100.0 %	0	

Figura 10: Interface homem-máquina do Emerson Wireless 1420A Gateway.

Ambos os testes implementados utilizaram como dispositivos de campo os dispositivos compatíveis com WirelessHART elaborados no LASCAR (Figura 11), como descritos em Muller *et al* (2010). Os dispositivos são compostos por um microcontrolador Freescale MC13224, um transceptor de rádio IEEE 802.15.4 integrado e diversos periféricos responsáveis por demais características necessárias a um dispositivo WirelessHART como, por exemplo, MAC, *clock* e criptografia.

Figura 11: Dispositivos de campo compatíveis com WirelessHART, desenvolvidos no LASCAR.

Uma vez que os parâmetros de qualidade de comunicação apresentam correlação direta com os parâmetros físicos do ambiente, como distâncias e barreiras entre dispositivos, apresenta-se, para cada estudo de caso, a planta baixa do LASCAR com a disposição dos equipamentos envolvidos no estudo de caso em questão. Como cada análise referencia um par de dispositivos, as *tags* (estampas) de cada par são relatadas conforme indicado na respectiva planta baixa.

3.4.2. REGIME NORMAL E REGIME INTERFERIDO

Para o regime normal de experimento, os dispositivos foram configurados para operar com funcionamento básico, sem aplicação para as transmissões de dados, apenas mantendo a

rede em funcionamento. Como parte de configuração da norma, cada dispositivo encaminha periodicamente ao *Network Manager* um reporte da qualidade de comunicação com seus vizinhos para que esse possa executar os algoritmos de otimização de rota e, assim, buscar o aumento da confiabilidade da rede. De acordo com a seção 3.3, o comando de interesse para avaliação da qualidade de comunicação ao longo do tempo é o comando 780, que pode ser empregado para a determinação da intensidade de sinal e da taxa de pacotes perdidos entre os dispositivos efetivamente conectados.

Durante os regimes normais de cada estudo, a rede foi sujeita apenas às interferências externas não-controladas, como as barreiras físicas oriundas de paredes, objetos e distâncias entre cada dispositivo. Durante o regime normal, é possível avaliar o quanto a qualidade de conexão é afetada em regime estático pela disposição dos equipamentos.

Durante o regime interferido, é acionado o *software* iPerf. O iPerf é uma ferramenta de medições ativas da máxima largura de banda em redes IP (DUGAN *et al*, 2018). Através dele, é possível configurar uma rede para injetar o máximo de pacotes TCP ou UDP durante determinado período de tempo e, assim, avaliar o desempenho e disponibilidade de banda da dessa rede.

Para os estudos de caso propostos, o iPerf foi empregado durante períodos pré-determinados de 5.000 segundos como um injetor de interferências por co-canal (seção 2.1.4) em uma rede formada por dois computadores conectados por um roteador WiFi dedicado. Como a comunicação de rede especificada foi o Wi-Fi, de norma IEEE 802.11, cujas faixas de frequência coincidem com as do WirelessHART na IEEE 802.14.5 (WINTER, 2013), o efeito da ativação do iPerf é um maior tráfego de dados dentro das faixas de frequência de ambos os protocolos e, assim, força-se um cenário de coexistência entre os dois protocolos.

Conforme a seção 2.1.2, o protocolo WirelessHART emprega suas estampas temporais (ASN, ou *Absolut Slot Number*) a cada 10 ms de acordo com o *clock* sincronizado pelo gerenciador de rede (seção 2.1.3). Cada estudo de caso seguiu uma sequência de procedimentos parecida (Figura 12): inicialização dos equipamentos, regime normal para estabilização da rede, regime interferido, regime normal final para avaliação da reestabilização. O primeiro ASN, contabilizado como zero, é configurado pelo gerenciador de rede logo após a sua inicialização.

Através do ASN coletado a cada reporte e sabendo os horários de inserção e remoção de interferências, faz-se possível correlacionar a performance ponto-a-ponto da rede com a presença ou ausência de interferência controlada. A Tabela 1 indica a correlação de cada janela de regime interferido com o respectivo ASN da rede para cada estudo de caso.

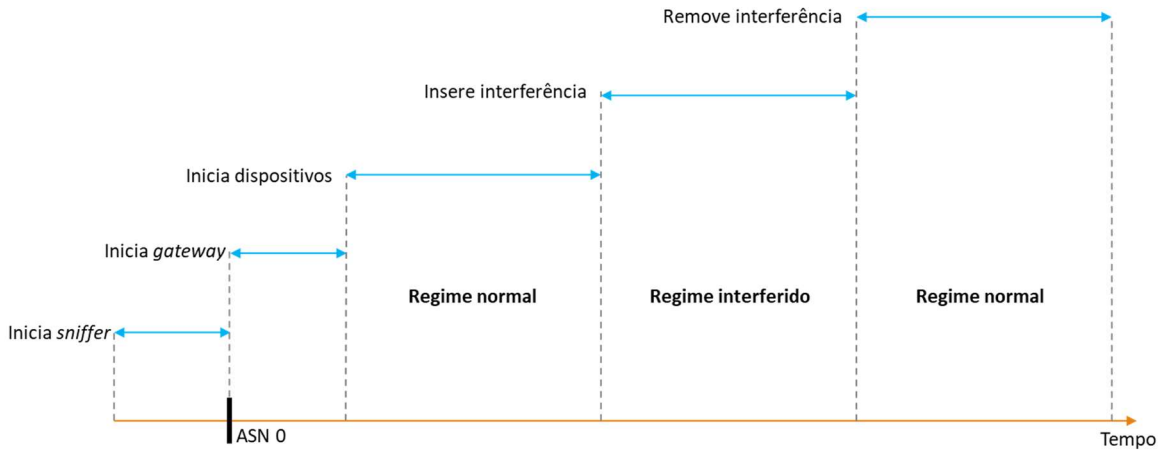


Figura 12: Diagrama de eventos para cada estudo.

Percebe-se que, com exceção do segundo estudo de caso, cada estudo apresenta apenas um regime interferido.

Tabela 1: Correlação de janelas de interferência com ASN da rede instrumentada para cada experimento.

	Experimento #1		Experimento #2		Experimento #3	
Evento	**Horário**	**ASN**	**Horário**	**ASN**	**Horário**	**ASN**
Inicia *sniffer*	10:45	-	10:35	-	10:45	-
Inicia *gateway*	10:49	0	10:45	0	10:53	0
Inicia dispositivos	10:55	34.978	10:52	43.318	11:00	40.341
Insere interferência 1	12:19	624.648	12:04	474.000	12:17	502.341
Remove interferência 1	13:42	1.124.648	13:28	978.000	13:31	946.341
Insere interferência 2	N/A	N/A	14:31	1.356.000	N/A	N/A
Remove interferência 2	N/A	N/A	15:55	1.860.000	N/A	N/A
Fim do experimento	16:27	2.112.785	19:18	3.078.000	14:38	1.401.841

CAPÍTULO 4 - RESULTADOS

Como validação da ferramenta elaborada, foram realizados três estudos de caso nos ambientes do LASCAR, o Laboratório de Automação, Controle e Robótica da UFRGS (Universidade Federal do Rio Grande do Sul), conforme descritos na seção 3.4. Cada experimento apresentou contraste em quantidade e disposição de dispositivos, assim como na quantidade de dados de interferência transmitidos pelo iPerf na rede WiFi coexistente.

Neste capítulo, são apresentados os resultados obtidos com o uso da ferramenta desenvolvida na seção 4.1, enquanto a seção 4.2 apresenta os parâmetros contrastantes entre cada experimento. Por fim, a seção 4.3 apresenta a discussão dos resultados obtidos e a comparação com bibliografias relacionadas.

4.1. IMPACTOS NAS MÉTRICAS

De acordo com a Tabela 1, esperou-se que a ferramenta desenvolvida para análise de robustez denotasse impacto de performance nas redes entre os seguintes intervalos de tempo, aproximadamente:

- $620.000 < ASN < 1.100.000$, para o primeiro experimento;
- $470.000 < ASN < 970.000$ e $1.350.000 < ASN < 1.850.000$, para o segundo experimento;
- $500.000 < ASN < 950.000$, para o terceiro experimento.

As seções 4.1.1 e 4.1.2 a seguir indicam, respectivamente, os impactos em PER e RSSI para cada um dos experimentos dentro dos intervalos esperados.

4.1.1. IMPACTOS EM *PACKET ERROR RATE*

No primeiro estudo de caso, o impacto em taxa de erro de pacotes foi notável em todos os *links* entre dispositivos, principalmente nos dispositivos mais próximos ao roteador WiFi que geria a rede de interferências do iPerf (Figura 13).

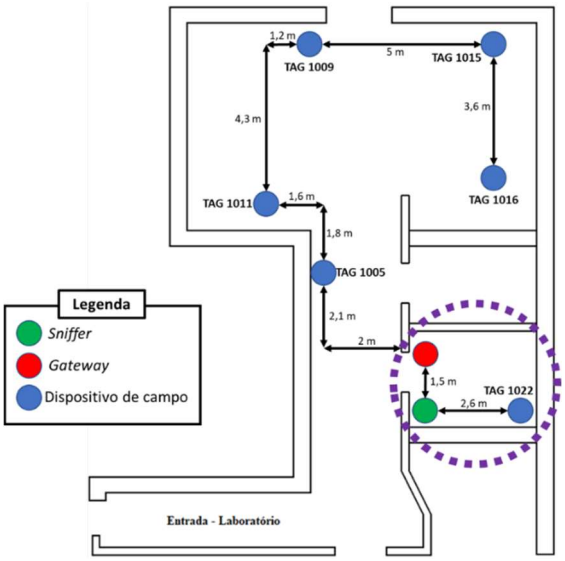


Figura 13: Planta baixa dos dispositivos do primeiro estudo de caso. Em destaque, a zona de roteamento da rede iPerf.

O impacto em PER ficou entre a faixa de 20% a 30%, como mostra a Figura 14.

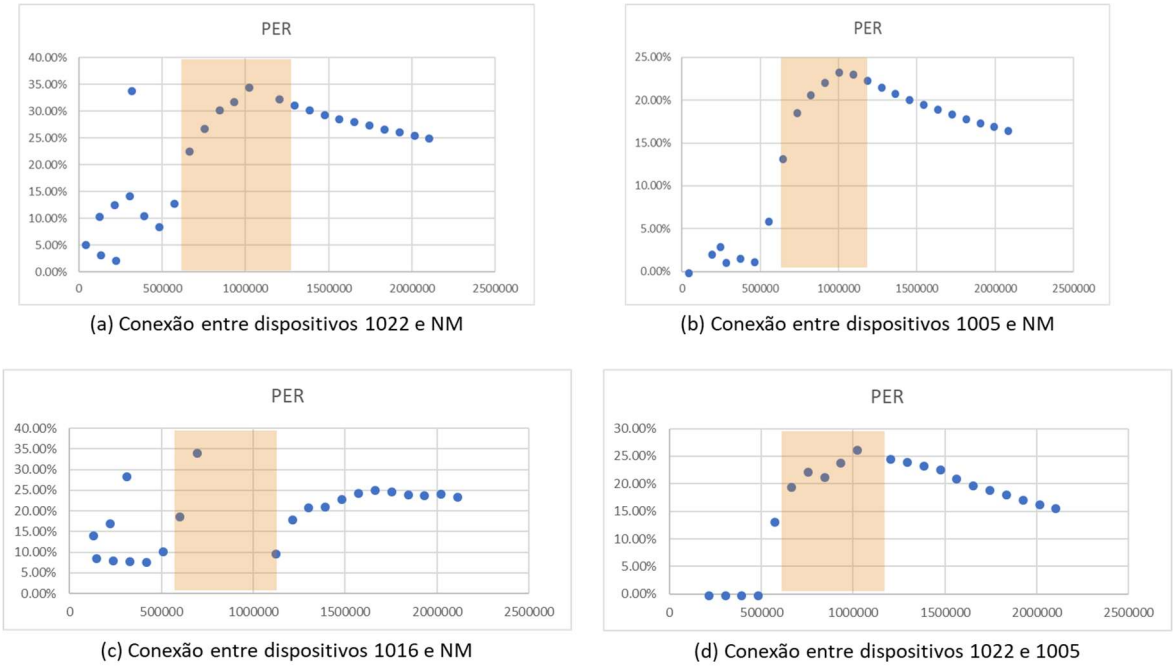


Figura 14: Gráficos de PER para pares de dispositivos sob impacto de interferência no primeiro estudo de caso.

Para o segundo estudo de caso, o impacto em PER foi notado somente em alguns *links* de dispositivos e, ainda assim, com uma média de aumento de taxa consideravelmente menor – cerca de 3 % a 6%. A Figura 15 mostra a planta baixa do segundo estudo de caso e a Figura 16 mostra alguns dos resultados em destaque.

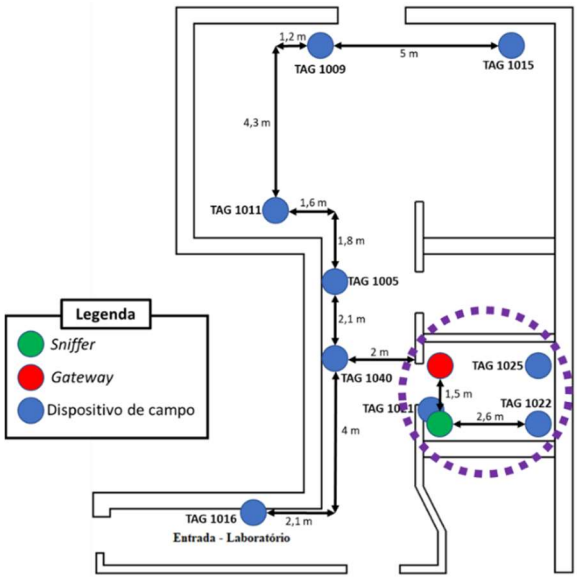


Figura 15: Planta baixa dos dispositivos do segundo estudo de caso. Em destaque, a zona de roteamento da rede iPerf.

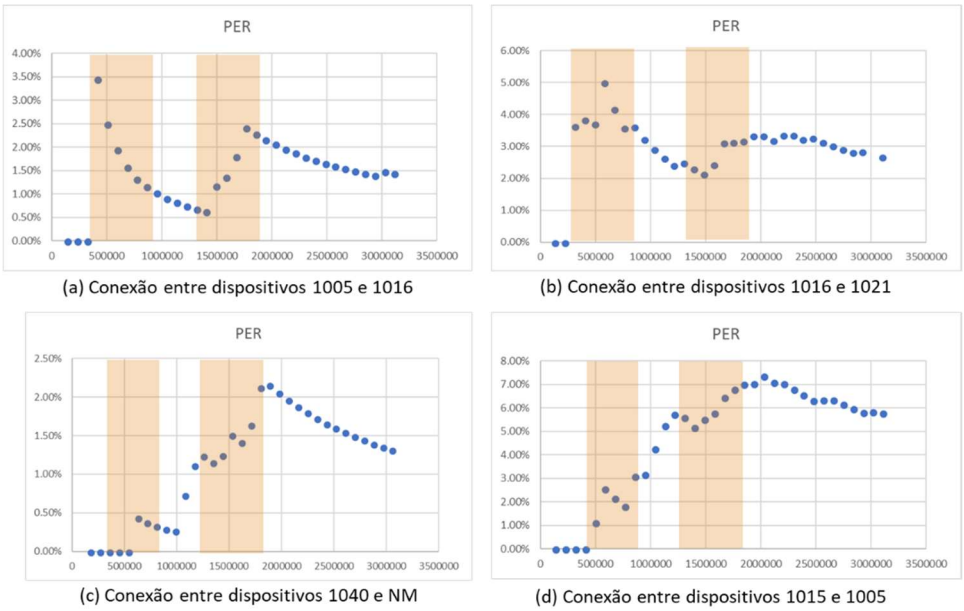


Figura 16: Gráficos de PER para pares de dispositivos sob impacto de interferência no segundo estudo de caso.

O terceiro estudo de caso, cuja planta baixa está mostrada na Figura 17, apresentou impactos em PER na faixa de 9% a 15%, como mostrado na Figura 18.

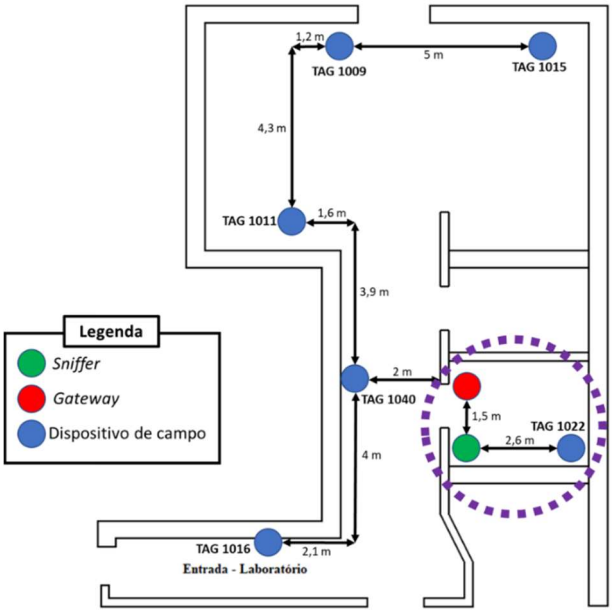


Figura 17: Planta baixa dos dispositivos do terceiro estudo de caso. Em destaque, a zona de roteamento da rede iPerf.

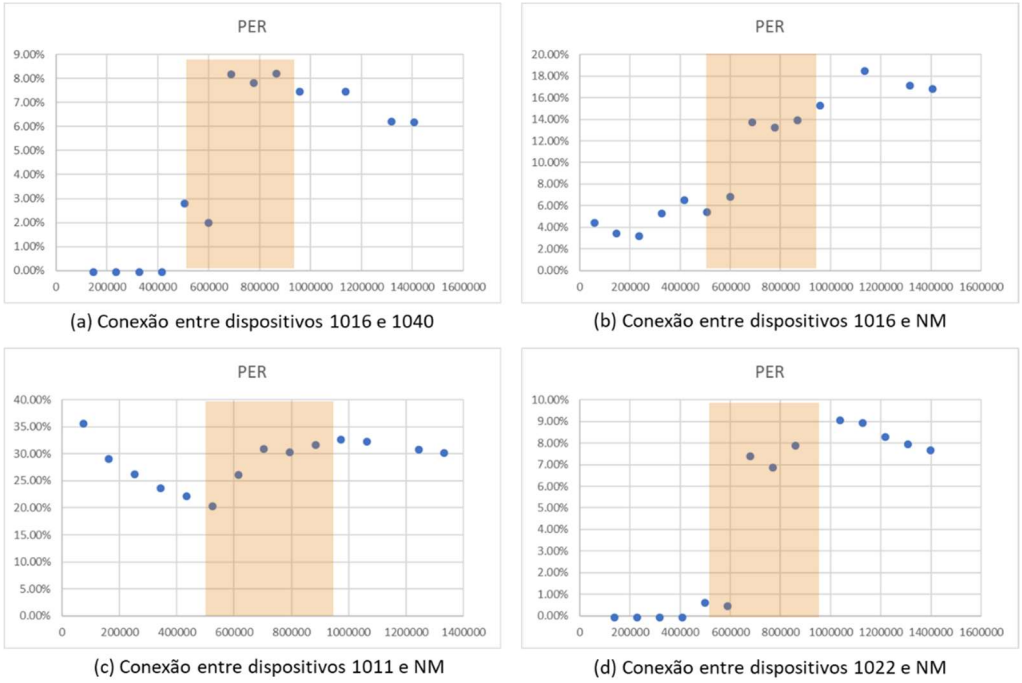
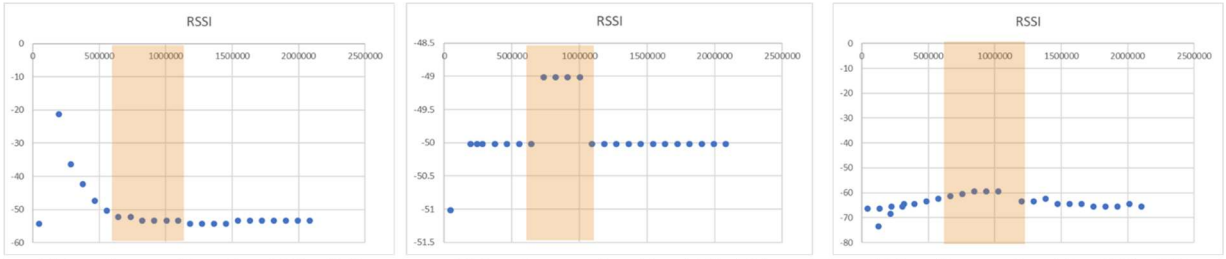


Figura 18: Gráficos de PER para pares de dispositivos sob impacto de interferência no terceiro estudo de caso.

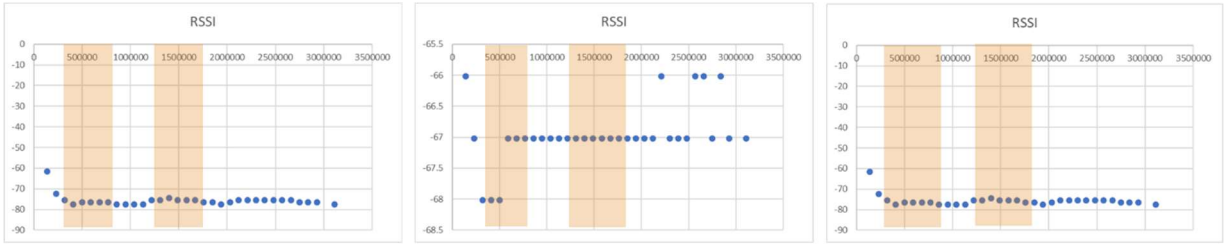
4.1.2. IMPACTOS EM *RECEIVED SIGNAL STRENGTH INDICATOR*

Diferentemente dos resultados obtidos sobre *Packet Error Rate*, os gráficos de *Received Signal Strength Indicator* não mostraram um impacto óbvio da interferência sobre a intensidade de sinal nos dispositivos receptores. As FigurasFigura 19, Figura 20 e Figura 21 mostram alguns dos resultados obtidos sobre cada estudo de caso.



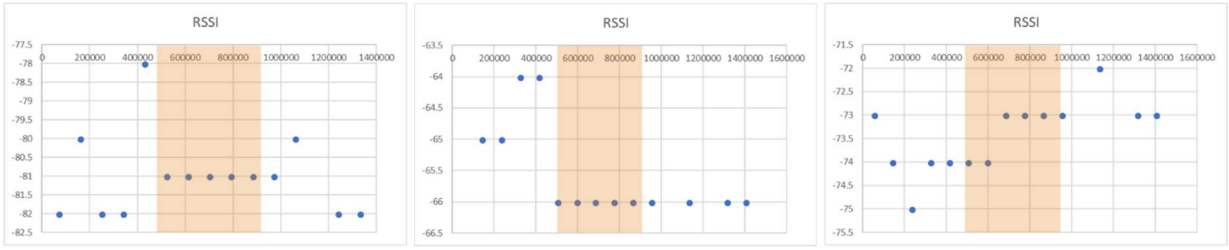
(a) Conexão entre dispositivos 1005 e 1022 (b) Conexão entre dispositivos 1005 e NM (c) Conexão entre dispositivos 1022 e NM

Figura 19: Gráficos de RSSI para pares de dispositivos sob impacto de interferência no primeiro estudo de caso.



(a) Conexão entre dispositivos 1016 e NM (b) Conexão entre dispositivos 1005 e 1016 (c) Conexão entre dispositivos 1016 e NM

Figura 20: Gráficos de RSSI para pares de dispositivos sob impacto de interferência no segundo estudo de caso.



(a) Conexão entre dispositivos 1011 e NM (b) Conexão entre dispositivos 1016 e 1040 (c) Conexão entre dispositivos 1016 e NM

Figura 21: Gráficos de RSSI para pares de dispositivos sob impacto de interferência no terceiro estudo de caso.

4.2. CONTRASTE ENTRE EXPERIMENTOS

Como pode ser inferido pelas plantas baixas das FigurasFigura 13,Figura 15 eFigura 17, cada experimento contou com uma quantidade variada de dispositivos de campo. Como cada dispositivo atua também como um roteador da rede e a intensidade de sinal apresenta correlação com performance ponto-a-ponto, quantidade e arranjo dos dispositivos podem apresentar impacto nas diferenças dos resultados mostrados.

Avalia-se também a possibilidade de que parte da diferença pode ser oriunda da diferença de intensidade de sinal entre os mesmos pares de dispositivos a cada estudo (como verificado na comparação entre os gráficos das FigurasFigura 20c e Figura 21c). Por mais que não houvesse qualquer contraste físico ou posicional nos dispositivos entre os estudos, cada estudo foi realizado em dias diferentes e, por isso, estava sujeito a interferências externas diferentes. Por não ser uma rede implementada em ambiente controlado, a rede Wifi do iPerf

está sujeita aos impactos da rede WirelessHART, como previsto, mas também ao impacto das demais redes WiFi do ambiente do laboratório, cujas bandas apresentam demandas variáveis e imprevisíveis.

O maior contraste quantificável identificado entre cada experimento, contudo, foi a quantidade de dados transferidos pelo iPerf. Como descrito na seção 3.4.2, o iPerf configura a rede para transmitir o máximo de dados dentro de um intervalo fixo de tempo, visando avaliar sua disponibilidade de banda. Quando comparadas as quantidades de dados transmitidos pelo iPerf em cada estudo, segundo reportado pelo próprio *software*, obtiveram-se os valores apresentados na Tabela 2.

Tabela 2: Quantidade e taxa média de transferência de dados no iPerf para cada estudo de caso, comparados à faixa de impacto em PER.

Estudo de Caso	Total de Dados Transmitidos (GB)	Taxa de Transferência Média (Mbps)	Faixa de Aumento em PER
#1	54	44,3	20-30%
#2	6	9,6	3-6%
#3	25,6	86,4	9-15%

Pode-se afirmar, com base nos dados dos três estudos, que a taxa de transferência de dados em cada estudo de caso apresenta correlação ao impacto em taxa de erros de pacote.

4.3. AVALIAÇÃO DOS RESULTADOS

4.3.1. CONTRASTE ENTRE IMPACTOS EM PER E RSSI

Dentre os três estudos de caso conduzidos, todos apresentaram impacto perceptível em *Packet Error Rate*. Como previsto na definição da métrica (seção 3.1.1), a presença de interferência por co-canal aumentou a quantidade de pacotes perdidos ponto-a-ponto, sendo a correlação entre PER e taxa de dados transferidos (a ser discutido na seção 4.3.2) o principal contraste mensurável.

Contudo, com exceção de exemplos pontuais como o denotado na Figura 19b, o impacto em *Received Signal Strength Indicator* não se mostrou perceptível. Mesmo parecendo contraintuitivo que interferências impactem em perda de pacotes mas não em perda de sinal, o fenômeno é explicável pela definição da métrica de acordo com a norma IEEE 802.15.4.

Segundo IEEE (2006), há duas funções de medição de interferência em um canal IEEE 802.15.4: ED (*Energy Detection,* ou "Detecção de Energia) e LQI (*Link Quality Indicator*, ou "Indicador de Qualidade de Conexão"). A função ED caracteriza uma estimativa de potência de todo e qualquer sinal recebido dentro do canal avaliado, sendo amplamente utilizada em estratégias de seleção de canal em roteamento. LQI, por outro lado, é uma estimativa de potência de sinal recebido (podendo ser do pacote recebido ou de SNR – *Signal-Noise Ratio,* ou "Proporção Sinal-Ruído"). A norma cita, inclusive, que a medição de LQI tanto em pacote recebido quanto em SNR pode permitir a estimativa da causa de eventuais perdas de pacotes, possibilitando a identificação de baixa intensidade de sinal do pacote ou de alta interferência, como consequente de um alto SNR.

RSSI, como visto na seção 3.1.2, se encaixa na definição de ED da norma IEEE 802.15.4. Sendo um parâmetro coletado pelo gerenciador de rede para dar entrada em seus algoritmos de roteamento (de modo a buscar transmitir pacotes pelo canal com menor índice de energia), o RSSI não distingue a energia no canal entre potência da interferência e potência do pacote recebido do dispositivo vizinho. Dessa forma, é possível concluir que o emprego de RSSI, uma medida de detecção de energia generalizada nos canais, não se mostra um parâmetro adequado para mensurar robustez em efeitos de coexistência, visto que, como nos estudos de caso supracitados, interferências por co-canal não apresentam impacto distinguível na intensidade de sinal do canal. LQI, por outro lado, poderia mensurar o impacto de intensidade de sinal especificamente nos pacotes da rede e, assim, possibilitaria a comparação de performance antes e após a interferência. Contudo, LQI não é especificamente empregado pela norma nas camadas de aplicação e rede (IEEE, 2006), de modo que sua implementação se mostra mais complexa.

4.3.2. CONTRASTE EM TRANSFERÊNCIA DE DADOS

Como mostrado na seção 4.2, o maior contraste quantificável entre cada estudo de caso, de modo a justificar os diferentes impactos em *Packet Error Rate*, foi a quantidade total de dados transferidos e a consequente taxa média de transferência de dados pela rede de interferência gerada através do *software* iPerf. Pela Tabela 2, percebe-se uma relação aproximadamente linear entre proporção de dados transmitidos e proporção de impacto percentual em perdas de pacotes.

Esse resultado indica uma forte relação de dependência entre quantidade de dados transmitidos em WiFi com perda de dados em WirelessHART. A hipótese é reforçada pela IEEE (2006), quando é citado que protocolos empregando o 802.15.4 em geral apresentarão perda de performance antes de seus interferentes quando em coexistência com o 802.11. Isso provém da diferença de intensidade de sinal entre as normas, sendo citado que dispositivos comerciais do 802.11 em geral operam com potências de transmissão na faixa de 12 a 18 dBm, enquanto que o 802.15.4 prevê o mínimo de transmissão em -10 dBm (seção 2.1.1). O valor comparativamente baixo de intensidade de sinal do 802.15.4 é configurado por ser citado como economicamente desvantajoso, visto que uma das métricas chave da norma é custo, mas apresenta impacto em perda de performance sob coexistência.

Mesmo considerando a desvantagem do 802.15.4 quando em coexistência com dispositivos 802.11, a coexistência de fato só se faz presente devido à sobreposição de canais. Como mostra a Figura 22, os canais de protocolos como o WirelessHART, seguindo a norma 802.15.4 de 2,4 GHz, apresentam coincidência com três canais da norma 802.11b.

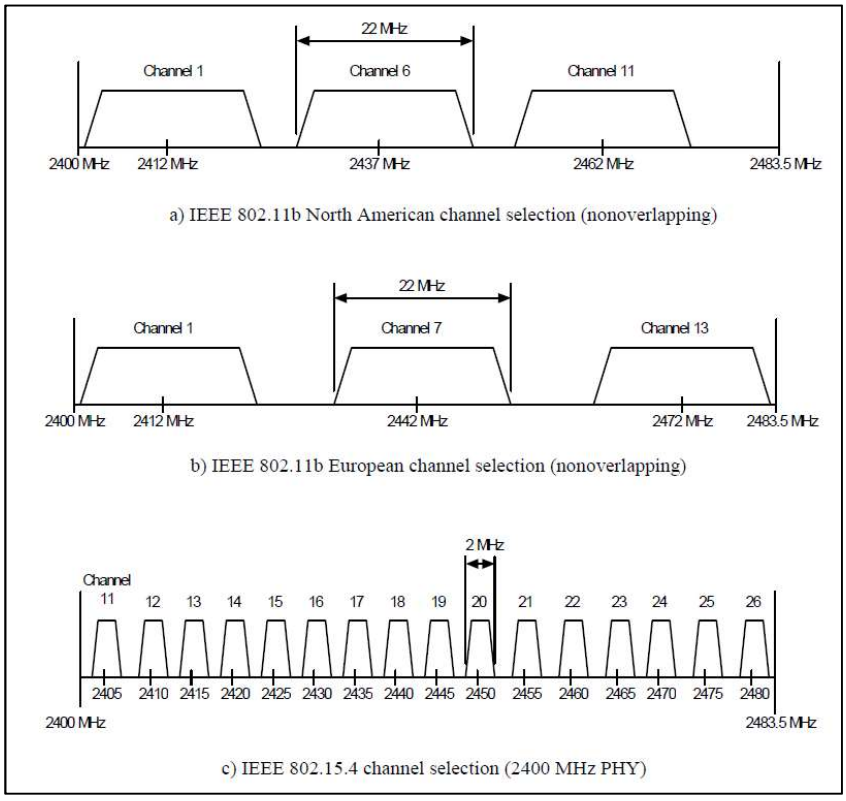


Figura 22: Comparação entre canais do WirelessHART e IEEE 802.11 (IEEE, 2006).

Durante os estudos realizados, a rede do iPerf foi implementada com um roteador WiFi configurado em B, G e N, fazendo alusão às variantes 802.11b, 8502.11g e 802.11n. A

diferença entre cada variante, entre outros fatores, é a quantidade de canais empregados e os valores mínimos e máximos da taxa de transferência (IEEE, 2009). Pelos valores obtidos na Tabela 2, avalia-se que a rede operou predominantemente nas variantes N, B e G nos experimentos #1, #2 e #3, respectivamente.

Conclui-se que nos experimentos #1 e #3, mesmo operando em variantes com mais disponibilidade de canais e consequente maior probabilidade de não apresentar conflito com o WirelessHART, a coexistência impactou de forma mais significativa na performance do WirelessHART quando o WiFi empregou a maior velocidade de transmissão de dados. Isso indica que mesmo identificando a presença de energia dos canais WirelessHART, a rede WiFi pode ter optado por transmitir seus pacotes nos canais coexistentes, visto que o impacto seria mais significativo no concorrente. Dessa forma, assim como avaliado por Han e Seungjoon (2007), quando em presente coexistência com redes 802.11, um algoritmo para seleção de canais que não apresentam coincidência (como o 15, o 25 e o 26) pode apresentar melhores resultados de performance para a rede WirelessHART.

4.3.3. IMPACTO EM CONFIABILIDADE E AVALIAÇÃO DE ROBUSTEZ

Paralelamente à utilização da ferramenta desenvolvida para avaliação de PER e RSSI, acompanhou-se a métrica de confiabilidade segundo o reportado pela interface do gerenciador de rede (Figura 10) nos experimentos #2 e #3. O menor valor encontrado durante interferência, em cada estudo de caso, está indicado na Tabela 3.

Tabela 3: Mínimos de confiabilidade encontrados em cada estudo de caso

Experimento	Mínimo de Confiabilidade
#1	N/A
#2	97,0%
#3	92,5%

Pelos resultados em PER, identifica-se que o impacto da interferência sobre a operação ponto-a-ponto é inegável, de modo que a capacidade da rede de manter o valor relativamente alto de confiabilidade mesmo fora de regime nominal de atuação pode classificá-la como robusta em todos os casos estudados.

CAPÍTULO 5 - CONCLUSÕES

O presente trabalho abordou a idealização, programação e validação de uma ferramenta em *software* para avaliação de performance ponto-a-ponto e análise de robustez de redes WirelessHART. Após a definição das métricas de campo a serem avaliadas e do estudo das camadas OSI do protocolo, elaborou-se, baseado em um *software* acadêmico de simulação de algoritmos de otimização de rotas, um ambiente em Java capaz de decriptar, interpretar e reportar parâmetros de qualidade de comunicação segundo a captura de transmissões obtidas através de um dispositivo de instrumentação passivo, o *sniffer*.

Os resultados obtidos através de estudos de caso permitiram inferir o impacto em performance ponto-a-ponto de uma rede WirelessHART prototipada quando sujeita a interferências por co-canal, mais especificamente coexistência com redes IEEE 802.11. As interferências, criadas a partir da utilização do *software* iPerf utilizando comunicação TCP sobre WiFi, apresentaram impacto na performance ponto-a-ponto, visto que a taxa de perda de pacotes da rede WirelessHART aumentou de forma proporcional ao emprego da disponibilidade de banda do WiFi. Contudo, as interferências não apresentaram impacto significativo na performance ponto-a-ponto referente à detecção de energia nos canais WirelessHART e na performance de confiabilidade conforme reportado pelo gerenciador de rede, indicando que a rede e o protocolo apresentam robustez ante coexistência.

5.1. CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Os resultados referentes a detecção de energia, que apresentaram uma aparente falta de relação entre coexistência e intensidade de sinal, puderam ser relacionados ao método de aquisição da variável empregada – o *Received Signal Strength Indicator* (RSSI), ou Indicador de Intensidade de Sinal Recebido. A hipótese levantada é a de que o RSSI é obtido como a detecção de energia no canal pelo qual o dispositivo receptor avalia a transmissão, mas não se realiza uma identificação da fonte de energia. O RSSI é relevante para o gerenciador de rede, visto que seus algoritmos internos de otimização de rotas devem levar em consideração a quantidade de energia detectada em cada canal e, assim, escolher rotas que priorizem canais com as menores intensidades de sinal (sejam oriundas de interferência ou de dispositivos da própria rede WirelessHART), mas não se mostra uma variável interessante para a avaliação de performance ponto-a-ponto. Como alternativa, levantou-se a possibilidade de se

desenvolver uma ferramenta que capture e calcule o *Link Quality Indicator* (LQI) ou Indicador de Qualidade de Conexão, uma variável de detecção de energia que leva em consideração a origem da fonte – seja o pacote recebido ou o SNR (*Signal-Noise Ratio* ou Proporção Sinal-Ruído). Essa métrica possibilitaria a avaliação da perda de performance ponto-a-ponto sob coexistência e ainda permitiria determinar, caso a caso, se um eventual pacote perdido apresentou baixa intensidade de sinal do emissor e/ou alta intensidade de interferência.

A correlação entre aumento da taxa de perda de pacotes com o aumento do emprego de banda da rede interferente indica a desvantagem do WirelessHART ante redes coexistentes 802.11, oriundo da menor intensidade de sinal do 802.15.4. Mesmo havendo menor probabilidade de interferência por co-canal considerando uma maior quantidade de canais nas variantes G e N do 802.11, foram nestes casos que o maior impacto em perda de pacotes foi identificado. Com isso, realça-se a oportunidade de desenvolvimento de um algortimo de otimização de canais que priorize os canais 15, 25 e 26 uma vez identificada a coexistência, visto que estes não apresentam coincidência com canais do 802.11.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAMPATZIS, T., LYGEROS, J., MANESIS, S. **A Survey of Applications of Wireless Sensors and Wireless Sensor Networks**. Limassol: IEEE Press, 2005.

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

DOMINICS, C. M. et al. **Investigating WirelessHART coexistence issues through a specifically designed simulator**. New York: IEEE Press, 2009.

DUGAN et al. **iPerf - The ultimate speed test tool for TCP, UDP and SCTP.** Disponível em <https://iperf.fr/>. Acesso em maio, 2018.

EMERSON ELECTRIC CO. **Emerson Wireless 1420 Gateway**. Disponível em: <http://www.emerson.com/en-us/catalog/emerson-1420>. Acesso em maio, 2018.

GOLMIE, N. **Coexistence in Wireless Networks**. New York: Cambridge University Press, 2006.

HAN, B. SEUNGJOON, L. **Efficient packet error rate estimation in wireless networks**. New York: IEEE Press, 2007.

HCF: HART COMMUNICATION FOUNDATION. **HCF_SPEC-065, Rev. 1.0**. Austin: HCF, 2007.

IEEE: INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE Std 610.12-1990 - IEEE Standard Glossary of Software Engineering Terminology**. New York: IEEE Standards Board, 1990.

IEEE: INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE Std 802.15.4-2006 – Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)**, New York: IEEE Computer Society, 2006.

IEEE: INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE Std 802.11n-2009 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**, IEEE Computer Society, 2009.

IEC: INTERNATIONAL ELECTROTECHNICAL COMMISSION**. IEC 62591, REV 1.0**, Massachusetts: IEC, 2010.

KUNZEL, GUSTAVO. **Ambiente para avaliação de estratégias de roteamento para redes WirelessHART**. 2012. 95 f. Dissertação (Mestrado em Engenharia Elétrica) - Programa de Pós-Graduação em Engenharia Elétrica, Universidade Federal do Rio Grande do Sul, Porto Alegre, RS, 2012.

MULLER, I. et al. **Development of WirelessHART Compatible Field Devices**. Austin: IEEE Press, 2010.

MULLER, I., NETTO, J.C., PEREIRA, C.E. **WirelessHART Field Devices**. New York: Instrumentation & Measurement Magazine, 2011.

SIKORA, A., GROZA, V. **Coexistence of IEEE 802.15.4 with other Systems in the 2.4 GHz ISM Band**. New York: IEEE Press, 2005.

SUBBU, K. P. HOWITT, I. **Empirical Study of IEEE 802.15.4 Mutual Interference Issues**. New York: IEEE Press, 2007.

WANG, H., SEAH, W.K.G., KONG, P.Y. **Maximizing End-to-End Reliability of Routing with Redundant Path by Optimal Link Layer Scheduling**. Kowloon: IEEE Press, 2007.

WANG, N., ZHANG, N. WANG, M. **Wireless Sensors in Agriculture and Food Industry – Recent Development and Future** Perspective, Amsterdam: Computer and Electronics in Agriculture, 2006.

WINTER, J. M. *et al*. **Study of routing mechanisms in a WirelessHART network**. Cape Town: IEEE Press, 2013.