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

CHRISTIAN ALAN KRÖTZ

FERRAMENTA E MÉTODO PARA OBTENÇÃO DE PARÂMETROS DE CONFIABILIDADE FIM-A-FIM DE REDES INDUSTRIAIS SEM FIO

Porto Alegre
2019

CHRISTIAN ALAN KRÖTZ

FERRAMENTA E MÉTODO PARA OBTENÇÃO DE PARÂMETROS DE CONFIABILIDADE FIM-A-FIM DE REDES INDUSTRIAIS SEM FIO

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: Prof. Dr. Ivan Müller

Porto Alegre
2019

CHRISTIAN ALAN KRÖTZ

FERRAMENTA E MÉTODO PARA OBTENÇÃO DE PARÂMETROS DE CONFIABILIDADE FIM-A-FIM DE REDES INDUSTRIAIS SEM FIO

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. Ivan Müller, UFRGS
Doutor pela Universidade Federal do Rio Grande do Sul – Porto Alegre, Brasil

Banca Examinadora:

Prof. Dr. Dennis Brandão, USP
Doutor pela Universidade de São Carlos – São Paulo, Brasil

Prof. Dr. João César Netto, UFRGS
Doutor pela Universidade Federal do Rio Grande do Sul – Porto Alegre, Brasil

Prof. Dr. Edison Pignaton de Freitas, UFRGS
Doutor pela Universidade Federal do Rio Grande do Sul – Porto Alegre, Brasil

Coordenador do PPGEE: _____
Prof. Dr. João Manoel Gomes da Silva Jr.

Porto Alegre, Março de 2019.

AGRADECIMENTOS

Ao professor Ivan Müller, por prover a oportunidade de trabalho na área de pesquisa e pela confiança depositada nesta realização.

Aos colegas do LASCAR em especial ao Gustavo Cainelli, Leomar Mateus Radke e Max Feldman, pelo auxílio nas tarefas e pesquisas desenvolvidas durante este período.

Aos meu pais, que me inspiram e me apoiam incondicionalmente.

À minha namorada, pelo incentivo, paciência e apoio para a conclusão desta etapa.

Aos amigos e familiares que de alguma forma contribuíram e me apoiaram durante este período.

Aos funcionários do Programa de Pós-Graduação em Engenharia Elétrica da UFRGS, pela assistência durante o período do mestrado.

À CAPES, pela provisão da bolsa de mestrado.

RESUMO

Sistemas de comunicação sem fio vem sendo cada vez mais empregados na indústria. Nesse contexto, os protocolos WirelessHART e ISA 100.11a são os mais utilizados atualmente, devido ao pioneirismo e elevada robustez. Este trabalho tem como objetivo geral realizar o estudo da latência de comunicações fim-a-fim em redes industriais sem fio, utilizando o WirelessHART como estudo de caso, visando a avaliação da aplicabilidade destas redes no controle de processos industriais. Para tanto, uma ferramenta para comunicação com o *gateway* da rede, capaz de extrair informações dos dispositivos de campo e do próprio *gateway*, é desenvolvida e utilizada em estudos de caso. Os estudos de caso contemplam métodos para avaliação da qualidade de serviço da rede, através da observação da latência das comunicações fim-a-fim, em situações de falhas diversas. As falhas são injetadas na rede e monitoradas pela própria ferramenta desenvolvida. Os resultados obtidos revelam que a ferramenta é capaz de analisar e obter de forma concreta os dados de latência da rede, sendo a sua utilização adequada para os mais diversos estudos sobre comunicação de redes industriais sem fio.

Palavras-chave: WirelessHART, Confiabilidade, Robustez, Latência, Redes sem fio, Redes industriais.

ABSTRACT

0 Wireless communication systems have been increasingly employed in the industry. In this context, the WirelessHART and ISA 100.11a protocols are the most used today due to the pioneering and high robustness. This work has as general objective to study the end-to-end communications latency in wireless industrial networks, using WirelessHART as a case study, aiming the evaluation of the applicability of these networks in the control of industrial processes. For this purpose, a tool for communication with the network gateway, capable of extracting information from the field devices and the gateway itself, is developed and used in case studies. The case studies contemplate methods to evaluate the quality of service of the network, by observing the latency of the end-to-end communications, in situations of diverse failures. The faults are injected into the network and monitored by the developed tool itself. The results show that the tool is capable of analyzing and obtaining the latency data of the network in a concrete manner, and its use is adequate for the most diverse studies on wireless industrial network communication.

Keywords: WirelessHART, Reliability, Robustness, Latency, Wireless networks, Industrial networks.

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ACK	*Acknowledge*
ASN	*Absolute Slot Number*
CSS	*Cascading Style Sheets*
HTML	*Hypertext Markup Language*
IP	*Internet Protocol*
NCS	*Networked Control Systems*
NPDU	*Network Protocol Data Unit*
OSI	*Open System Interconnection*
PHP	*Hypertext Preprocessor*
RF	Rádio Frequência
PA	*Power Amplifier*
RSL	*Received Signal Level*
RSSFI	Redes de Sensores Sem Fio Industriais
TCP	*Transmission Control Protocol*
TX	*Transmit*
RX	*Receive*
UDP	*User Datagram Protocol*
WH	*Wireless*HART

1 INTRODUÇÃO

Nos últimos anos, as Redes de Sensores Sem Fio Industriais (RSSFI) deixaram de ser uma tecnologia promissora, para se tornarem uma tecnologia de fato usada em aplicações industriais (RAPOSO et al., 2017). As RSSFI estão ganhando impulso em relação às tecnologias cabeadas, pois oferecem benefícios tais como baixo custo operacional, facilidade de instalação, autoconfiguração e flexibilidade, o que as tornam desejáveis para aplicações industriais (MULLER, 2012). Como consequência de seu enorme potencial, na última década, esforços tem sido feitos para tornar a tecnologia das RSSFI confiável, robusta, interoperável e pronta para substituir as tecnologias tradicionais (RAPOSO et al., 2017). Com o passar do tempo as RSSFI foram padronizadas e protocolos tais como IEEE802.15.4e, OpenWSN, *Wireless*HART (WH), Zigbee PRO, ISA100.11a e WIA-PA foram desenvolvidos.

Apesar das diversas vantagens oferecidas pelas RSSFI, também há desvantagens, principalmente relacionadas à confiabilidade e latência, que podem não ser adequadas para utilização em sistemas de malha fechada, como provado em diversos estudos. Diferentes tipos de falhas podem ocorrer em RSSFI. Tais como, falha de *links* de rede, congestionamentos na rede e pacotes corrompidos ou perdidos (PARADIS; HAN, 2007). O controle da latência fim-a-fim é fundamental para muitas aplicações e serviços baseados em *Networked Control Systems* (NCS), que vem encontrando aplicação em uma ampla gama de áreas. Como por exemplo, aplicações que incluem automação industrial, redes de sensores móveis, cirurgia remota, sistemas rodoviários automatizados e veículos aéreos não tripulados (HESPANHA; NAGHSHTABRIZI; XU, 2007). Embora a medição de desempenho de redes com fio tenha sido amplamente estudada, a medição e a quantificação do desempenho de redes sem fio enfrentam novos desafios e exigem diferentes abordagens e técnicas (GALLOWAY; HANCKE, 2013). No que se refere ao estudo das

NCS argumenta-se que, desde que as métricas de desempenho, como a latência, possa ser medida com precisão nas camadas mais baixas do protocolo, a avaliação de desempenho é facilitada nas camadas superiores do protocolo. Este fato motiva a criação de um método para avaliação da qualidade de serviço da rede, através da obtenção da latência das comunicações fim-a-fim, em situações de falhas diversas.

Este trabalho apresenta métodos e o desenvolvimento de uma ferramenta que utiliza tais métodos, para obtenção de informações de RSSFI de modo que é possível avaliar o comportamento temporal da mesma, tanto em funcionamento normal quanto sob condições de falhas. Por conveniência e por abrangência do uso, são utilizadas redes WH, mas o método é extensível a outros protocolos.

A avaliação temporal refere-se especificamente na obtenção dos atrasos fim-a-fim, parâmetro relevante em redes sem fio com múltiplos saltos de comunicações. São avaliados os tempos em fluxos de baixo para cima (*uplink*) e de cima para baixo (*downlink*), onde o maior valor é o *gateway* (por onde se faz o acesso externo à rede) e o menor valor é o dispositivo de campo, conectado diretamente à planta.

Os métodos e ferramenta desenvolvidos servem para dois propósitos fundamentais: o primeiro, avaliar a empregabilidade da rede em NCS (*Networked Control Systems*), e o segundo, a utilização como um sistema do tipo *site survey*. O primeiro refere-se à obtenção das latências, que constituem os principais problemas relacionados com a estabilidade do sistema de controle, e o segundo, refere-se a uma ferramenta capaz de obter dados prévios para avaliação de uma instalação final deste tipo de rede, onde é possível saber de antemão se determinada configuração espacial/temporal vai atender os requisitos demandados. Nesse sentido, a ferramenta é capaz de emular falhas típicas, tais como bloqueios, interferências, falhas de *hardware*, entre outras.

A apresentação deste trabalho é organizada da seguinte forma: no Capítulo 2, são apresentados os conceitos básicos utilizados ao longo da dissertação. Um estudo sobre o estado da arte é apresentado no Capítulo 3, apresentando os trabalhos anteriormente realizados. Os meios e ferramentas usados na dissertação estão descritos no Capítulo 4. A implementação da ferramenta está descrita no Capítulo 5. Os estudos de caso para a validação da proposta e a apresentação dos resultados obtidos é apresentada no Capítulo 6. O trabalho é finalizado com as conclusões sobre os resultados obtidos e sugestões para a continuidade do trabalho no Capítulo 7.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo é apresentada uma revisão dos sistemas de comunicação sem fio industriais, com destaque para o protocolo WH, uma vez que este protocolo foi utilizado na validação da proposta. É apresentada também uma revisão sobre técnicas de clusterização aplicadas a análise probabilística. Aborda-se ainda a confiabilidade destes protocolos, bem como as principais possíveis falhas que podem demandar diferentes tipos de falhas na rede.

2.1 Sistemas de comunicação sem fio industriais

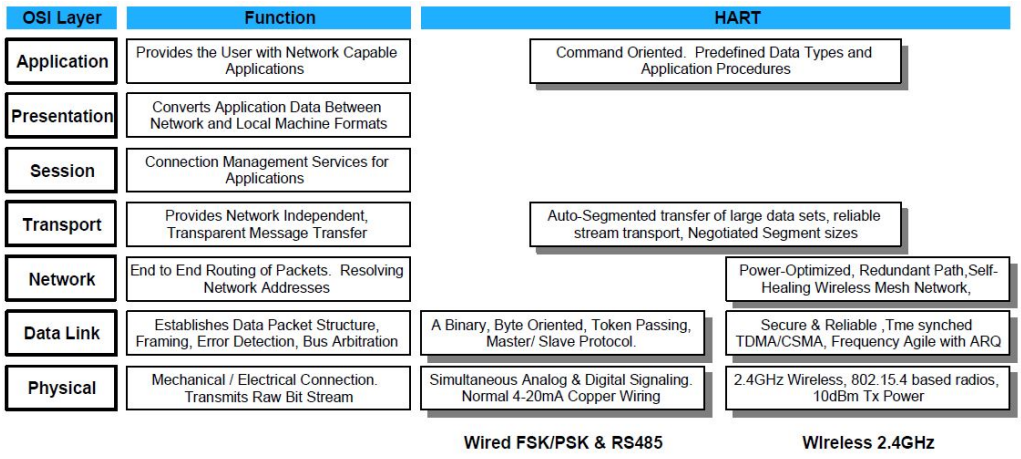
As RSSFI típicas requerem pouca infraestrutura. O projeto das RSSFI depende significativamente dos requisitos da aplicação em particular, uma vez que diferentes aplicações podem ter diferentes requisitos e finalidades (WANG; JIANG, 2016). O uso das RSSFI adquiriram uma enorme atenção devido a seus requisitos e desafios, pois oferecem alternativas atraentes com relação as redes cabeadas, ajudando a melhorar a qualidade do produto, agilizando operações, acelerar a produção, facilitar a instalação, aumentar a flexibilidade e mobilidade nas fábricas, reduzindo os gastos com infraestrutura e danos causados nos cabos em chão da fábrica, lidando com máquinas em movimento (MULLER, 2012).

Com a internacionalização e com o rápido desenvolvimento das RSSFI, diversos protocolos de comunicação para este tipo de rede foram desenvolvidos tais como, o WH, o WIA-PA, o ISA100.11a e o ZigBee (WANG; JIANG, 2016). Como todos estes protocolos são baseados no IEEE 802.15.4, existem muitas semelhanças entre si, no entanto, existem também diferenças significativas, que acarretam em vantagens e desvantagens de cada protocolo. Para o desenvolvimento desta proposta, optou-se pela utilização do pro-

tocolo WH para a validação da proposta, uma vez que este protocolo está disponível em laboratório, bem como a pilha do protocolo. Alia-se ao fato de que este é o protocolo mais amplamente empregado na indústria atualmente.

As comunicações no WH ocorrem em *slots* de tempo de 10 ms cada (MULLER, 2012). Os slots podem ser dedicados através de mecanismos de acesso ao meio determinístico (TDMA), ou compartilhados entre vários nós da rede, disputados por meio do mecanismo CSMA-CA (*Carrier sense multiple access with collision avoidance*). Os valores máximos de latência são estabelecidos pelo escalonamento da comunicação de modo que os pacotes alcançam seus destinos em tempo conhecido, considerando o número máximo de saltos na rede e possíveis retransmissões. As ligações entre os nós da rede são feitas por meio de *superframes* que são repetidos periodicamente para proporcionar tráfego das comunicações na rede. De acordo com o modelo de sete camadas OSI (*Open System Interconnection*) apresentados na Figura 1, o WH contém claramente as camadas física, enlace, rede, transporte, embora a funcionalidade de algumas das camadas seja um pouco diferente do modelo original.

Figura 1: Camadas do modelo OSI do WH



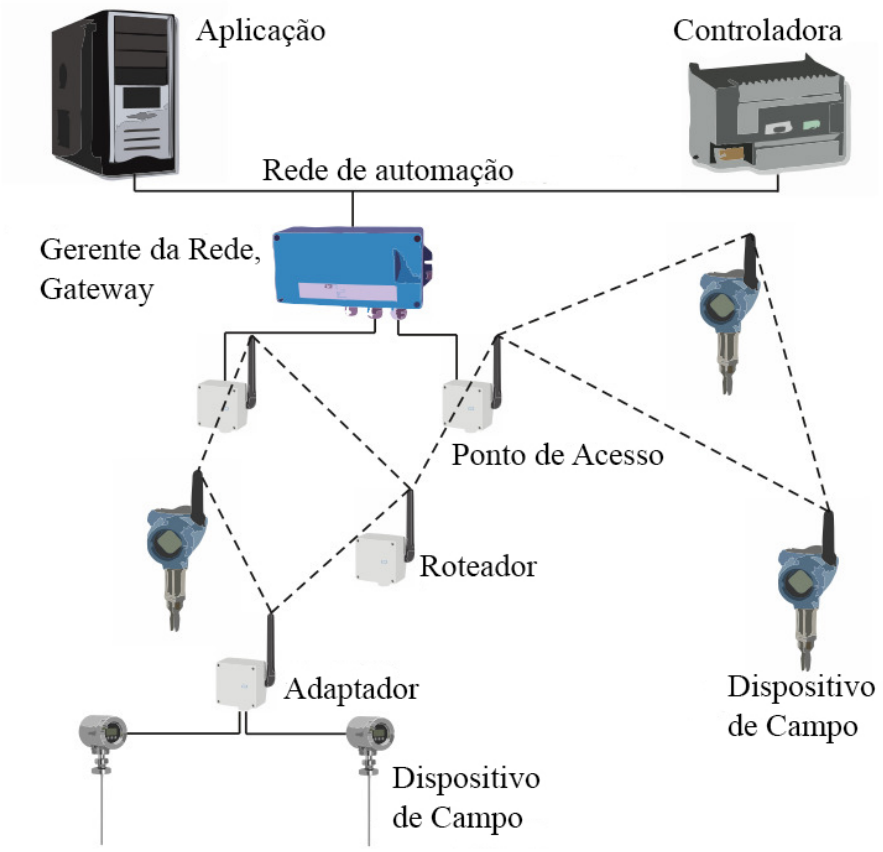
Fonte: (HART COMMUNICATION FOUNDATION, 2008a).

O protocolo WH foi desenvolvido com o objetivo de estabelecer um padrão de comunicação sem fio para uso em aplicações industriais. O WH é uma extensão do protocolo cabeado HART (HART COMMUNICATION FOUNDATION, 2008b) e permite compatibilidade total com sistemas legados, suportando aplicações por ciclos desde 250 ms. Por ser um protocolo seguro, sincronizado em tempo e de baixo consumo, é adequado ao controle de processos industriais. A compatibilidade é definida basicamente pela estru-

tura de comandos DDL (*device description language*), anteriormente desenvolvida pela organização HART (SMAR, 2018).

O protocolo especifica três elementos principais para a formação da rede (CHEN; NIXON; MOK, 2010): dispositivos de campo sem fio (*Field Devices*), o *Gateway* e o gerenciador de rede (*Network Manager*). Os dispositivos de campo podem ser sensores ou atuadores dispostos na planta. O *gateway* possibilita a comunicação entre o *host* da planta e os dispositivos de campo, possuindo assim, um ou mais pontos de acesso à rede. O gerenciador de rede é responsável pela configuração da mesma, por meio do agendamento das comunicações entre os dispositivos, pela criação e manutenção dos *superframes* e dos *links*, gerenciando as tabelas de roteamento de mensagens e reportando o estado geral da rede. A estrutura geral de uma rede WH pode ser visualizada na Figura 2. Nela, é possível identificar os elementos que compõem uma rede WH.

Figura 2: Topologia de uma rede WH



Fonte: Adaptado de (KUNZEL, 2012).

2.2 Análise de confiabilidade de redes

Confiabilidade e robustez são parâmetros críticos na escolha de um protocolo de comunicação sem fio para que possa ser usado na indústria (WINTER et al., 2011). O controle e o monitoramento de processos em ambientes industriais vêm mudando nos últimos anos, devido ao crescente avanço das pesquisas relacionadas às redes industriais sem fio (MACHADO et al., 2014). Há semelhanças entre os padrões de RSSFI, pois utilizam bandas de frequência não licenciadas, cujo meio físico é tipicamente suscetível a interferências de rádio, como a adoção de intervalos de tempo no nível MAC, para suportar a comunicação em tempo real (VALLE et al., 2015).

No entanto, apesar dos esforços consideráveis para fornecer mecanismos que aumentem a disponibilidade, confiabilidade, segurança e capacidade de manutenção da rede, as RSSFI mantém como característica indesejável, a elevada propensão à falhas devidas aos fenômenos de propagação de ondas eletromagnéticas (RAPOSO et al., 2017). Alguns exemplos de falhas tipicas das RSSFI, são falhas de enlace, congestionamento e pacotes corrompidos ou perdidos, devido a bloqueios, mudança de rotas de comunicação ou problemas relacionados à coexistência de redes.

As RSSFI podem ser definidas como redes de dispositivos distribuídos, e trabalham cooperativamente para comunicar informações, coletadas do campo, e monitoradas por meio de *links* sem fio. Os dados coletados pelos diferentes nós, são enviados para um gerenciador que usa os dados localmente ou está conectado a outras redes, por meio de um *gateway*. As tecnologias empregadas nas RSSFI oferecem inúmeras vantagens em relação a soluções de redes convencionais, permitindo que sejam utilizados em uma ampla gama de aplicações (BELKNENI et al., 2018). Assim, as RSSFI podem ser empregadas para dar suporte a aplicações críticas, e, portanto, é essencial garantir que o desempenho possa ser assegurado ou controlado nesses ambientes, a fim de torná-los confiáveis.

Segundo (SILVA et al., 2012), existem dois tipos de falhas que podem ocorrer numa RSSFI: as falhas transitórias, que geralmente afetam os *links* de comunicação entre os dispositivos de rede, e são tipicamente causadas por interferências, coexistência ou bloqueios, e as falhas permanentes, que afetam os dispositivos da rede, tendo origem normalmente no *hardware*. Como exemplo de falha permanente, pode-se considerar o desligamento por falta de energia, falha de *hardware* ou a retirada inadvertida de um nodo da rede, acarretando a perda de comunicação entre dois pares (SAIFULLAH et al., 2014).

Desse modo, as RSSFI devem ser confiáveis e funcionar adequadamente, de forma com que os dados possam ser entregues de maneira confiável e segura ao seu destino e com latência máxima atendida (BELKNENI et al., 2018). Sendo assim, estas falhas foram implementadas, emuladas, analisadas e serão abordadas mais adiante.

2.3 Latência

RSSFI são uma infra-estrutura de comunicação emergente para aplicações de monitoramento e controle em indústrias de processo. Em um sistema de controle de realimentação onde os *loops* de controle em rede são fechados, os dispositivos do sensor enviam periodicamente os dados para os controladores, e os dados de entrada de controle são então entregues aos atuadores através da rede. Para manter o desempenho de estabilidade e controle, aplicações de monitoramento e controle industrial impõem requisitos de atraso fim-a-fim rigorosos na comunicação de dados entre sensores e atuadores (SAIFULLAH et al., 2015).

O WH foi projetado como um protocolo aberto para RSSFI buscando enfrentar os desafios do monitoramento e controle industrial. Para atender aos rigorosos requisitos de confiabilidade em ambientes industriais hostis, o protocolo apresenta uma arquitetura de gerenciamento de rede centralizada, acesso múltiplo por divisão de tempo, TDMA, rotas redundantes e saltos entre canais. Essas características introduzem desafios únicos na análise de atrasos fim-a-fim para monitoramento e controle de processos (SAIFULLAH et al., 2015).

A latência ou atraso, definido como o tempo que leva um pacote para viajar da origem para o destino, tem sido um dos fatores críticos que afetam o desempenho das RSSFI, podendo levar à instabilidade do sistema (CHUNG et al., 2016). O reconhecimento do atraso das comunicações é importante para investigar os efeitos que eles causam e suas consequências. Embora o protocolo WH aborde algumas limitações das NCS com fio, e mesmo com confiabilidade muito alta, atrasos e perda de pacotes, devido à chegada tardia das mensagens são a chave dos problemas associados à rede. Neste trabalho não foi avaliado a periodicidade do comportamento da rede sob falha, sendo assim, considera-se mais adequado o uso das palavras latência máxima e latência mínima ao invés de *jitter*.

Sem o conhecimento do atraso ou das incertezas no tempo de chegada dos sinais de controle, o desempenho das RSSFI será severamente afetado. Esses atrasos são causados,

por exemplo, quando um novo dispositivo quer se conectar na rede, durante a manutenção da rede, dispositivos em movimento, entre outros. O tempo de resposta do controle de uma planta consiste em vários componentes de atraso, como atraso bidirecional fim-a-fim do controlador para o atuador, do sensor para o controlador, além de cada atraso interno do dispositivo individual (gateway, sensor, atuador, controlador). A informação combinada de atraso (atraso de ida e volta) é essencial para avaliar o desempenho do controle de uma planta (JIN; WANG; ZENG, 2015).

3 ANÁLISE DO ESTADO DA ARTE

Com o intuito de realizar o estudo da latência de comunicações fim-a-fim em redes WH e, visando a avaliação e a aplicabilidade destas redes no controle de processos industriais, fez-se uma revisão dos artigos relacionados. Uma vez que a comunicação deste, assim como de todos os protocolos de comunicação sem fio são suscetíveis a falhas de transmissão devido aos fenômenos de propagação de ondas eletromagnéticas, dificultando a análise da escalabilidade dos fluxos de dados. O WH adota o roteamento por grafos para lidar com falhas de transmissão por meio de retransmissões e diversidade de rotas, e a latência está relacionada com as técnicas de escalonamento e roteamento empregadas.

Tendo como ideia o desenvolvimento de uma ferramenta para a obtenção da latência na comunicação fim-a-fim e a inserção de falhas na rede em diversos estudos de casos, os trabalhos desenvolvidos por (WINTER, 2010) e (WINTER et al., 2011) vão de encontro com a proposta aqui apresentada, uma vez que o autor deu início ao desenvolvimento do *software* para obtenção de dados de redes WH, utilizado no desenvolvimento desta dissertação. O *software* anteriormente desenvolvido permite identificar questões relevantes para a verificação e manutenção de redes WH, apresentando como contribuição a capacidade de personalizar dos testes, sendo permitido avaliar dados de maior interesse para uma finalidade específica. Os estudos de caso apresentados, foi possível identificar as rotas mais utilizadas da rede que levam à identificação dos "gargalos", ou seja, locais da rede onde a latência pode ser aumentada devido a sobrecargas de roteamento, ou locais onde a rede é mais suscetível a falhas generalizadas devido a falhas locais (bloqueios ou problemas de *hardware*).

Com o objetivo de inserir falhas na rede para a realização dos estudos de caso, (SILVA et al., 2011) propõe um modelo de simulação utilizando Redes de Petri Estocásticas, na ferramenta Mobius, com o finalidade de avaliar redes WH na presença de falhas transitó-

rias, assumindo que essas falhas resultam de ambientes ruidosos que perturbam a comunicação entre os dispositivos. Posteriormente (SILVA et al., 2012) realizam a avaliação de confiabilidade das melhores práticas indicadas pelo HART Communication Foundation (HCF), quando os dispositivos de rede estão sujeitos a falhas permanentes. Os resultados apresentados pelo autor mostram que as melhores práticas têm impacto diferente na rede.

No trabalho de (KUNZEL et al., 2012) é proposta uma arquitetura de software para inspeção de redes WH. A captura de informações é feita de maneira passiva usando *Sniffer* implantado na rede. As mensagens são filtradas de acordo com a análise e a visualização é feita por meio de grafos, gráficos e listas. Uma rede WH foi implantada em laboratório para avaliação de desempenho usando a ferramenta desenvolvida. O estudo feito por (KARBASCHI; SAILHAN; ROVEDAKIS, 2012) propõem uma arquitetura para injeção de falhas, concentrando em uma rede de sensores que visa detectar a presença de veículos em estacionamentos. O autor busca caracterizar as falhas geradas por este sistema como o primeiro passo no desenvolvimento de um injetor de falhas.

Já (MACHADO et al., 2013) apresenta uma ferramenta para inspeção e análise lógica e física da rede, apresentando como vantagens a mobilidade e a inspeção em todos os 15 canais da uma rede WH utilizando apenas um rádio, que é programado dinamicamente durante o funcionamento da rede. O sistema tem a capacidade de medição do nível de energia nos 15 canais de RF (Rádio Frequência) e produz informações sobre aspectos lógicos dos enlaces. Dando continuidade no trabalho ja desenvolvido (MACHADO et al., 2014) propõe algumas melhorias na ferramenta, desenvolvendo um aplicativo *off-line* que apresenta diversas análises sobre os dados capturados. Os resultados mostram que a ferramenta funciona de maneira similar a um *sniffer* multicanais, capaz de realizar a detecção de interferência na rede.

(NOBRE; SILVA; GUEDES, 2014) realizaram uma avaliação do consumo de energia e confiabilidade em um cenário industrial de RSSFI com *links* defeituosos, usando o simulador de redes NS-3 para a camada física WH. A proposta inclui o modelo de erro, posicionamento da estação, atenuação do sinal e consumo de energia, sendo possível configurar cada *link* com diferentes probabilidades de falha, mas somente em ambientes simulados. Já (SOTO et al., 2014) apresentam uma proposta de desenvolvimento de um sistema de controle em malha fechada sobre a rede WH por meio de uma aplicação hospedeira usando um cenário real. O autor apresenta alguns problemas do controle em redes

sem fio e a implementação de uma arquitetura para controle por meio de uma aplicação hospedeira para redes WH, o que diferencia o trabalho do autor com o aqui proposto é que o autor faz uso do protocolo UDP para as comunicações com o *gateway*, e ainda, verifica o atraso fim-a-fim na camada de aplicação.

O estudo desenvolvido por (SANTOS, 2015), também foi considerado como referência para o presente trabalho visto que este realiza uma abordagem sobre o problema da análise de ativos em redes industriais sem fio para o padrão WH, implementando um sistema de monitoramento que permitindo realizar as mais diversas atividades de gestão de ativos, independentemente do fabricante. Posteriormente (SANTOS et al., 2015) apresenta uma avaliação do comportamento de uma rede WH em um processo de controle de nível de água em um sistema de tanques acoplados, usando a latência e a confiabilidade da rede como métricas de avaliação, gerando os resultados através de ensaios reais.

Com a finalidade de avaliar uma rede WH em situações adversas causadas por injeções de falhas, (WINTER et al., 2016) utilizam uma rede WH, aonde a rede é modificada e controlada para produzir um cenário específico em que uma falha de rádio pode levar a uma falha de rede. O estudo aponta que a falha leva a uma interpretação errônea do estado da rede, o que é provado na prática. Propostas para a identificação e resolução de problemas são apresentadas pelos autores. Um ponto negativo deste trabalho é que as falhas são inseridas manualmente na rede, e não por meio de uma ferramenta como é a proposta deste trabalho.

No trabalho de (RAPOSO et al., 2017) apresenta-se uma ferramenta de diagnóstico de pós-implantação de uma RSSFI para um padrão Industrial Internet of Things (IIoT) em uma aplicação industrial real usando dois componentes: uma ferramenta de registro e um algoritmo para mineração de dados, a proposta dos autores baseia-se no padrão WH. A fim de comparar ferramentas, (HASSAN et al., 2016) apresenta uma rede WH usando um kit de avaliação de redes em escala laboratorial, avaliando o efeito de localizar os vários dispositivos na rede. Embora o software ainda esteja em fase de desenvolvimento, o autor obteve alguns resultados ainda que falte uma implementação real para controle.

Nesse contexto, foi feita uma comparação mais abrangente de algumas aspectos mais relevantes dentre os trabalhos aqui citados, quem tem correlação com o desenvolvimento de uma ferramenta para a análise da rede, método para obtenção da latências das comunicações com os dispositivos e ainda estudos referentes as inserção de falhas na rede, as

quais se encontram de forma sintetizada na Tabela 1.

Tabela 1: Comparação entre as referências consultadas

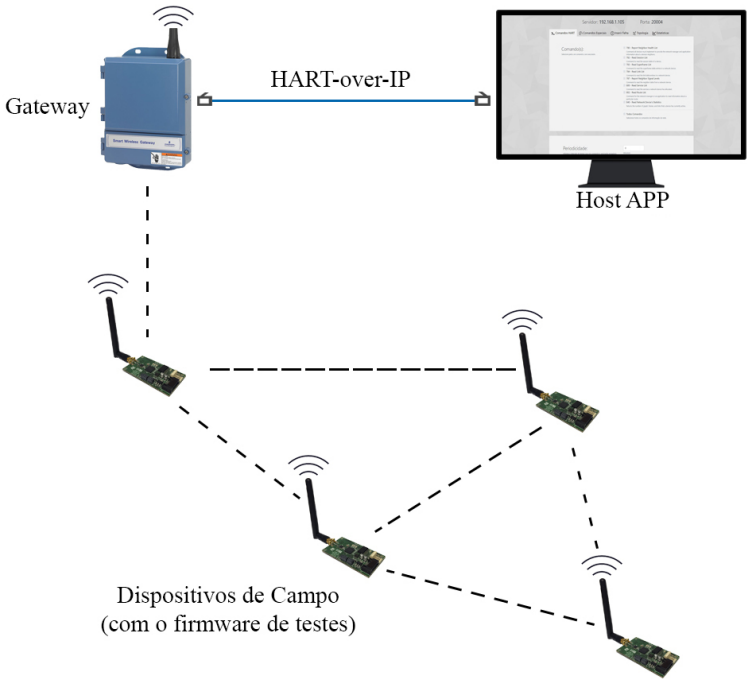
Referências	**Características**		
	Desenvolvimento de ferramenta	Análise da latência	Inserção de falha
(WINTER, 2010)	✓		
(WINTER et al., 2011)	✓		
(SILVA et al., 2011)			✓
(SILVA et al., 2012)		✓	✓
(KUNZEL et al., 2012)	✓	✓	
(KARBASCHI; SAILHAN; ROVEDAKIS, 2012)			✓
(MACHADO et al., 2013)	✓		
(MACHADO et al., 2014)	✓		
(NOBRE; SILVA; GUEDES, 2014)		✓	
(SOTO et al., 2014)	✓	✓	
(SANTOS, 2015)	✓	✓	
(SANTOS et al., 2015)	✓	✓	
(WINTER et al., 2016)			✓
(RAPOSO et al., 2017)	✓		
(HASSAN et al., 2016)	✓		

No esforço de pesquisa bibliográfica, não foram encontrados trabalhos como o aqui proposto, que constitui-se de métodos e uma ferramenta capaz de obter informações de uma RSSFI de forma ampla. O sistema proposto é capaz de obter de forma automática a latência de uma rede WH, revelando os "gargalos" através da observação dos dados obtidos, tanto em funcionamento norma quanto após a injeção de falhas pela própria ferramenta. A proposta é avaliada na forma de três estudos de caso apresentados no Capítulo 6.

4 MÉTODOS E MATERIAIS

Uma visão geral da proposta deste trabalho pode ser obtida pela análise da Figura 3. Ela apresenta os principais componentes que consistem a ferramenta e a descrição detalhada de cada um dos métodos e materiais empregados é apresentado a seguir.

Figura 3: Visão geral da proposta



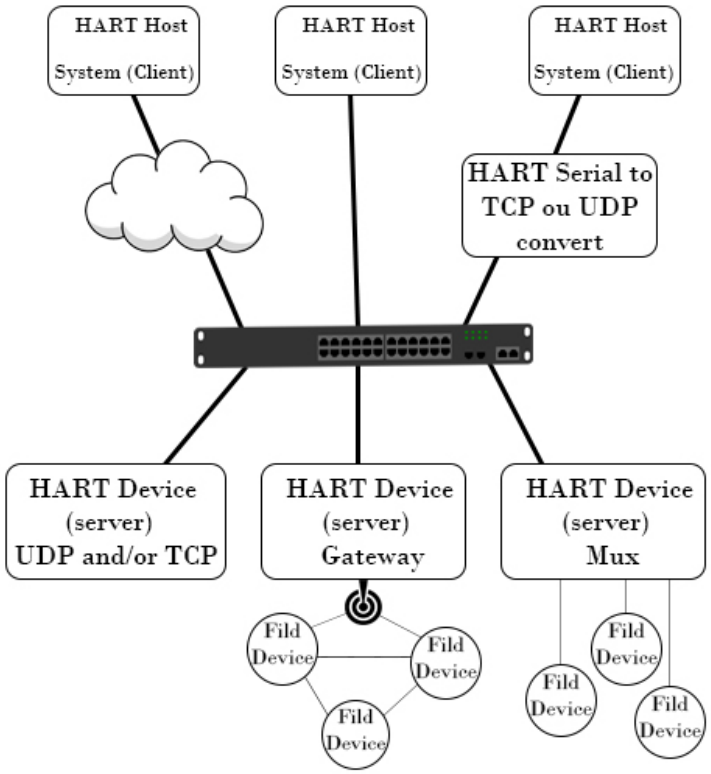
Fonte: Elaborado pelo autor.

A ferramenta foi desenvolvida utilizando a linguagem de programação PHP e C para *back-end* e HTML e CSS para *front-end*. O *front-end* é a parte de interação com o usuário, ou seja, a interface visual da ferramenta. Já o *back-end* é responsável por interpretar os dados informados no *front-end*, encapsulá-los e enviá-los ao *gateway*.

4.1 HART-over-IP

Para efetuar a comunicação entre o *host* e o *gateway* a fim de obter as informações da rede é utilizado o protocolo HART-over-IP. Este protocolo de comunicação suporta tanto o protocolo *Transmission Control Protocol* (TCP) quanto o *User Datagram Protocol* (UDP) em sua implementação (HART COMMUNICATION FOUNDATION, 2011). A arquitetura geral do protocolo HART-over-IP, mostrada na Figura 4, define dois elementos: o servidor HART-over-IP e o cliente.

Figura 4: Topologia de uma rede HART-IP



Fonte: Adaptado de (HART COMMUNICATION FOUNDATION, 2011).

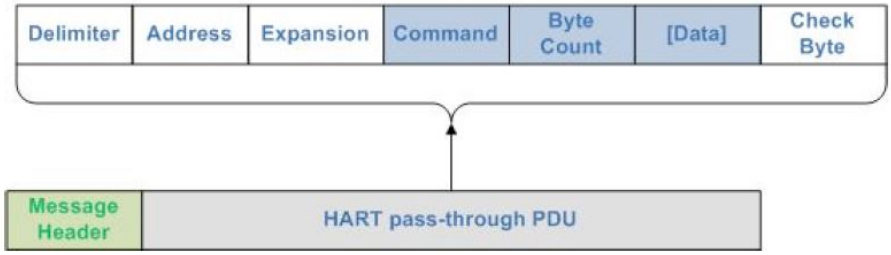
A porta utilizada na comunicação pode ser alterada em função de necessidades específicas da rede, que no caso deste trabalho foi usada a porta 20004, que é a porta que esta configurada no *gateway* usado neste trabalho. O servidor HART-over-IP aguarda comandos HART. Ao receber um pedido HART, a mensagem é processada e retornada para o cliente que fez o pedido. O cliente HART-over-IP permite que uma aplicação se comunique com um dispositivo remoto, o qual requer que todos os dispositivos suportem os comandos universais. O cliente monta uma requisição HART-over-IP com as informações necessárias à aplicação e as envia ao servidor HART-over-IP. Os pedidos podem ser cons-

truídos tanto dentro de pacotes TCP quanto UDP. O servidor deve responder utilizando o mesmo pacote de dados.

O formato básico da mensagem inclui um cabeçalho para descrever o conteúdo da carga útil TCP ou UDP, e uma mensagem padrão de formato de quadro com transmissão de *Token-Passing*. Isso permite que um aplicativo *host*/cliente HART direcione o dispositivo HART diretamente ou faça o servidor encaminhar a mensagem com base no endereçamento para o sub-dispositivo HART apropriado.

No caso específico da rede WH utilizada nesse trabalho, a aplicação cliente HART-over-IP está localizada em um microcomputador fora da rede sem fio enquanto que o servidor HART-over-IP é implementado no *firmware* do *gateway* WH. Assim, por meio da rede *Ethernet*, a aplicação se conecta na porta padrão e coleta os dados necessários dos dispositivos de campo. A especificação dos campos e formatação das mensagens é apresentada nas Figuras 5 e 6.

Figura 5: Formato da mensagem



Fonte: (HART COMMUNICATION FOUNDATION, 2011).

Figura 6: Cabeçalho HART-over-IP

Fonte: (HART COMMUNICATION FOUNDATION, 2011).

4.2 Hardware

Para a validação da ferramenta e do método de análise da confiabilidade fim-a-fim de redes industriais sem fio, foram utilizados os seguintes equipamentos.

- ***Host***

O *host* utilizado é um computador com processador Intel(R) Core(TM) i5 CPU 2.80GHz com 4,0 GB de memória, utilizando um sistema operacional Windows x64. A ferramenta

é desenvolvida para ambiente *web*, com isso, foram utilizadas as linguagens de programação PHP (*Hypertext Preprocessor*), HTML (*HyperText Markup Language*) e CSS (*Cascading Style Sheets*), implementadas em um editor de texto, juntamente com a linguem de programação C, implementada no ambiente de programação Visual Studio 2017. Para a execução da ferramenta é utilizado o servidor Xampp, que é um servidor independente de plataforma, de *software* livre, método utilizado por desenvolvedores a fim de criar um servidor *web* local para fins de teste.

- ***Gateway***

Como *Network Manager*, *gateway* e *access point* da rede, foi utilizado o dispositivo comercial Emerson Wireless 1420A Gateway (EMERSON, 2013), com capacidade de conexão com até 100 dispositivos de campo, configuração automática de rede WH com rotas otimizadas e garantia de confiabilidade de 99,3% (Figura 7). O dispositivo também apresenta uma interface homem-máquina de onde se obteve os dados de *uplink* dos dispositivos da rede. A interface é provida por um servidor Web interno ao *gateway*, do qual são extraídos os dados de *uplink* (dados de latência). Para aplicações de monitoramento de processos industriais, isto é suficiente, pois a rede funciona basicamente como um sistema *convergecast*, onde os dados dos sensores são encaminhados ao *gateway* pela rede em malha. Neste caso, o próprio *gateway* fornece dados da taxa de atualização médias do tempo das comunicações, porém, não coleta os dados, o que a ferramenta proposta faz de forma automática. Ainda, com a inserção de falhas, é possível além da observação normal dos eventos de comunicação, obter informações sobre o desempenho da rede de forma automatizada.

Figura 7: Emerson Wireless 1420A Gateway.

Fonte: Elaborado pelo autor.

- **Dispositivos de campo**

Como dispositivos de campo foram utilizados os rádios elaborados no LASCAR (Figura 8), compatíveis com WH (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 WH. Para a análise da latência das comunicações fim-a-fim dos dispositivos, foi necessária a alteração do *firmware* anteriormente desenvolvido (MULLER, 2012), algo que só foi possível devido ao acesso a pilha do protocolo WH. A ferramenta utilizada para fazer as alterações no *firmware* foi o IDE IAR Embedded Workbench 5.4.

As modificações no firmware permitem a obtenção dos ASN (*Absolute Slot Number*) das mensagens que chegam e que saem do dispositivo, tanto em *uplink* quanto em *downlink*. O ASN é a estampa temporal das mensagens, que revelam a latência dos eventos de comunicação. Além desta alteração, os dispositivos de campo podem receber comandos diretamente do Host APP, que normalmente são restritos ao gerenciador da rede e ao *gateway*. Cabe mencionar também, que, para o funcionamento da ferramenta, não é necessário que todos os dispositivos de campo sejam os proprietários (com *firmware* modificado), ou seja, podem ser utilizados dispositivos comerciais, contanto que não estejam dispostos no final de uma aresta do grafo na rede (o dispositivo proprietário deve estar no final).

Figura 8: Dispositivos de campo.

Fonte: Elaborado pelo autor.

- ***Sniffer***

O instrumento para captura dos sinais de comunicação da rede WH para posterior análise e validação dos métodos e da ferramenta desenvolvidos (Figura 9), é o *sniffer* Wi-Analys (HAN et al., 2009). Trata-se de um dispositivo receptor de RF que captura as mensagens de transmissões da rede WH dentro de seu raio de alcance e salva os *logs*/registros de cada mensagem, que posteriormente foram relacionadas com os dados obtidos pela ferramenta desenvolvida.

Figura 9: *sniffer* - Wi-Analys Network Analyzer.

Fonte: Elaborado pelo autor.

5 IMPLEMENTAÇÃO

Neste capítulo, são apresentadas as implementações realizadas utilizando os métodos e materiais anteriormente descritos.

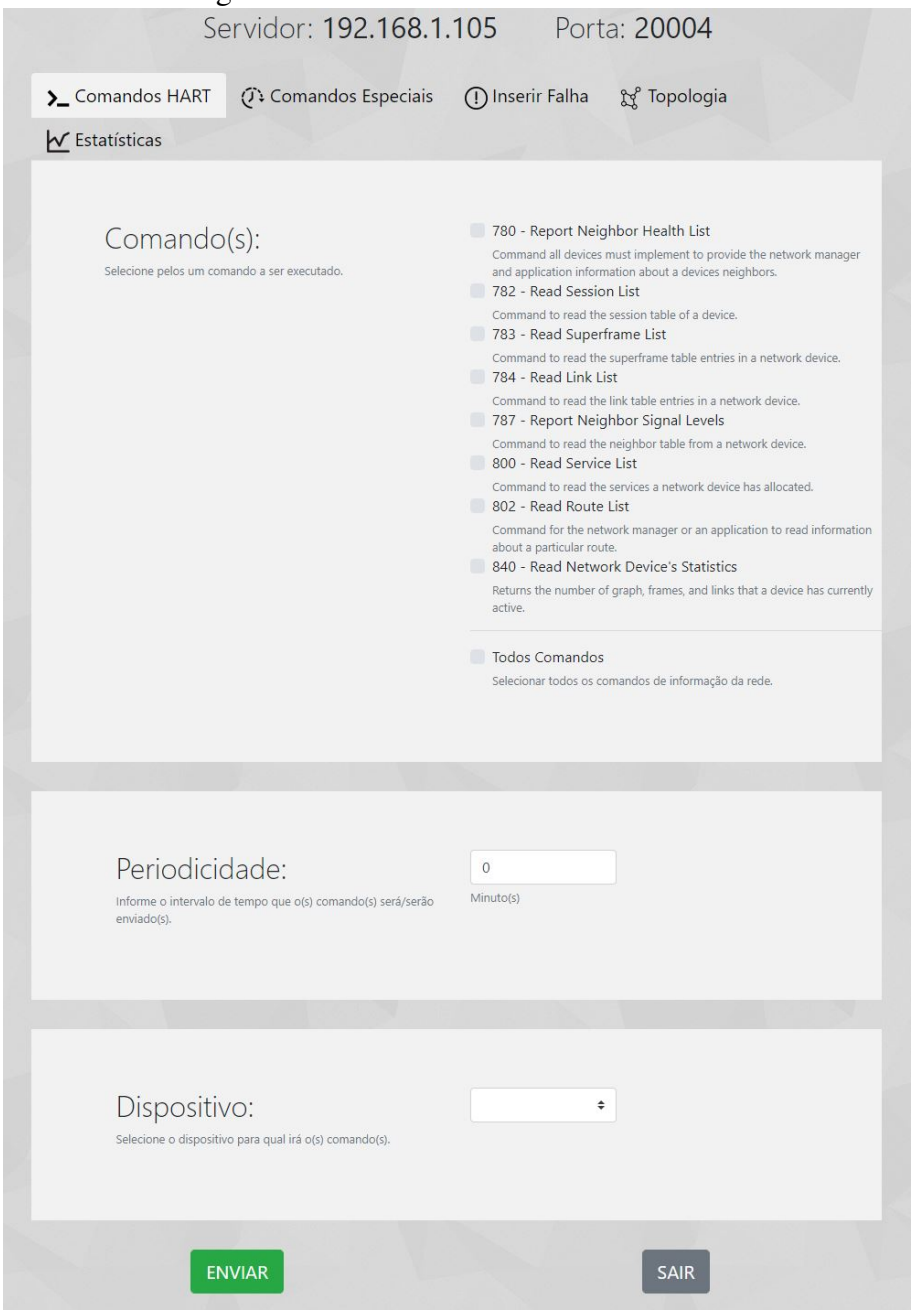
5.1 Ferramenta para Análise e Injeção de Falhas

Utilizando uma rede sem fio WH, a ferramenta desenvolvida utiliza o protocolo HART-over-IP para realizar a comunicação com o *gateway*. O *gateway* por sua vez, comunica-se com os dispositivos na rede por meio do ponto de acesso WH. A aplicação desenvolvida faz uso de comandos HART, implementados para a obtenção dos dados desejados para análise da rede e dos dispositivos. Os comandos HART são encapsulados e enviados para o *gateway*, que responde à requisição, enviando os dados solicitados.

A interface da ferramenta é dividida em cinco abas: a primeira, "Comandos HART" (Figura 10) contém uma relação dos comandos HART implementados de acordo com a norma do WH, comandos estes responsáveis por obter informações tais como: características da rede, quais dispositivos estão na rede e o estado atual deles, topologia da rede, tipos de *links*, grafos de roteamento de mensagens, qualidade do sinal dos enlaces, apelido dos dispositivos, endereço do dispositivo, entre outras informações. Os comandos HART implementados nesta aba são: 780, 782, 783, 784 , 787, 800, 802 e 840. Cujos detalhes estão descritos na seção 5.2.

A Figura 11 apresenta o diagrama de processos que representa a interface dos comandos HART implementados, a utilização de diagramas de processos BPMN (*Business Process Modeling Notation*) foi usada somente para fins de representação e não para geração de código. Os diagramas de processos possuem três raias que representam os elementos da proposta, como eles são e seus fluxos dentro do funcionamento do projeto (BERLI-

Figura 10: Interface dos comandos HART.

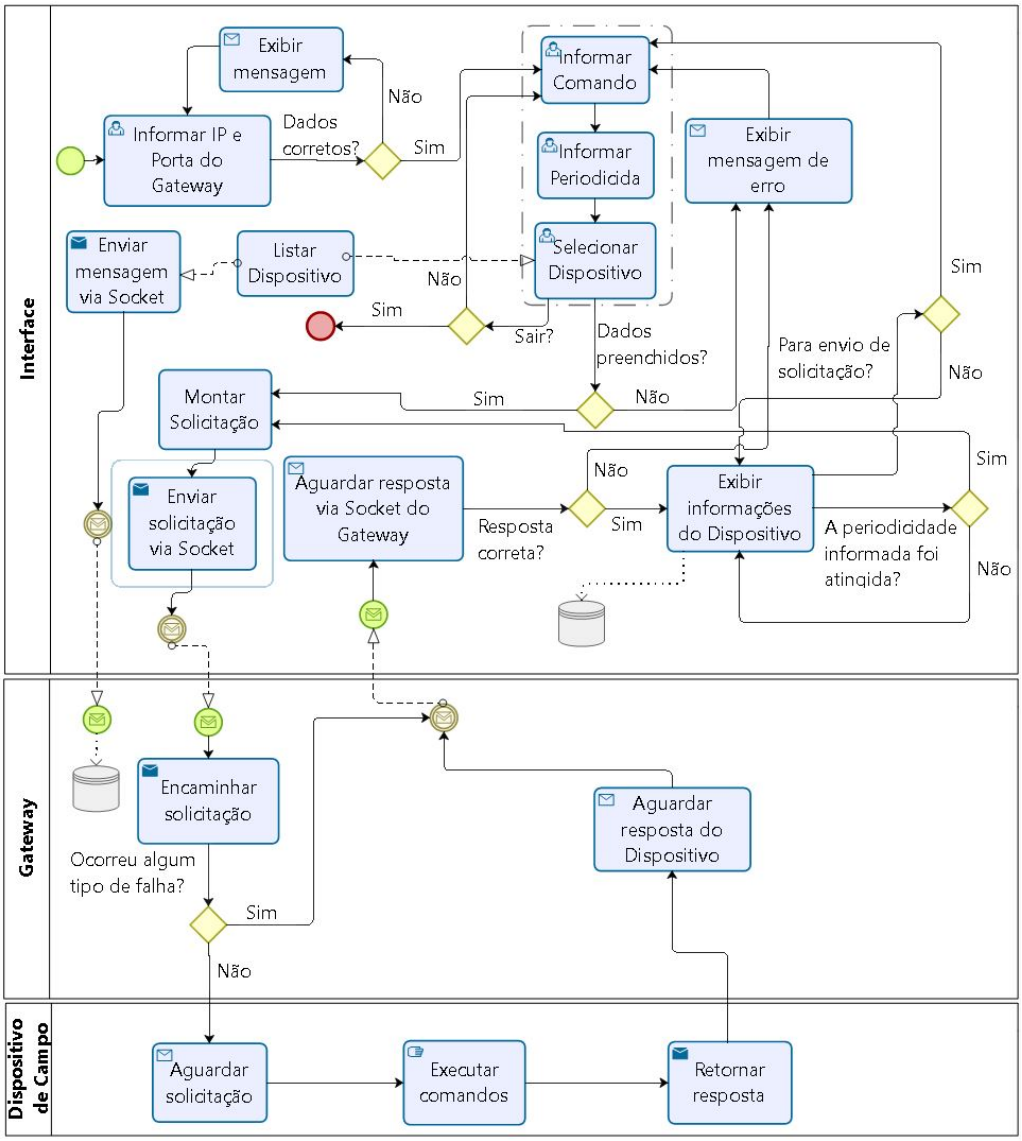


Fonte: Elaborado pelo autor.

NER BPM OFFENSIVE, 2019). Na Figura 11 a raia "Interface"apresenta as ações que a ferramenta realiza de acordo com o que for informado pelo usuário (comandos, periodicidades e o dispositivo alvo), informações estas representadas nos retângulos dentro do retângulo pontilhado. Essas informações são encapsuladas e enviadas via *socket* ao *gateway* da rede, representado na raia "*Gateway*", o *gateway* é responsável então por redirecionar os comandos informados na interface para o dispositivo alvo, representado na raia "Dispositivo de Campo", o disposiviro então recebe o comando, executa e retorna a

resposta ao *gateway*, que por sua vez repassa a resposta para a interface, que interpreta a resposta, armazena a informação e exibe ao usuário.

Figura 11: Diagrama de processos da interface dos comandos HART.

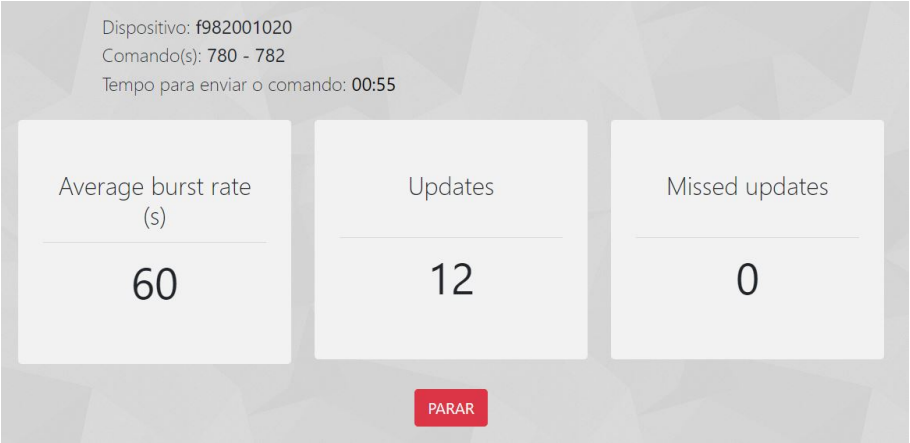


O usuário ao iniciar a aplicação deve informar o endereço IP (*Internet Protocol*) e a Porta do *gateway*, a ferramenta então verifica se o gateway esta ativo e o usuário é então redirecionado para a interface dos comandos HART. Nesta interface, o usuário então escolhe quais comandos serão executados, selecionando para qual dispositivo esses comandos serão enviados, a partir de uma lista de dispositivos que estão ativos na rede. O usuário deve informar ainda, a periodicidade dos comandos selecionados, ou seja, o tempo de espera entre os comandos a serem enviados ao dispositivo selecionado.

O usuário é então redirecionado para uma nova página onde é exibido os dispositivos selecionados, os comandos que serão enviados e um contador do tempo que falta para o

envio dos comandos selecionados. Também são apresentadas informações de taxa média de *burst* (periodicidade de envio de mensagens em *uplink*), atualizações recebidas e atualizações perdidas (Figura 12).

Figura 12: Interface de execução dos comandos HART.



Fonte: Elaborado pelo autor.

A aba "Comandos Especiais", é composta pela implementação dos comandos responsáveis pelo cálculo da latência das comunicações fim-a-fim, além de possuírem outras funcionalidades. Na Figura 13 a raia "Interface"apresenta a opção do usuário selecionar o dispositivo alvo apresentado na Figura 14, para a obtenção da latência da comunicação fim-a-fim com o dispositivo, representado pelo retângulo "Selecionar Dispositivo". A solicitação é então montada e enviada via *socket* ao *gateway* da rede (raia "*Gateway*"), o *gateway* é responsável então por redirecionar a solicitação para o dispositivo alvo (raia "Dispositivo de Campo"), o dispositivo então recebe o comando, executa e retorna a resposta ao *gateway*, que por sua vez repassa a resposta para a interface, que interpreta a resposta, armazena a informação e exibe ao usuário.

O usuário é então redirecionado para uma nova página (Figura 15), que contém as informações de taxa média de *burst*, atualizações recebidas e atualizações perdidas, informações estas obtidas diretamente do *gateway* e ainda são exibidos o *Absolute Slot Number* (ASN) no momento do envio da requisição, o ASN do momento em que o dispositivo recebeu a requisição e a latência do comando (em segundos).

Através dos comandos especiais, é possível ainda a interação com sensores e atuadores, que no caso é uma válvula, sendo possível controlar a abertura da mesma. Desta forma é apresentado um campo para informar o percentual da abertura da válvula e uma barra de progresso informando o estado atual da abertura da válvula.

Figura 13: Diagrama de processos da interface dos comandos especiais.

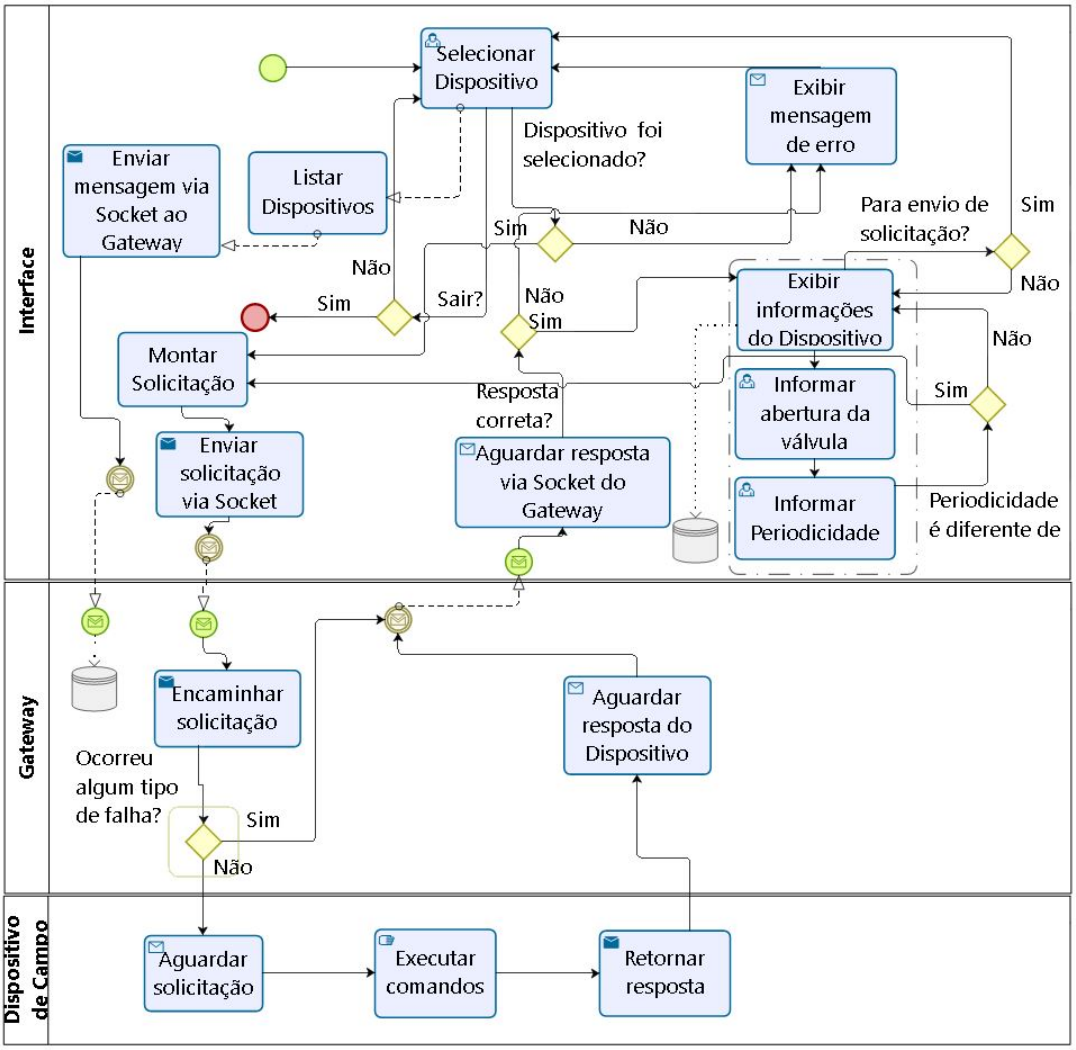
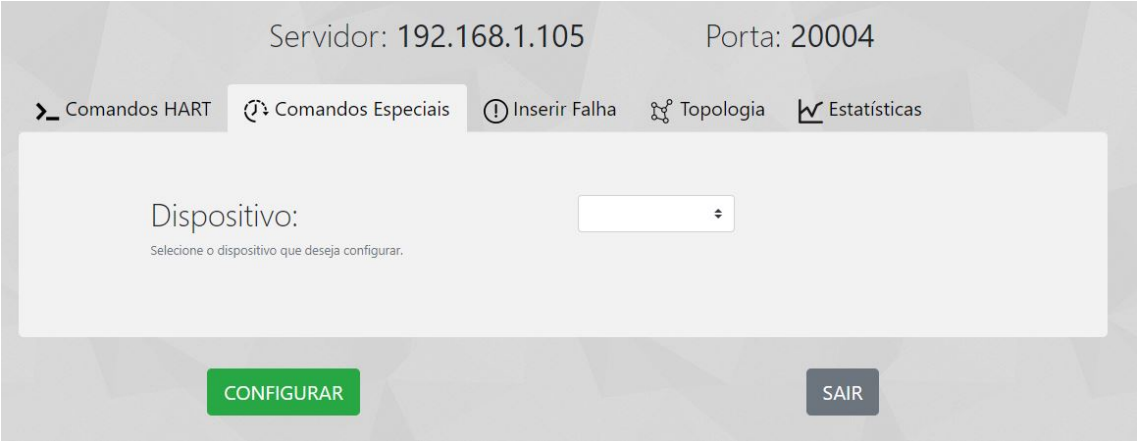
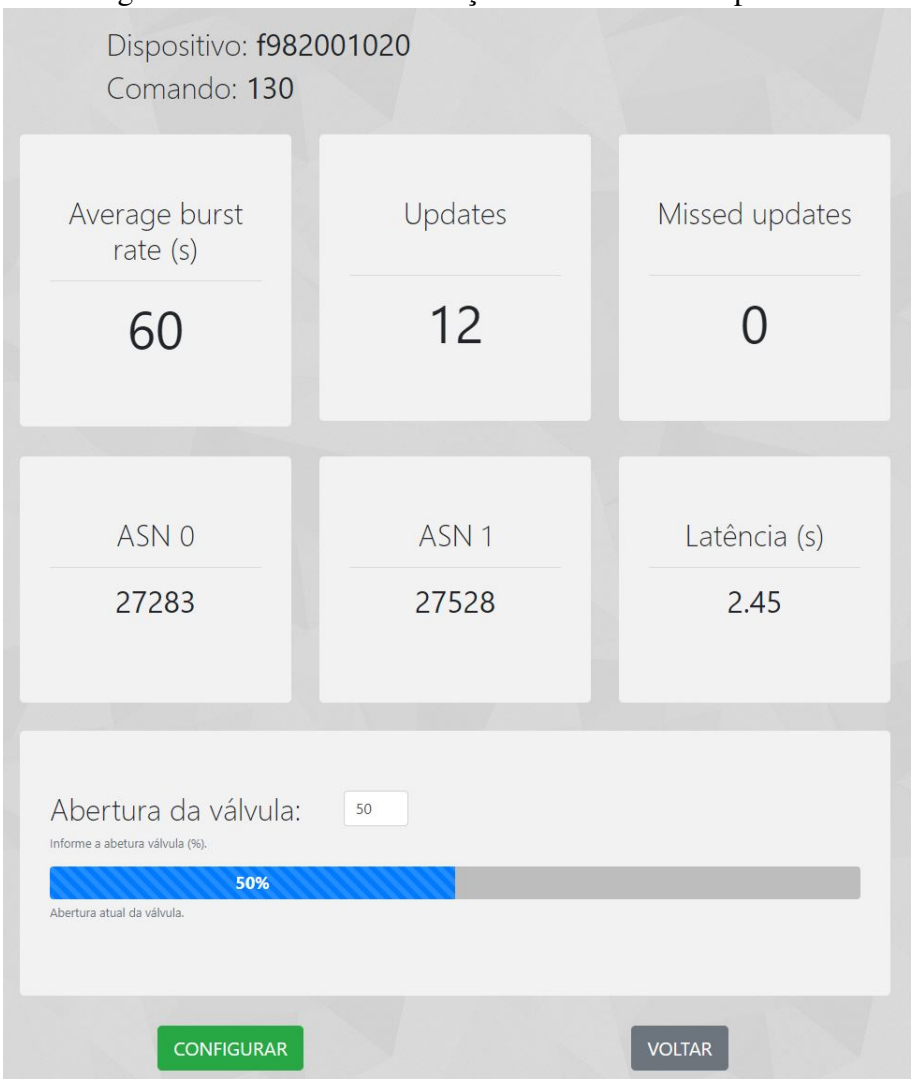


Figura 14: Interface dos comandos especiais.



Fonte: Elaborado pelo autor.

Figura 15: Interface de execução dos comandos especiais.



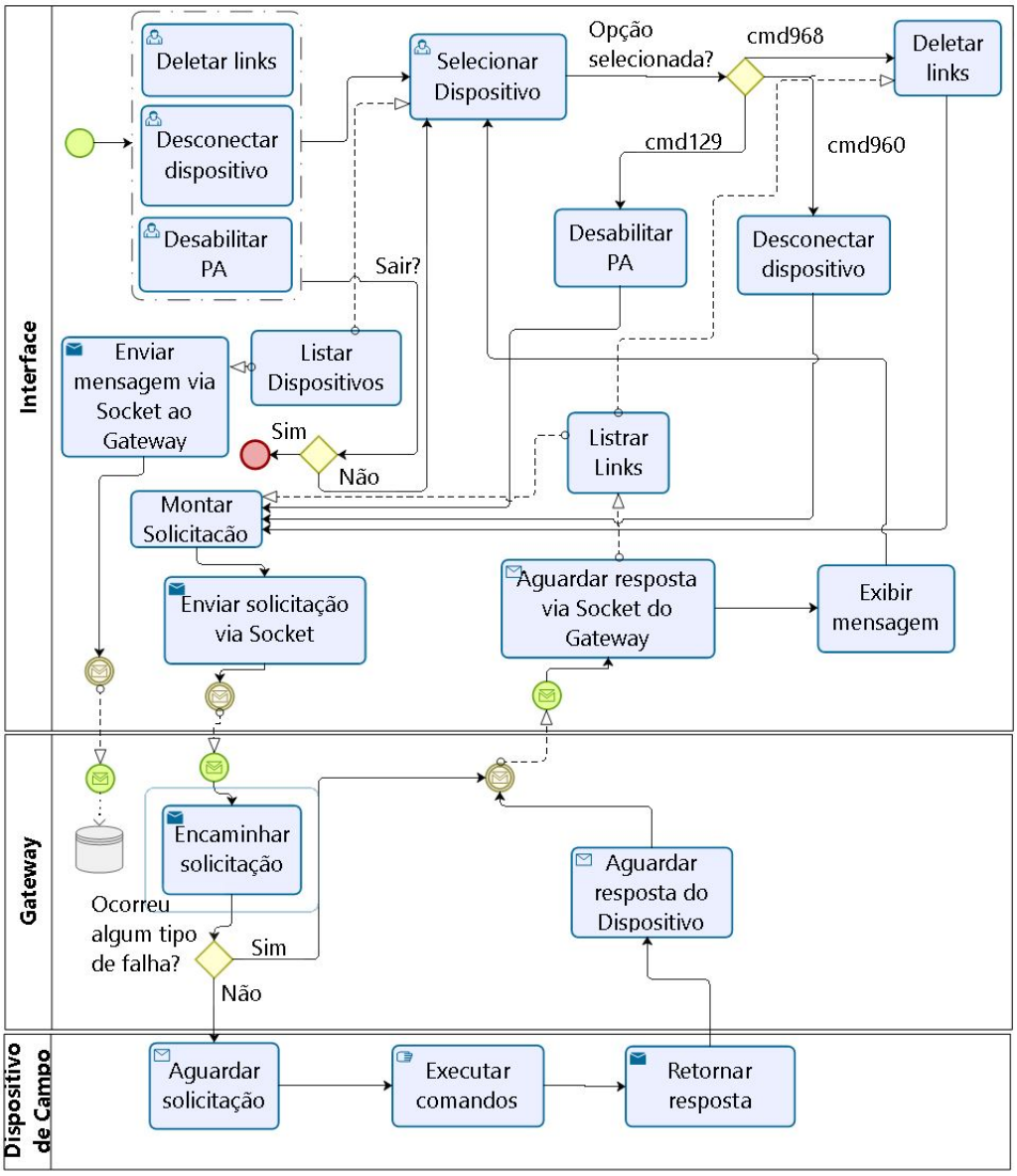
Fonte: Elaborado pelo autor.

A aba "Injeção de Falhas", contém os comandos implementados para inserção de falhas na rede. As falhas implementadas foram elaboradas para refletir situações reais no uso de RSSFI, e neste sentido, podem emular problemas de *hardware*, cuja consequência é a sua desconexão da rede (comando 960), ocorrendo devido a bateria descarregada, mau contato ou antena quebrada. Simular bloqueios de enlaces (comando 968), bloqueios que podem ocorrer quando veículos, como caminhões, ou até mesmo uma pessoa por exemplo, posicionam-se na frente de um dispositivo de campo, interferindo no enlace. Falhas que levam à assimetria do enlace entre dois pares (comando especial 129), esta falha pode ocorrer por dois motivos: por comissionamento inadequado da potência de RF ou por falha no PA (*Power Amplifier*).

A Figura 16 apresenta o diagrama de processos para inserção de falhas na rede, sendo

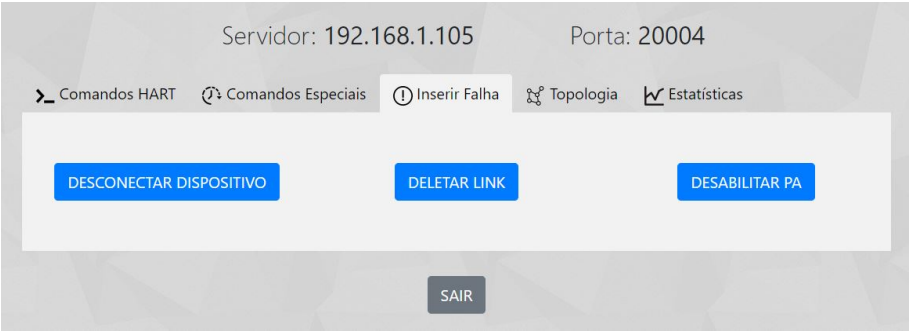
na raia "Interface"apresentado os três tipos de falhas possíveis de serem inseridas na rede pela aplicação, sendo elas representadas pelos retângulos "Deletar Links", "Desconectar Dispositivo"e "Desabilitar PA", o usuário então selecionar qual falha deseja inserir na rede. O comando da falha é então encapsulado e enviado via *socket* ao *gateway* da rede (raia "*Gateway*"), que redireciona a solicitação para o dispositivo que irá conter a falha (raia "Dispositivo de Campo").

Figura 16: Diagrama de processos para a inserção de falhas na rede.



Nesta aba o usuário tem três botões referentes a cada comando (Figura 17), onde ao clicar no botão para desligar um dispositivo, o usuário é redirecionado para uma nova página, que contém os dispositivos ativos na rede (Figura 18). O usuário seleciona um dispositivo que receberá o comando 960, provocando a retirada do dispositivo da rede.

Figura 17: Interface para injeção de falhas na rede.



Fonte: Elaborado pelo autor.

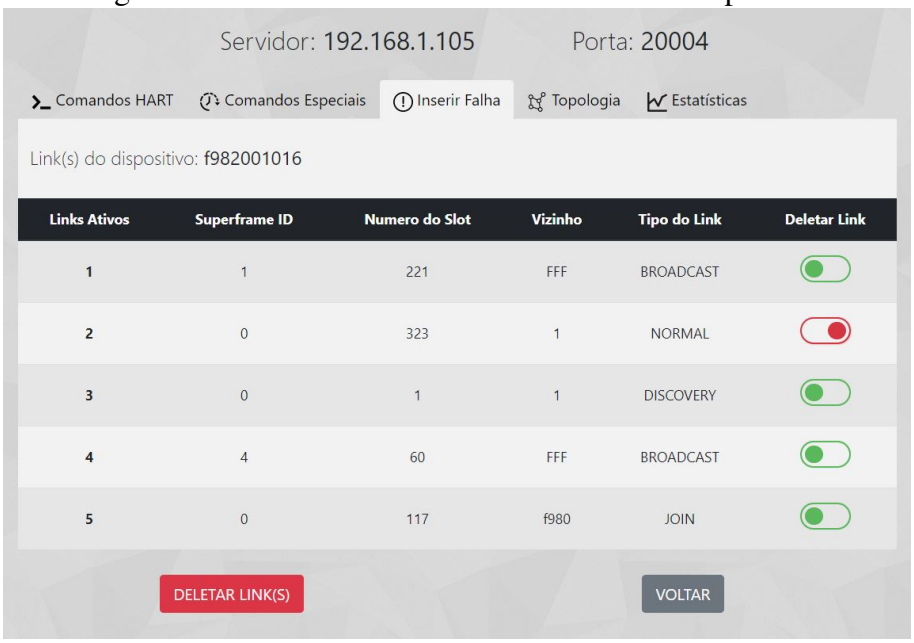
Figura 18: Interface para desconectar dispositivo.

Fonte: Elaborado pelos autor.

Já o botão "Deletar Link", redireciona o usuário para uma página semelhante à de desligar um dispositivo, apresentando os dispositivos ativos na rede, o usuário seleciona um dispositivo, e é lhe apresentado uma tabela (Figura 19) contendo todos os links ativos do dispositivo selecionado (comando 784), com isso, o usuário marca o(s) *link(s)* que ele quer deletar, é então enviado o comando 968 para o dispositivo selecionado, que provoca a exclusão dos *links* selecionados.

Por último, o usuário, ao clicar no botão de desabilitar PA (Power Amplifier), é redirecionado para uma página idêntica a de desligar um dispositivo, o usuário escolhe o dispositivo no qual será desabilitada a potência de transmissão (comando especial 129).

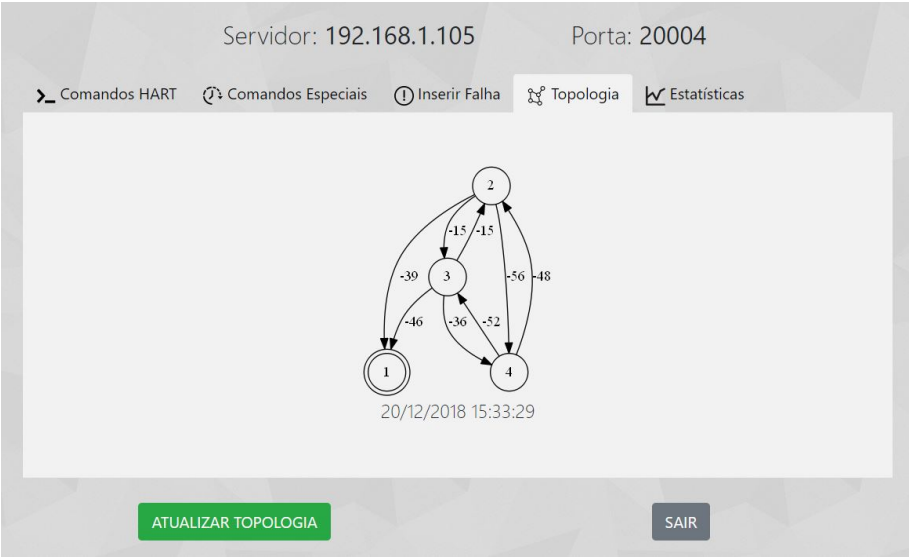
Figura 19: Interface com os *links* ativos de um dispositivo.



Fonte: Elaborado pelos autor.

Na aba "Topologia", é possível gerar uma topologia gráfica da rede (Figura 20). Ao usuário, ao selecionar a aba, é lhe apresentada a topologia na forma de grafo da rede gerada anteriormente, juntamente com a data e hora do momento quem que foi gerada.

Figura 20: Interface para visualização gráfica da topologia da rede.

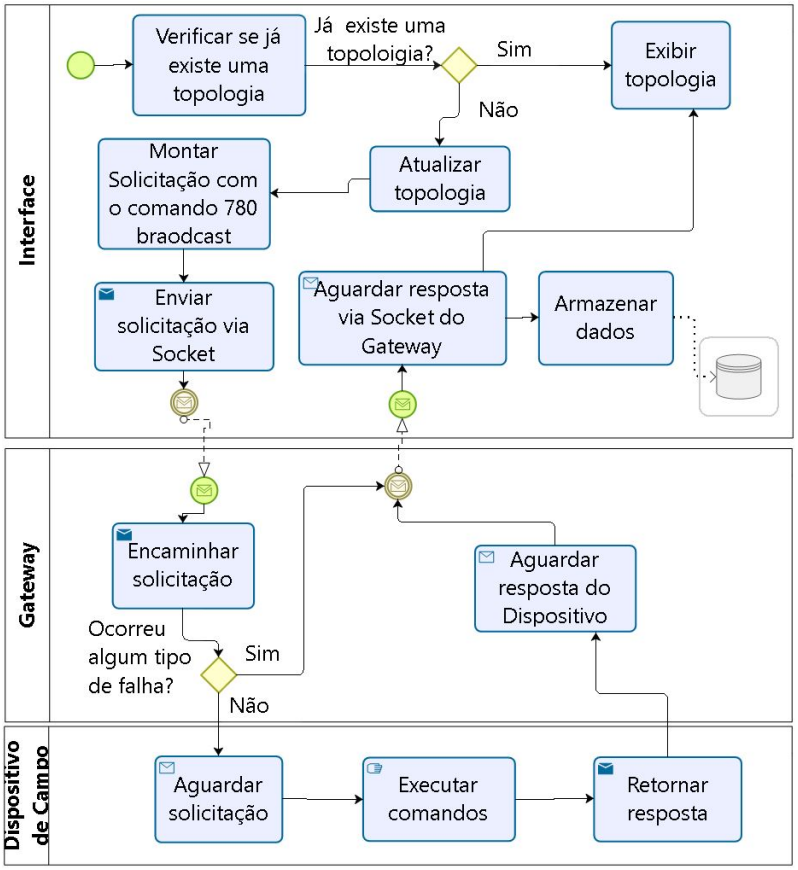


Fonte: Elaborado pelo autor.

A Figura 21 apresenta o diagrama de processos da interface para gerar a topologia da rede, para gerar uma nova topologia o usuário clicar no botão "Atualizar Topologia"da interface, representado pelo retângulo "Atualizar Topologia"do diagrama, é enviado uma

solicitação *broadcast* (comando 780), essa solicitação é encapsulado e enviado via *socket* ao *gateway* (raia "*Gateway*"), que redireciona a solicitação para todos os dispositivos (raia "Dispositivos de Campo") ativos na rede, gerando assim uma lista de todos os dispositivos ativos na rede naquele instante. Essa lista é então armazenada e por meio desta lista é gerada uma imagem com o *software* Graphviz (*Graph Visualization Software*), essa imagem é carregada na interface e apresentada ao usuário. Na imagem é possível visualizar as ligações entre os dispositivos na rede juntamente com o *Received Signal Level* (RSL) de cada ligação.

Figura 21: Diagrama de processos da interface para gerar a topologia da rede.



Na quinta aba "Estatísticas", é apresentada uma tabela com alguns dados da rede, referentes a quantidade e o percentual dos tipos de *links* existentes na rede (Figura 22).

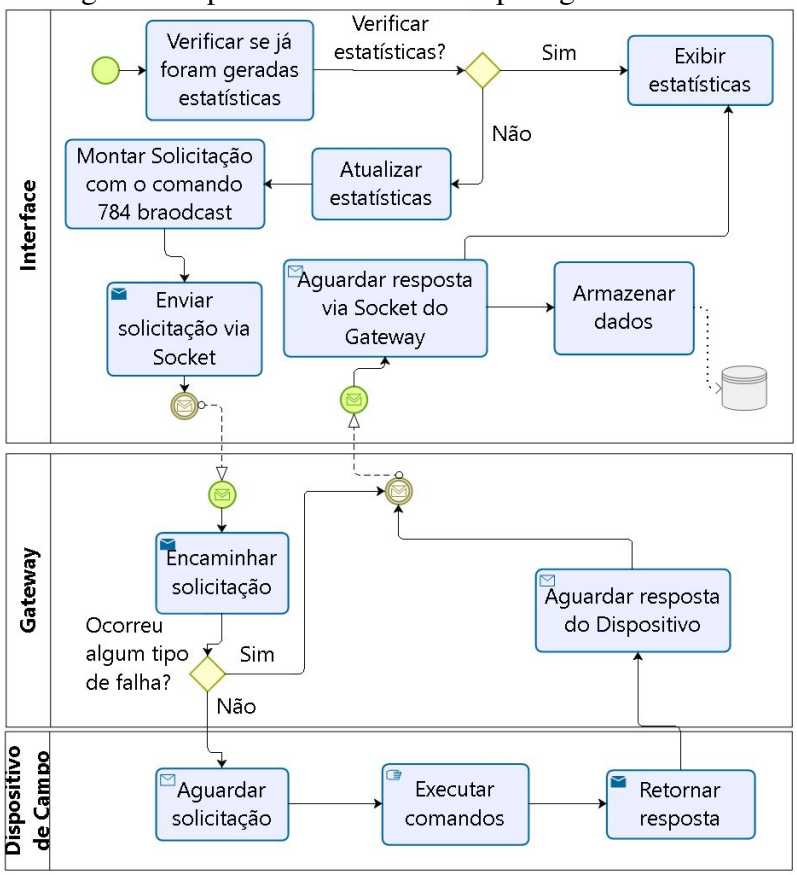
A Figura 23, representa o diagrama de processos da interface para gerar as estatísticas da rede, ao selecionar a aba, são apresentados ao usuário dados estatísticos da rede. Para atualizar esses dados, basta o usuário clicar no botão "Atualizar Estatísticas"da interface, que é representado no retangular "Atualizar Estatísticas"no diagrama. O usuário ao selecionar esta opção é enviado ao *gateway* (raia "Gateway") uma solicitação *broadcast*

do comando 784 aos dispositivos da rede (raia "Dispositivos de Campo"), ativos naquele instante, obtendo assim os *links* de cada dispositivo na rede. Esses dados são então armazenados e carregados na interface.

Figura 22: Interface de estatísticas da rede.

Fonte: Elaborado pelo autor.

Figura 23: Diagrama de processos da interface para gerar as estatísticas da rede.



5.2 Comandos Implementados

Como o protocolo WH é baseado em comandos, a ferramenta também depende de comandos para a obtenção dos dados desejados para análise da rede e dos dispositivos. Os comandos HART são encapsulados no protocolo IP e enviados para o *gateway* que responde à requisição enviando os dados solicitados. A seguir, são apresentados detalhamentos dos comandos implementados.

- **Comando Especial 129**

O comando especial 129 é utilizado para desabilitar o PA de um determinado dispositivo. Este comando foi implementado para poder propiciar uma falha relacionada à perda de potência do rádio, que passa a ter sua transmissão (TX) comprometida.

- **Comando Especial 130**

O comando especial 130 foi implementado para escrita em variáveis de processo de um dispositivo. Este comando é utilizado para obter o ASN das comunicações de um dispositivo, sendo sua utilização descrita com mais detalhes no Capítulo 5.3.

- **Comando Especial 131**

O comando especial 131 tem a finalidade de leitura das variáveis de processo de um dispositivo. Assim como o comando especial 130, foi modificado para obter o ASN obtido pelo comando 130, sendo descrito com maiores detalhes no Capítulo 5.3.

- **Comando 780 - *Report Neighbor Helth List***

O comando 780 retorna dados estatísticos dos vizinhos que possuem *links* de comunicação com um dispositivo. Todos os dispositivos devem ter este comando implementado a fim de fornecer ao gerenciador da rede as informações sobre o estado de saúde da rede (HART COMMUNICATION FOUNDATION, 2008c).

- **Comando 782 - *Read Session List***

Este comando devolve a lista de sessões criadas entre os dispositivos da rede. Através deste comando é possível obter informações sobre as sessões (comunicações confidenciais fim-a-fim) estabelecidas entre os dispositivos e o gerenciador ou *gateway* da rede. Uma sessão permite uma comunicação privada e segura entre um par de endereços na rede (HART COMMUNICATION FOUNDATION, 2008c).

- **Comando 783 - *Read Superframe List***

O comando 783 retorna informações de um *superframe* (conjunto de links gerados pelo gerenciador e programados nos dispositivos de campo) atribuído a um dispositivo. Este comando possibilita obter diferentes cronogramas de comunicação e matrizes de conectividade (HART COMMUNICATION FOUNDATION, 2008c).

- **Comando 784 - *Read Link List***

Os *links* de comunicação estão associados a um dispositivo específico, sendo que para cada *link* há um *slot* alocados para um ou mais dispositivos. Os links estão endereçados pela sua posição na lista de *links* dos dispositivos. Este comando possibilita a leitura desta lista de *links* (HART COMMUNICATION FOUNDATION, 2008c).

- **Comando 787 - *Report Neighbor Signal Levels***

Este comando é periodicamente enviado ao gerenciador de rede, fazendo a leitura da tabela de vizinhos de um determinado dispositivo. Através deste comando é possível indicar novos vizinhos descobertos na rede (HART COMMUNICATION FOUNDATION, 2008c).

- **Comando 800 - *Read Service List***

O comando 800 retorna os serviços solicitados pelos dispositivos de campo e atendidos ou não pelo gerenciador de rede. Tipicamente, os serviços são de publicação periódica de variáveis de processo. Neste trabalho, este comando é utilizado para obter as taxas de publicação (*burst rates*), que retornam os ASN *Snippets*, devido à modificação feita no *firmware* do dispositivo (HART COMMUNICATION FOUNDATION, 2008c).

- **Comando 802 - *Read Route List***

Este comando é utilizada para obter as informações sobre uma rota específica, podendo ela ainda estar ativa ou não. A solicitação deste comando pode ser feita pelo gerenciador da rede ou por uma aplicação (HART COMMUNICATION FOUNDATION, 2008c).

- **Comando 840 - *Read Network Device's Statistics***

Este comando retorna estatísticas dos dispositivos na rede, como o número de grafos, *superframes* e *links* programado no dispositivo (HART COMMUNICATION FOUNDATION, 2008c).

- **Comando 960 - *Disconnect Device***

Esse comando permite que o gerenciador da rede force um dispositivo a se desconectar da rede (HART COMMUNICATION FOUNDATION, 2008c). A desconexão do dispositivo da rede pode emular uma falha de *hardware* do dispositivo, fazendo com que o dispositivo tenha que se desconectar da rede. Melhor descrito no Capítulo 6.2

- **Comando 968 - *Delete Link***

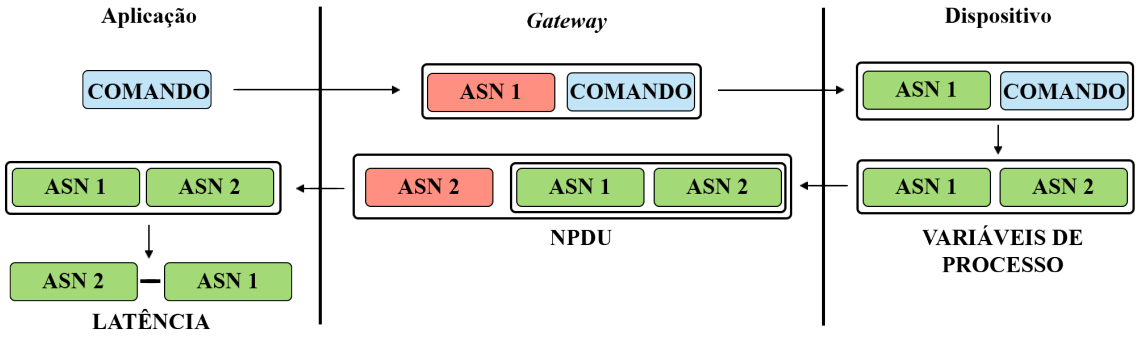
Este comando permite que o gerenciador exclua uma atribuição de *link* de um dispositivo da rede (HART COMMUNICATION FOUNDATION, 2008c). A exclusão de um *link* de comunicação do dispositivo simula uma falha de obstrução de uma rota de comunicação entre dispositivos. A implementação deste comando é melhor explicada no Capítulo 6.3.

5.3 Estratégia de Análise da Latência

Para calcular a latência das comunicações fim-a-fim da rede foram implementados dois comandos, um de escrita (comando 130) e um de leitura (comando 131) das variáveis de processo, fazendo uso da variável ASN *Snippet*, referente aos dois *bytes* menos significativos do ASN, que faz parte do *Network Protocol Data Unit* (NPDU). Porém, por ser uma variável restrita em segmentos da rede (sem acesso pelo usuário), optou-se por fazer alterações no *firmware* dos dispositivos com o propósito de extração do ASN *Snippet*. Quando a ferramenta se comunica com o *gateway*, que por sua vez comunica-se com um dispositivo através do ponto de acesso, cria-se um ASN que está no cabeçalho do NPDU. Com a alteração do *firmware* realizada no dispositivo, o pacote recebido pelo dispositivo passa pelas camadas física e de enlace, chegando à camada de rede, onde é obtido os ASNs presente no cabeçalho do NPDU no momento em que o *gateway* criou

o pacote, e o ASN do momento em que o dispositivo recebeu o pacote, esses ASNs são armazenados, e retornados para a aplicação através das variáveis de processo. Essas variáveis são encaminhadas ao *gateway*, como uma variável de processo, através de outra modificação no *firmware* (mudança das variáveis de processo). Uma vez que o *timeslot* possui um tempo fixo de 10 ms, é calculada a diferença entre os valores dos ASNs, obtendo-se então uma relação direta com a latência fim-a-fim da comunicação entre os dispositivos. A ferramenta, ao ter acesso a essas variáveis, pode calcular a latência das comunicações fim-a-fim da rede, como ilustrado na Figura 24.

Figura 24: Método para determinar a latência

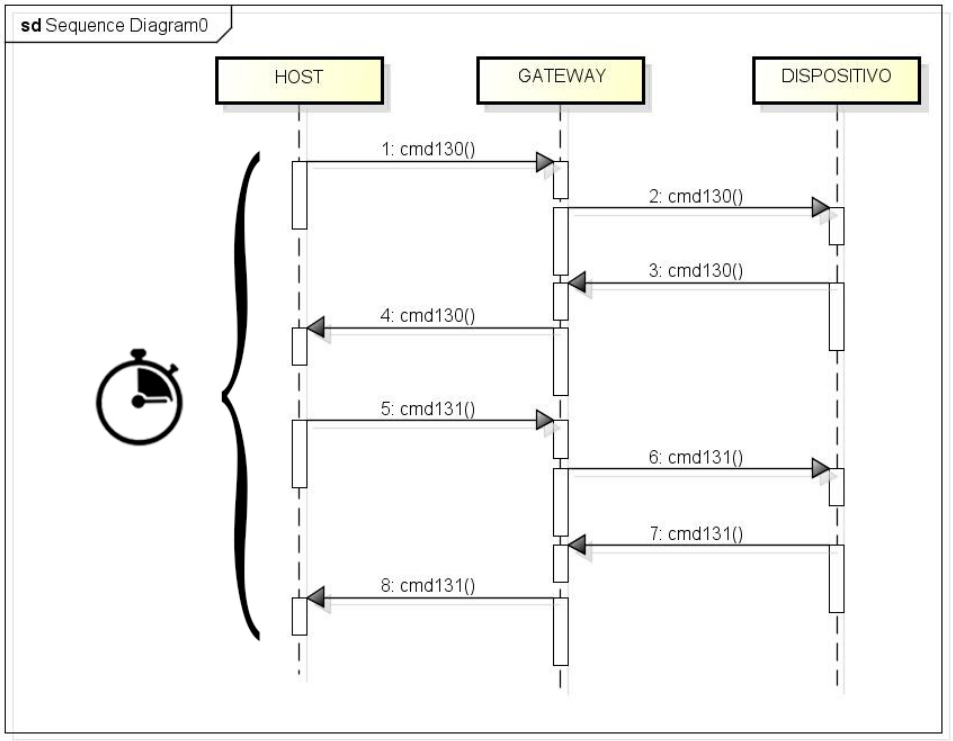


Fonte: Elaborado pelo autor.

Como estudos de caso para a validação deste trabalho, tem-se como cenários possíveis, a partir de redes WH reais, o monitoramento de um dispositivo por meio do levantamento periódico da topologia e da latência da rede (Figura 25). Realizado o monitoramento, é então inserida uma falha na rede através da ferramenta desenvolvida, por exemplo, interrompendo uma rota pela qual o dispositivo se comunicava normalmente, avaliando a nova topologia da rede, juntamente com o impacto na latência ocasionada pela falha e o tempo para a rede normalizar.

Com isto, a ferramenta fornece dados relevantes para a verificação da aplicabilidade da rede em NCS, por exemplo, fornecendo o pior valor de latência. De outra forma, a ferramenta pode ser utilizada como um sistema de *site survey* para avaliação prévia de uma rede a ser instalada numa planta, revelando latência máximas, "gargalos", qualidades dos enlaces, todos obtidos de forma automática. Eventos tais como falhas de *hardware* e bloqueios são emulados e revelam o que se pode esperar de uma instalação definitiva. Diversas decisões podem ser tomadas de antemão, com o intuito de produzir um mapa de localização de dispositivos definitivos, tendo em conta a localização de repetidores.

Figura 25: Ciclo para obtenção da latência



Fonte: Elaborado pelo autor.

Uma vez avaliado o local de uso definitivo, a rede de testes é retirada e substituída pelos dispositivos comerciais, de elevado valor econômico.

6 ESTUDOS DE CASO

Para a validação da proposta desta dissertação, foram realizados três estudos de caso que simulam falhas reais que ocorrem em ambientes de redes industriais sem fio, nos quais todos os estudos seguem um padrão para a sua realização. Para a realização dos estudos de caso, o *sniffer* Wi-Analys foi utilizado para a coleta de dados e posterior comparação com os dados obtidos pela ferramenta. A coleta de dados das comunicações fim-a-fim entre os dispositivos é feita em média por uma hora de duração, ao iniciar o teste até a inserção da falha e de mais uma hora após a inserção da falha. Os dados de latência são coletados a cada 60 segundos, tendo assim produzidas uma média de 120 amostras em cada estudo de caso.

A topologia da rede é montada de forma que pelo menos um dispositivo não esteja ao alcance de comunicação direta com o *gateway*, forçando a criação de uma topologia que tenha pelo menos um dispositivo repetidor intermediário nas comunicações com o dispositivo alvo. Os dados de latência são sempre obtidos em função do dispositivo que não tem comunicação direta com o *gateway*, e a falha inserida em um dispositivo intermediário, para que possa ser feita a análise das comunicações fim-a-fim do dispositivo.

6.1 Validação da ferramenta

Para a validação da ferramenta com relação à obtenção da latência das comunicações fim-a-fim entre os dispositivos, foi utilizado o ASN *Snippet* para a realização do cálculo, o ASN *Snippet* é o valor de tempo limite da camada de rede com tamanho de dois *bytes* que é calculado com base em uma parte do ASN. Foram realizadas diversas comunicações utilizando a ferramenta, e os dados das comunicações foram armazenados e comparados com os dados dos *logs* do *sniffer*. Nas Tabelas 2 e 3 são apresentados os dados das trocas

de três ciclos da comunicação entre dois dispositivos, sendo enviados o comando especial 130 para escrita nas variáveis de processo do *gateway* (dispositivo Tag 1) para o Tag 1019, e posteriormente enviado o comando especial 131 para fazer a leitura das variáveis de processo.

Tabela 2: Dados da latência obtidos pela ferramenta.

Índice	**Hora**	**Comando**	**Origem**	**ASN Origem**	**Destino**	**ASN Destino**
1	08:22:00	130	1	57149	1019	57184
2	08:22:53	130	1	61936	1019	62047
3	08:23:38	130	1	1700	1019	1887

Tabela 3: Dados da latência obtidos pelo *sniffer*.

Índice	**Hora**	**Comando**	**Origem**	**Destino**	**ASN**
1	08:21:47	130	1	1011	57149
1	08:21:47	130	1011	1019	57149
1	08:21:49	130	1019	1008	57184
1	08:21:50	130	1008	1	57184
2	08:22:35	130	1	1011	61936
2	08:22:35	130	1011	1019	61936
2	08:22:37	130	1019	1008	62047
2	08:22:39	130	1008	1	62047
3	08:23:29	130	1	1011	1700
3	08:23:29	130	1011	1019	1700
3	08:23:31	130	1019	1008	1887
3	08:23:33	130	1008	1	1887

Analisando a Tabela 3, com os dados coletados pela ferramenta juntamente com os dados coletados pelo *sniffer* é possível identificar que, na primeira troca de mensagem (Índice = 1), o *gateway*, ao receber (Origem 1) a solicitação do *host*, de envio do comando especial 130, gera o ASN no *timeslot* 57149. O comando é então enviado, passando pelo dispositivo Tag 1011, e, o dispositivo Tag 1019 ao receber a mensagem gera o ASN no *timeslot* 57184. Os valores de ASN são armazenados em variáveis de processo que serão retornadas para a ferramenta através do comando 131, e então é calculada a latência da comunicação em segundos. Sucedendo-se assim este procedimento.

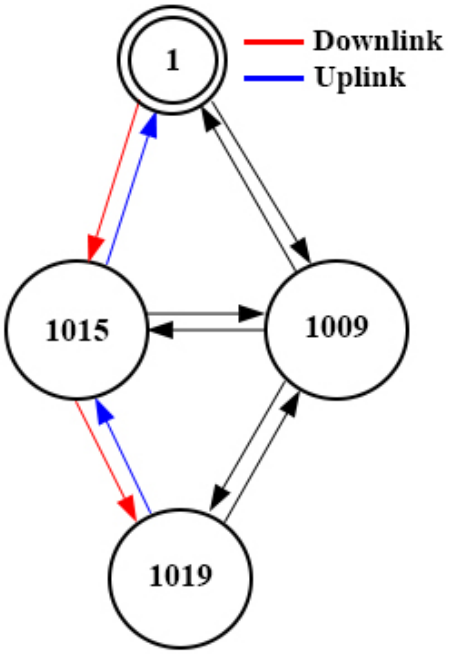
Comparando-se os dados das Tabelas 2 e 3, é possível afirmar que a ferramenta é capaz de obter a latência fim-a-fim das comunicações entre os dispositivos, sem a necessidade

da utilização de um terceiro equipamento (um *sniffer* 802.15.4 multicanais), desta forma, comprovando-se a utilização da ferramenta para posterior análise de latência nos estudos de caso.

6.2 Estudo de Caso 1: desconectando um dispositivo da rede

Para o estudo de caso 1, foi implementado o comando 960 (*Disconnect Device*). Este estudo de caso emula uma falha no dispositivo, cuja consequência é a sua desconexão da rede. Esta falha simula uma falha real, que pode ocorrer devido a um problema de *hardware*, bateria descarregada, mau contato ou antena quebrada. Neste estudo de caso, avaliou-se a latência fim-a-fim entre os dispositivo Tag 1 e Tag 1019. A Figura 26 apresenta a topologia da rede destacando-se as rotas de comunicação com o dispositivo alvo e sendo o *gateway* representado pela Tag "1".

Figura 26: Topologia da rede do estudo de caso 1 antes da inserção da falha.



Fonte: Elaborado pelo autor.

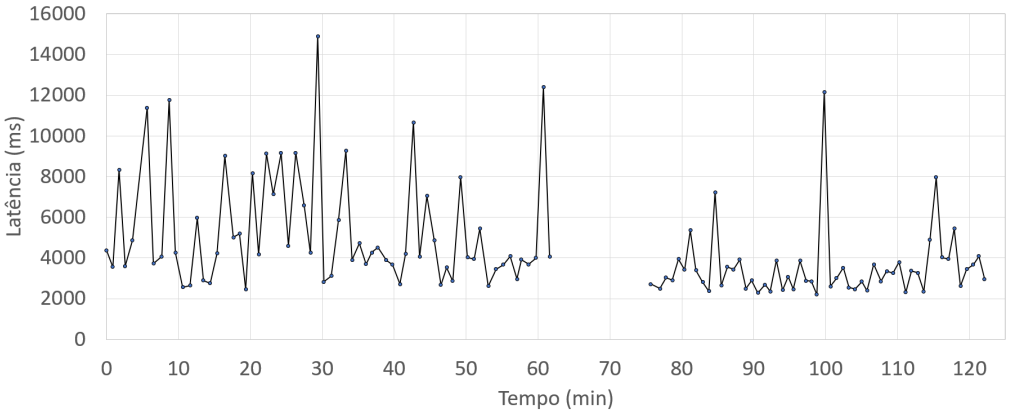
As 09:58 são enviados os comando especiais 130 e 131 periodicamente para obtenção da latência fim-a-fim da comunicação com o dispositivo Tag 1019. Após o período estipulado de aproximadamente uma hora tem-se uma média de 55 comunicações com o dispositivo, cujos valores de latência são apresentados na Tabela 4, tendo uma variação da latência de 12,44 segundos.

Tabela 4: Dados da latência em segundos antes da inserção da falha.

	Latência
Mínima	2,46
Máxima	14,9
Média	4,25

Às 11:00 é inserida uma falha na rede, referente a desconexão do dispositivo Tag 1015 (comando 960). A Figura 27 apresenta o diagrama temporal do estudo de caso, denotando o período transcorrido entre a operação normal e a inserção da falha.

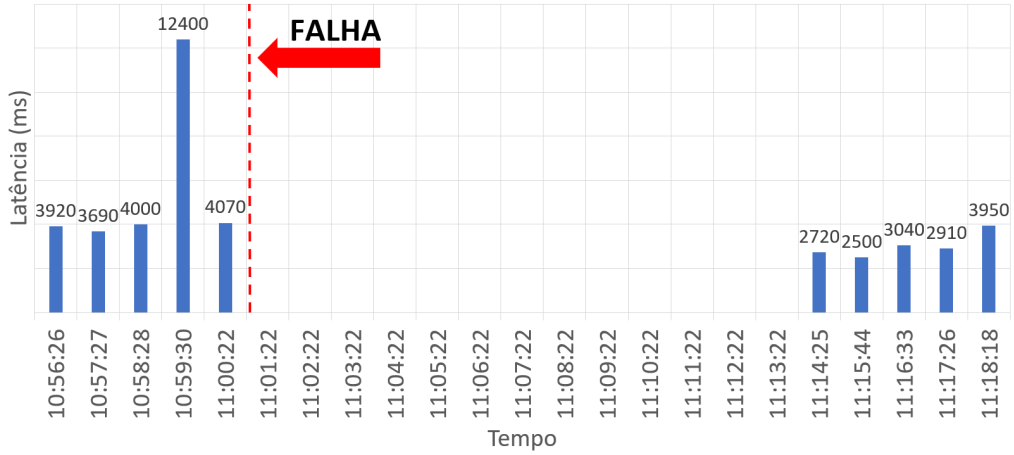
Figura 27: Linha do tempo completa do estudo de caso 1.



Fonte: Elaborado pelo autor.

A Figura 28 apresenta o diagrama temporal do estudo de caso, no momento da inserção da falha até a retomada da aquisição da latência com o dispositivo Tag 1019.

Figura 28: Linha do tempo do instante da inserção da falha do estudo de caso 1.



Fonte: Elaborado pelo autor.

Novamente, após aproximadamente mais uma hora, foram coletadas mais 64 comuni-

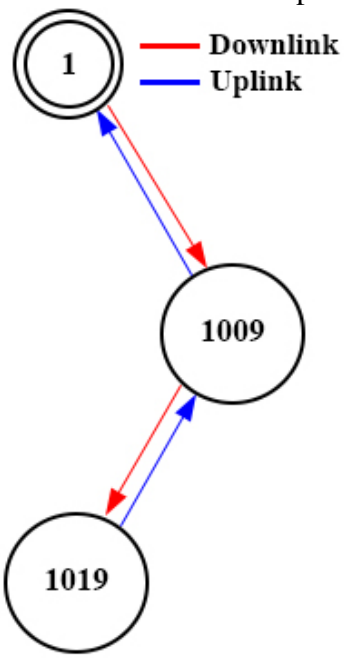
cações, das quais o dispositivo Tag 1019 somente voltou a responder às 11:14. A inserção da falha resultou em uma nova latência, apresentada na Tabela 5, com uma variação da latência de 9,95 segundos.

Tabela 5: Dados da latência em segundos após a inserção da falha.

	Latência (s)
Mínima	2,20
Máxima	12,15
Média	3,26

Com a desconexão do dispositivo, é observada uma alteração na topologia da rede (Figura 29). Alterando-se assim a rota de comunicação com o dispositivo Tag 1019.

Figura 29: Topologia da rede do estudo de caso 1 após a inserção da falha.

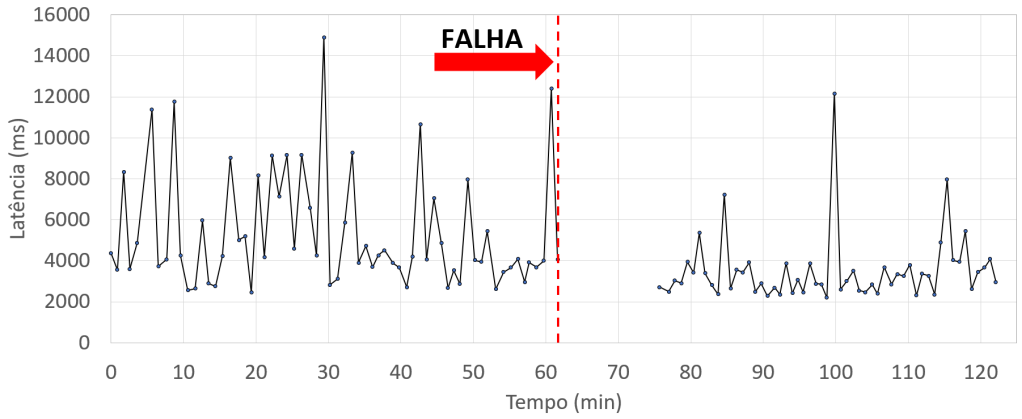


Fonte: Elaborado pelo autor.

Feita a coleta dos dados, obteve-se um total de 119 comunicações, tendo uma variação média de 12,7 segundos das comunicações (Figura 30).

Com os dados coletados pela ferramenta e conferidos com os dados do *sniffer* (Tabela 6), foi possível constatar que no estudo de caso 1 o dispositivo Tag 1019 demorou aproximadamente 14 minutos para encontrar uma nova rota e voltar a responder as solicitações (Figura 28). Após restabelecer as comunicações com o dispositivo Tag 1019, observou-se que houve uma melhora na latência das comunicações fim-a-fim entre os dispositivos,

Figura 30: Variação da latência durante o estudo de caso 1.



Fonte: Elaborado pelo autor.

com a mudança na topologia da rede. Sendo possível observar que não necessariamente a topologia da rede é formada visando uma menor latência nas comunicações entre os dispositivos.

Tabela 6: Dados coletados pelo *sniffer* Wi-Analys durante o período do estudo de caso 1.

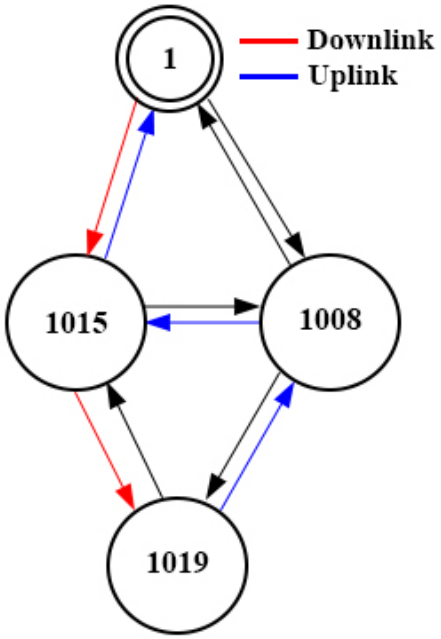
Hora	**Origem**	**Destino**	**Dados**	**Rota**
09:59:20	1	1015	cmd130	*downlink*
09:59:23	1015	1019	cmd130	*downlink*
09:59:24	1015	1019	ACK	*uplink*
09:59:25	1015	1	cmd130	*uplink*
09:59:25	1	1015	cmd131	*downlink*
09:59:28	1015	1019	cmd131	*downlink*
09:59:30	1019	1015	cmd131	*uplink*
09:59:36	1015	1	cmd131	*uplink*
...	...	...	...	...
11:00:39	1	1015	cmd960	*downlink*
11:00:39	1015	1011	cmd960	*uplink*
11:00:42	1011	1	cmd930	*uplink*
...	...	...	...	...
11:14:11	1	1009	cmd130	*downlink*
11:14:13	1009	1019	cmd130	*downlink*
11:14:15	1019	1009	cmd130	*uplink*
11:14:15	1009	1	cmd130	*uplink*
11:14:18	1	1009	cmd131	*downlink*
11:14:20	1009	1019	cmd131	*downlink*
11:14:25	1009	1019	ACK	*uplink*
11:14:25	1009	1	cmd131	*uplink*
...	...	...	...	...
12:00:50	1009	1	cmd131	*uplink*

A Tabela 6 demonstra que em algumas comunicações durante o estudo de caso, foram registrados o ACK de um dispositivo para o outro, o que ocorreu devido ao posicionamento do *sniffer* no momento da realização do estudo de caso, visto que o *sniffer* captura as transmissões da rede WH dentro do seu raio de alcance. Isto não invalidando o estudo, dado que não foi registrado o envio da mensagem, mas sim a resposta de recebimento pelo dispositivo vizinho, e comparados com os dados obtidos pela ferramenta. Fato este corrigido para os demais estudos de caso.

6.3 Estudo de Caso 2: deletando *links* de comunicações de um dispositivo

No estudo de caso 2, foi utilizado o comando 968 (*Delete Link*). Neste estudo de caso, são escolhidos *links* entre dispositivos para que sejam deletados pela ferramenta, para simular bloqueios de enlaces. Em plantas industriais de grande porte, tais como refinarias, estações de tratamento de água ou plantas químicas, os bloqueios podem ocorrer quando veículos, como caminhões, por exemplo, posicionam-se na frente de um dispositivo de campo, interferindo no enlace. Os links podem ser excluídos e posteriormente restabelecidos, para que se possa avaliar a latência nas comunicações bem como as modificações na topologia de rede em malha.

Figura 31: Topologia da rede do estudo de caso 2 antes a inserção da falha.



Fonte: Elaborado pelo autor.

Dada a topologia da rede (Figura 31), é iniciado o estudo às 06:28, enviado os comandos especiais para obtenção da latência fim-a-fim da comunicação com o dispositivo Tag 1019, e enviado o comando 784 para obter os *links* de comunicação do dispositivo Tag 1015.

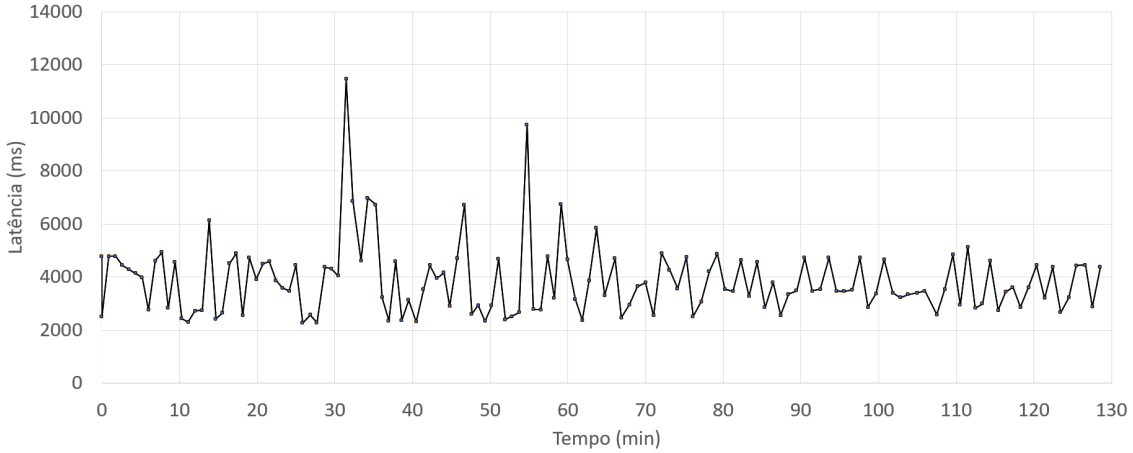
Após o período estipulado de aproximadamente uma hora, tem-se uma média de 75 comunicações com o dispositivo antes da inserção da falha na rede, com uma variação da latência de 9,19 segundos, apresentados na Tabela 7.

Tabela 7: Dados da latência em segundo antes da inserção da falha.

	Latência (s)
Mínimo	2,27
Máximo	11,46
Média	3,92

Às 07:34 é enviado o comando 968 para deletar os *links* de comunicação do dispositivo Tag 1015 com o dispositivo Tag 1019, inserindo assim uma falha na rede. A Figura 32 apresenta o diagrama temporal do estudo de caso, denotando o período completo do estudo de caso.

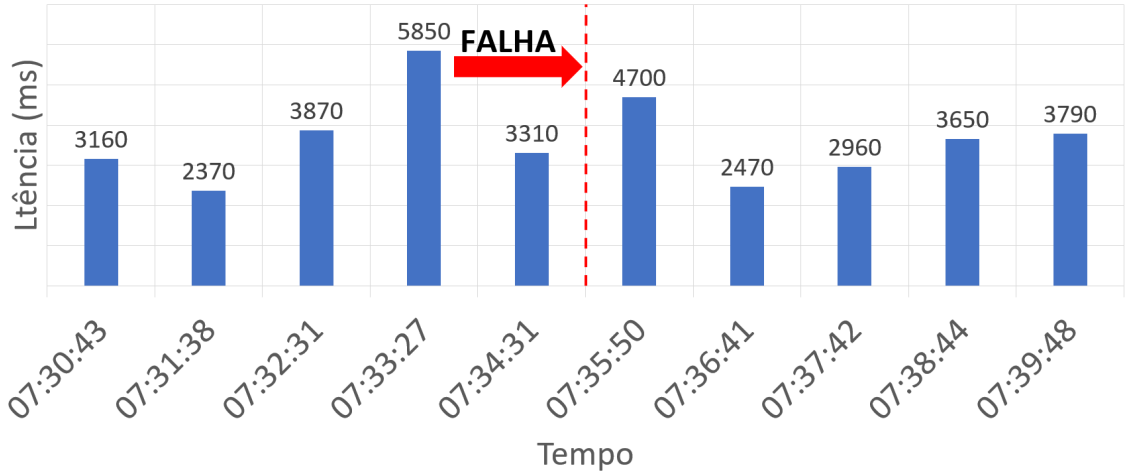
Figura 32: Linha do tempo completa do estudo de caso 2.



Fonte: Elaborado pelo autor.

A Figura 33 apresenta o diagrama temporal, do período transcorrido entre a inserção da falha e a retomada da operação normal.

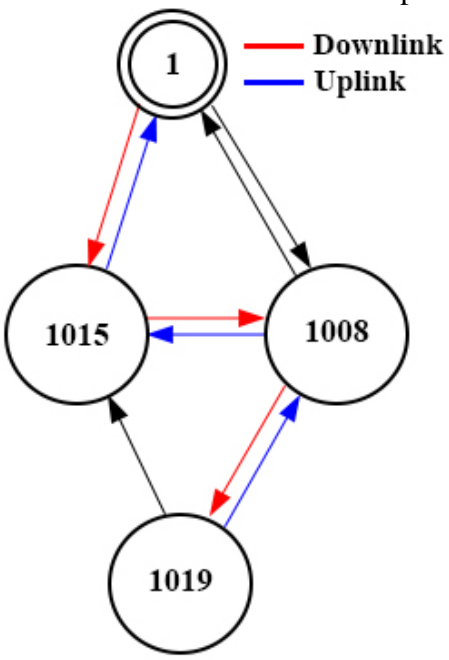
Figura 33: Linha do tempo do instante da inserção da falha do estudo de caso 2.



Fonte: Elaborado pelo autor.

Como consequência da falha, o gerenciador gerou uma nova rota de comunicação com o dispositivo Tag 1019 (Figura 34). Transcorrido aproximadamente mais uma hora, às 08:37, o estudo foi pausado e obtidos mais 62 comunicações com o dispositivo Tag 1019, gerando uma nova latência, apresentada na Tabela 8.

Figura 34: Topologia da rede do estudo de caso 2 após a inserção da falha.



Fonte: Elaborado pelo autor.

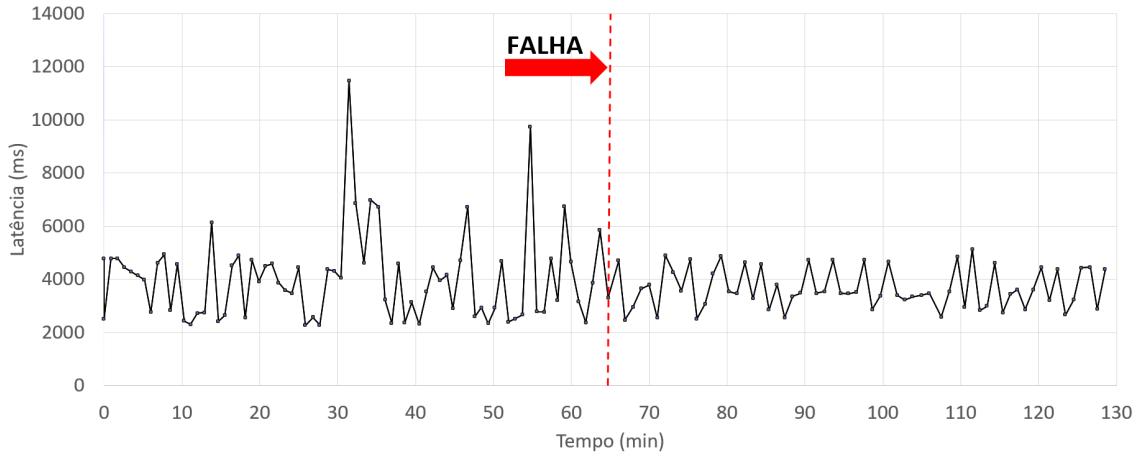
Feita a coleta dos dados, obteve-se um total de 137 comunicações, tendo uma variação média de 2,66 segundos entre as comunicações (Figura 35). Novamente, foram coletados os dados da ferramenta, e estes, conferidos com os dados do *sniffer* (Tabela 9).

Tabela 8: Dados da latência em segundos após a inserção da falha.

	Latência (s)
Mínimo	2,47
Máximo	5,13
Média	3,48

Neste estudo de caso é possível constatar que a troca da rota da comunicação foi rápida, sendo possível a obtenção da latência ja no próximo envio do comando, houve ainda uma mudança também na topologia da rede, sendo possível destacar que a inserção da falha causou o envio da mensagem tanto de *downlink* quanto de *uplink* pelo mesmo caminho, o que acarretou uma melhora na latência da comunicação fim-a-fim com o dispositivo.

Figura 35: Variação da latência durante o estudo de caso 2.



Fonte: Elaborado pelo autor.

Tabela 9: Dados coletados pelo *sniffer* Wi-Analys durante o período do estudo de caso 2.

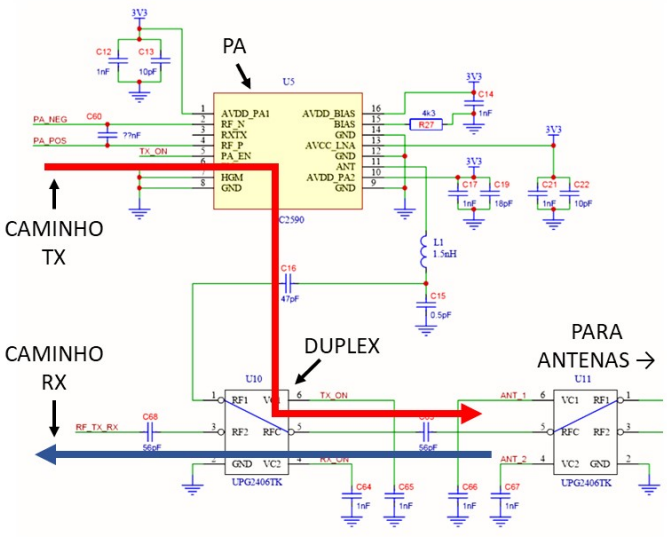
Hora	**Origem**	**Destino**	**Dados**	**Rota**
06:28:41	1	1015	cdm130	*downlink*
06:28:43	1015	1019	cmd130	*downlink*
06:28:43	1019	1008	cmd130	*uplink*
06:28:46	1008	1015	cmd130	*uplink*
06:28:48	1015	1	cmd130	*uplink*
06:28:49	1	1015	cmd131	*downlink*
06:28:51	1015	1019	cmd131	*downlink*
06:28:51	1019	1008	cmd131	*uplink*
06:28:54	1008	1015	cmd131	*uplink*
06:28:56	1015	1	cmd131	*uplink*
...	...	...	...	...
07:34:08	1	1015	cmd968	*downlink*
07:34:10	1015	1	cmd968	*uplink*
...	...	...	...	...
07:34:39	1	1015	cmd968	*downlink*
07:34:41	1015	1	cmd968	*uplink*
...	...	...	...	...
07:37:15	1	1015	cmd130	*downlink*
07:37:17	1015	1008	cmd130	*downlink*
07:37:17	1008	1019	cmd130	*downlink*
07:37:20	1019	1008	cmd130	*uplink*
07:37:22	1008	1015	cmd130	*uplink*
07:37:24	1015	1	cmd130	*uplink*
07:37:28	1	1015	cmd131	*downlink*
07:37:30	1015	1008	cmd131	*downlink*
07:37:30	1008	1019	cmd131	*downlink*
07:37:38	1019	1008	cmd131	*uplink*
07:37:40	1008	1015	cmd131	*uplink*
07:37:42	1015	1	cmd131	*uplink*
...	...	...	...	...
08:37:19	1015	1	cmd131	*uplink*

6.4 Estudo de Caso 3: desabilitando o PA de um dispositivo

O estudo de caso 3 é inspirado no trabalho de (WINTER et al., 2016) e (SOUSA, 2013), onde é inserida uma falha que leva à assimetria do enlace entre dois pares de uma rede WH. A assimetria refere-se à capacidade de um dispositivo de campo receber mensagens, reconhece-las e transmitir a confirmação (ACK). Porém, a confirmação não é recebida pelo par. Este tipo de falha pode ocorrer numa rede por dois motivos: por comissionamento inadequado da potência de RF ou por falha no PA. A primeira, é decorrente do ajuste inadequado da potência de transmissão de RF, que pode ocorrer tanto no

comissionamento como no ajuste de um dispositivo de campo já operacional. O problema ocorre quando o transceptor com a potência mal ajustada (muito baixa) está perto de um par mas longe do outro. A segunda é decorrente de uma falha de *hardware* no PA, que pode ocorrer uma vez que este componente é de potência e, por motivos diversos (excesso de calor ou sobretensão), pode queimar. A Figura 36 mostra uma arquitetura de *hardware* usual para transceptores com PA externo. Pela análise da figura, vê-se que o caminho para a recepção dos sinais é diferente do caminho para a transmissão, que passa por um PA. Logo, uma falha no PA não compromete a sensibilidade da recepção de sinais de RF, mas sim, a transmissão. Notar que esta falha é diferente de um bloqueio de sinal, onde há simetria (perda de potência transmitida e recebida).

Figura 36: Arquitetura de *hardware* usual para transceptores com PA externo.



Fonte: Elaborado pelo autor.

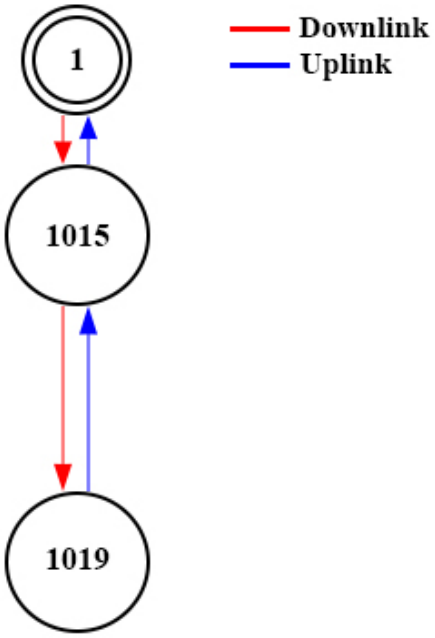
No trabalho anteriormente apresentado por (WINTER et al., 2016) e (SOUSA, 2013), os autores perceberam que o gerenciador de rede acaba por tomar uma ação equivocada na presença deste tipo de falha, eliminando da rede o dispositivo par não defeituoso. Neste terceiro estudo de caso, buscou-se validar o trabalho anterior e estender o estudo para o caso de uma rede de topologia mais complexa (malha) que a anterior (linha), além de deixar como legado, subsídios para a continuidade de uma proposta para solucionar o problema.

Diferentemente do trabalho anterior, onde os autores utilizaram o comando 797 (*Write*

Radio Power Output) para diminuir gradativamente a potência de transmissão do dispositivo. Neste estudo de caso foi implementado o comando especial 129, desabilitando o PA do dispositivo, fazendo com que somente os dispositivos mais próximos a ele sejam capazes de receber os dados transmitidos. Desta forma, é mais fácil gerar a falha, pois é possível estabelecer com segurança a distância mínima necessária para a comunicação entre o dispositivo com falha e o primeiro par, de uma só vez.

Dada a topologia sem rotas redundantes proposta pelos autores, realizou-se o experimento da mesma forma, apresentada na Figura 37. Para a realização do estudo de caso é necessário que o dispositivo no qual será inserida a falha (Tag 1011) esteja próximo ao *gateway*, com a finalidade de que mesmo após inserida a falha no dispositivo ainda seja possível a comunicação entre ele e o *gateway*, mesmo com baixa potência de transmissão. E um segundo dispositivo (Tag 1019) deve estar disposto de tal forma que conecte-se apenas com o dispositivo Tag 1011.

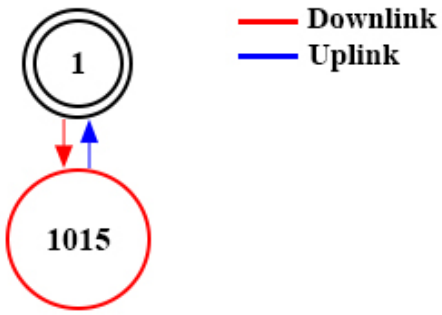
Figura 37: Topologia da rede antes da inserção da falha.



Fonte: Elaborado pelo autor.

Formada a topologia desejada, é inserida a falha para desabilitar o PA do dispositivo Tag 1011, através do comando especial 129. Após aguardar o tempo de estabilização da rede recomendado pela norma (cerca de 15 minutos), é observada uma nova topologia da rede, apresentada na Figura 38.

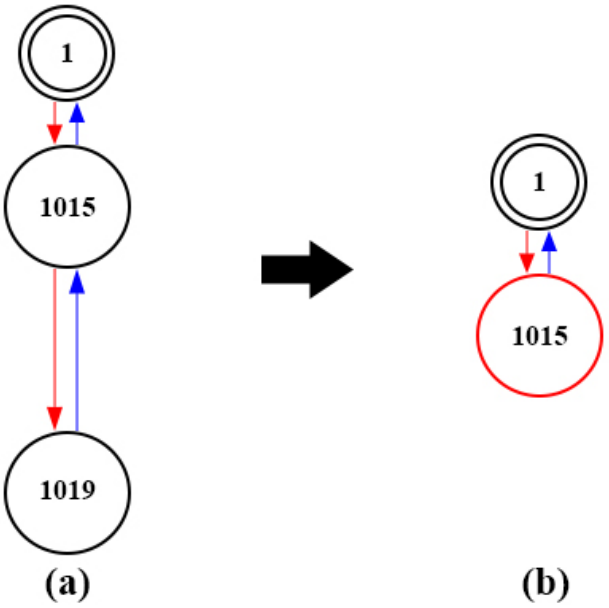
Figura 38: Topologia da rede depois da inserção da falha (gerada pela ferramenta).



Fonte: Elaborado pelo autor.

Observa-se que o dispositivo Tag 1019 não mais faz parte da rede, mesmo estando em condições normais de funcionamento, conforme apontado pelos autores anteriormente e ilustrado na Figura 39 .

Figura 39: (a) antes da falha X (b) depois da falha.

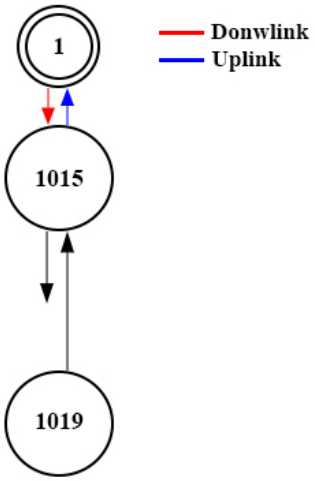


Fonte: Elaborado pelo autor.

O que de fato acontece na rede é que o dispositivo Tag 1019 envia uma mensagem para o dispositivo Tag 1011, o dispositivo Tag 1011 recebe a mensagem, porém não tem potência suficiente para responder o ACK ao dispositivo Tag 1019 (Figura 40), o dispositivo Tag 1019 reenvia a mensagem periodicamente, fazendo com que o mesmo, por falta de comunicação com o Tag 1011 (rádio com a falha), seja removido da rede. Desta forma, foi observado o mesmo comportamento observado no trabalho anterior, onde o

gerenciador de rede remove o dispositivo sem defeito e mantém o que tem defeito.

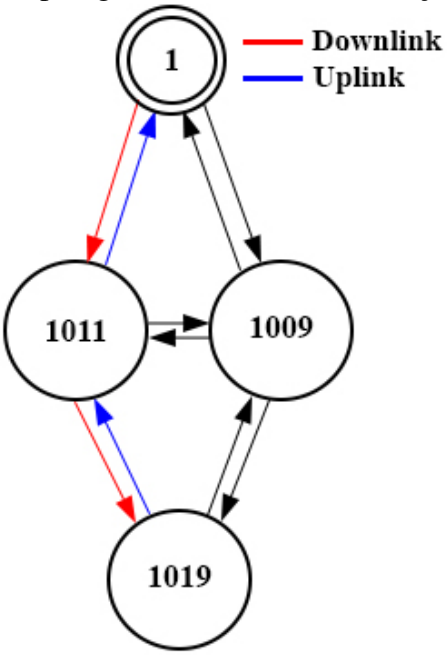
Figura 40: Topologia real da rede.



Fonte: Elaborado pelo autor.

Ainda para este estudo, propõe-se uma topologia de rede com rotas redundantes, a qual não foi abordada pelos autores, visando a análise do comportamento da rede. A topologia de rede proposta é apresentada na Figura 41, tendo o *gateway* enlaces inicialmente com os dispositivos Tag 1011 e Tag 1009, o Tag 1011 e o Tag 1009 estão próximos um do outro e comunicam entre si, e ambos também se comunicam com o Tag 1019. O Tag 1011 é roteador para a comunicação entre o gateway e o dispositivo Tag 1019.

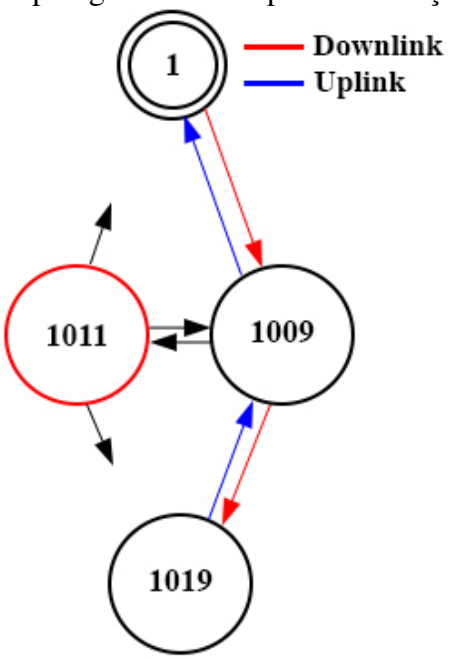
Figura 41: Topologia da rede antes da inserção da falha.



Fonte: Elaborado pelo autor.

O PA do dispositivo Tag 1011 foi desabilitado (comando 129), e analisado o comportamento da rede. Após inserida a falha e transcorrido um tempo foi gerada uma nova topologia da rede, apresentada na Figura 42.

Figura 42: Topologia da rede depois da inserção da falha.

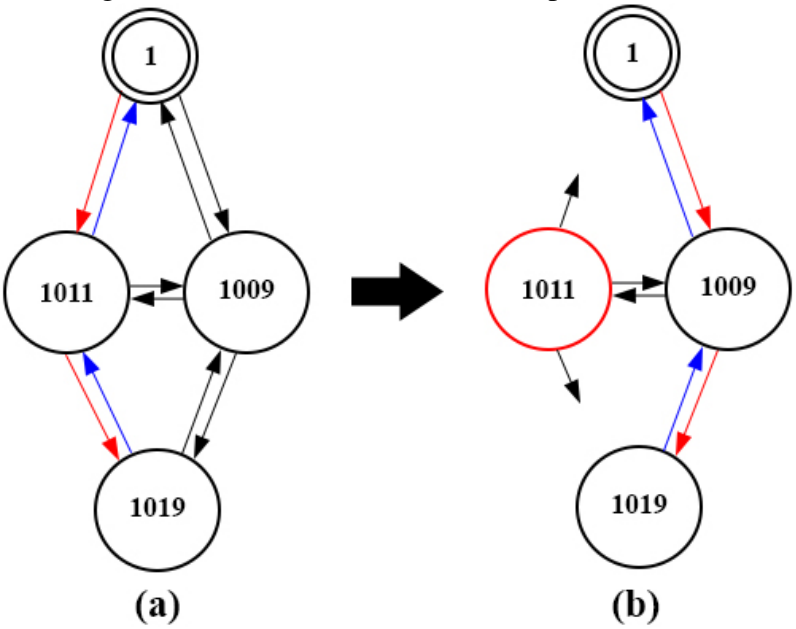


Fonte: Elaborado pelo autor.

Nota-se que houve uma alteração na topologia da rede, a rota principal de comunicação entre o *gateway* e o dispositivo Tag 1019 passou a ser pelo dispositivo Tag 1009, como ilustrado na Figura 43. Diferentemente do que aconteceu na topologia sem rotas redundantes, neste caso o dispositivo Tag 1011 se manteve ativo na rede porém sem comunicação com o *gateway* e com o Tag 1019. Esse fato se deu por conta de que os dispositivos Tag 1011 e o Tag 1009 estavam próximos um do outro, possibilitando uma troca de comunicações entre si. Isto possibilita que o Tag 1011 consiga responder solicitações dos demais dispositivos, não mais de forma direta, mas por meio do Tag 1009.

Este tipo de falha pode levar a um diagnóstico errôneo na manutenção do equipamento, pois caso o técnico responsável pela rede não tenha um conhecimento prévio da topologia da rede, e se baseie somente nos relatórios gerados pelo *gateway*, irá realizar a substituição de um rádio sem defeito, porém o problema continuará a existir na rede, como relatado pelos autores no trabalho anterior. A repetição deste estudo de caso serve para comprovar o problema anteriormente relatado e para deixar preparada a ferramenta para que se possa dar continuidade na solução para o problema, elaborada anteriormente,

Figura 43: (a) antes da falha X (b) depois da falha.



Fonte: Elaborado pelo autor.

mas não implementada. Trata-se de um aplicativo que monitora periodicamente as potências dos sinais percebidas pelos pares na rede (LQI, *link quality inidicator*) e que relata ao usuário da rede alguma discrepância observada, dentro de um limiares pré-estabelecidos.

7 CONCLUSÕES

A comunicação sem fio apresenta muitos desafios em relação à confiabilidade, especialmente em ambientes hostis. Protocolos para automação de fábrica, como o WH, apresentam uma série de mecanismos para garantir robustez à rede. No entanto, além dos recursos do protocolo, é importante se preocupar com o design do *hardware* desenvolvido para ser usado em aplicações de rede sem fio. As condições de operação do protocolo associadas a falhas de *hardware* podem resultar em perda de recursos e danos severos no processo industrial. Este trabalho explorou um método para a análise de latência dos dispositivos na rede, juntamente com injeções de falhas provocadas pelas ferramenta desenvolvida, falhas estas relacionadas a desconexão de dispositivos da rede, perda de comunicação entre dispositivos e problemas no amplificador de potência de saída de um dispositivo de campo WH.

A ferramenta permite analisar e verificar as características de uma rede WH, obter o estado dos dispositivos na rede, qualidade do sinal das comunicações, apelido do dispositivo, endereço do dispositivo, sendo possível ainda a visualização gráfica da topologia da rede e a apresentação de estatísticas como a quantidade e porcentagem dos tipos de *links*. Contudo, a ferramenta tem como principal funcionalidade a obtenção da latência das comunicações fim-a-fim, auxiliando na análise da rede tanto em operação normal como em um caso de ocorrência de falha. As falhas estas são inseridas na rede pela ferramenta, sendo possível análises detalhadas do comportamento da rede, análises estas, capazes de prover melhorias para os protocolos de comunicação sem fio industriais.

Os estudos de caso aqui apresentados mostram a aplicabilidade da ferramenta dentro das mais diversas situações que transcorrem no uso diário dos sistemas de comunicação sem fio industriais. Sendo primeiramente desenvolvido o método para a obtenção da latência fim-a-fim das comunicações entre os dispositivos, método este validado através

do *sniffer* Wi-Analys e utilizado para a análise dos estudos de caso. Os estudos de caso abordaram três situações distintas de falhas que podem ocorrer na indústria, sendo os estudos de caso realizados em laboratório contendo influências do ambiente.

O primeiro estudo de caso emula uma falha que pode ocorrer por um problema de *hardware* do dispositivo causando uma falha permanente na rede, forçando o dispositivo a se desconectar da mesma. Neste estudo de caso foi possível constatar que o dispositivo em análise demorou cerca de 14 minutos para encontrar uma nova rota e voltar a responder as solicitações.

No segundo estudo de caso foi abordada a questão falhas na comunicação entre dois dispositivos, cujo a consequência é a incapacidade de trocar de informações por *links* obstruídos, o que pode vir a acontecer por algum obstáculo impedir a comunicação entre os dispositivos. Tendo como resultados uma troca de rota da comunicação rápida se comparado com o primeiro estudo de caso.

No terceiro estudo de caso, foi reproduzido o estudo proposto em trabalho anterior, visando a alteração da potência de transmissão de um determinado dispositivo, fazendo com que o mesmo não tenha potência suficiente para se comunicar com dispositivos que estejam mais distantes, porém, com potência suficiente para manter os enlaces com seus vizinho mais próximos, uma vez que a alteração realizada no TX não interfere no RX. Este estudo de caso não foi voltado para a análise da latência das comunicações, uma vez que após a inserção da falha, a comunicação é perdida com o dispositivo. Entretanto, que pode-se considerar esta falha como grave, uma vez que pode ser interpretada de forma errônea na realização da manutenção do equipamento.

Por meio dos estudos de casos realizados utilizando a ferramenta para comunicação com o *gateway* da rede, extraindo informações dos dispositivos de campo e do próprio *gateway*, foi possível constatar que nos dois primeiros estudos de caso houve uma melhora na latência das comunicações entre os dispositivo, mesmo após a inserção da falha. Isto não significa que a topologia da rede é formada visando uma menor latência nas comunicações entre os dispositivos, pois existem diversos tipos de algoritmos de roteamento e escalonamento que podem utilizar os mesmos parâmetros de entrada, mas com funções objetivos diferentes (latência, consumo de energia, número de saltos), especificações estas que são desconhecidas, assim como os algoritmos. Logo, a rota principal de uma comunicação não é necessariamente baseada na menor latência e sim em outros critérios

desconhecidos, como robustez da rede.

7.1 Contribuições da Dissertação

Esta dissertação apresenta como contribuições principais o desenvolvimento de uma ferramenta para análise de RSSFI e estudos de caso realizados com a mesma. A ferramenta é resultado da continuidade de trabalhos anteriormente desenvolvidos que culminaram com este trabalho, onde foram desenvolvidas as partes de automação de *software*, interface web e a inclusão de um conjunto de técnicas para inserção das principais falhas que podem ocorrer nestas redes. A ferramenta utiliza um método para extração dos ASN *Snippets*, que por sua vez, fornecem informações sobre a latência das comunicações fim-a-fim. Estes dados são observáveis tanto durante o funcionamento normal da rede, quanto durante a injeção de falhas e após a recuperação. Uma vez que a ferramenta possui uma interface gráfica amigável, sua utilização é simplificada, não requerendo amplo conhecimento por parte do usuário, dos comandos do protocolo. Para efeito de comparação com os trabalhos anteriores, uma injeção de falha era realizada através do envio programados em código, enviados através de uma interface tipo console.

A dissertação contribui também com três estudos de casos, que avaliam as principais falhas que podem ocorrer numa RSSFI do tipo malha, como o WH ou ISA SP100.11a. Os estudos foram sistematizados e podem ser reproduzidos utilizando a ferramenta e outros dispositivos comerciais (*geteway* e dispositivos de campo), contato que utilizados em conjunto com os dispositivos de campo modificados, que fornecem os dados de latência para análise.

A ferramenta e métodos empregados podem ser utilizados para a realização de *site surveys*, realizados previamente à aquisição dos equipamentos comerciais, de elevados custo. Os dispositivos de campo alterados, de baixo custo, por não empregarem invólucros resistentes ao uso industrial, são instalados previamente, de forma simplificada, no local a ser avaliado. A rede é posta em funcionamento e as falhas são injetadas, tendo-se em consideração, locais com possibilidades de bloqueios e dispositivos considerados "gargalos” na rede. Uma vez avaliado o local, a rede de testes é retirada, e os equipamentos definitivos, instalados, dado as diferenças entre os equipamentos de teste e os comerciais.

7.2 Trabalhos Futuros

Como trabalhos futuros, sugere-se a implementação de novos comandos, relatórios e *scripts* de testes na ferramenta, bem como a realização dos estudos de caso em situações que não tenham interferências do ambiente, afim de torna-la ainda mais útil para a avaliação de RSSFI. A utilização em novos estudos de caso é facilmente vislumbrada, com apontado no terceiro estudo de caso e já em andamento. Uma nova funcionalidade para obtenção periódica e monitoramento constante das potências percebidas pelo dispositivos de campo evitará que dispositivos sem defeitos venha a ser substituídos no lugar de defeituosos, como apontado.

Na continuidade do desenvolvimento da ferramenta, sugere-se que seja totalmente web, sem a utilização de programa *back end*, como é feito hoje. Isto facilitaria a utilização em campo, não havendo a necessidade de instalação de *software*, apenas de um web *browser* e da configuração das portas TCP e IP.

REFERÊNCIAS

BELKNENI, M. et al. Congestion control dependability assessment. In: INTERNATIONAL WIRELESS COMMUNICATIONS MOBILE COMPUTING CONFERENCE (IWCMC), 14., 2018, Limassol. **Proceedings...** Limassol: IEEE, 2018. p.969–974.

BERLINER BPM OFFENSIVE. **Notação e Modelo de Processo de Negócio**. Agosto de 2017. Disponível em: <https://http://www.bpmb.de/>. Acesso em: 11 Mar 2019.

CHEN, D.; NIXON, M.; MOK, A. K.-L. **WirelessHART**: real-time mesh network for industrial automation. New York: Springer, 2010.

CHUNG, T. D. et al. Effect of network induced delays on WirelessHART control system. In: INTERNATIONAL CONFERENCE ON INTELLIGENT AND ADVANCED SYSTEMS (ICIAS), 6., 2016, Kuala Lumpur. **Proceedings...** Kuala Lumpur: IEEE, 2016. p.1–5.

EMERSON. **Process Management, Gateway Smart Wireless**. Abril de 2013. Disponível em: <https://www.emerson.com/>. Acesso em: 10 Jan 2019.

GALLOWAY, B.; HANCKE, G. P. Introduction to industrial control networks. **IEEE Communications Surveys Tutorials**, Hsinchu, v.15, p.860–880, 2013.

HAN, S. et al. Wi-HTest: compliance test suite for diagnosing devices in real-time wirelesshart network. In: PROCEEDINGS OF REAL-TIME AND EMBEDDED TECHNOLOGY AND APPLICATIONS SYMPOSIUM, 15., 2009, San Francisco. **Proceedings...** San Francisco: IEEE, 2009. p.327–336.

HART COMMUNICATION FOUNDATION. **WirelessHART Device Specification, HCF SPEC-290 Revision 1.1**. Austin: HCF, 2008.

HART COMMUNICATION FOUNDATION. **WirelessHART TDMA Data Link Layer Specification, HCF SPEC-075 Revision 1.1**. Austin: HCF, 2008.

HART COMMUNICATION FOUNDATION. **Wireless Command Specification, HCF SPEC-155 Revision 1.1**. Austin: HCF, 2008.

HART COMMUNICATION FOUNDATION. **Network Management Specification, HCF SPEC-085 Revision 2.0**. Austin: HCF, 2011.

HASSAN, S. M. et al. Implementation of real-time WirelessHART network for control application. In: INTERNATIONAL CONFERENCE ON INTELLIGENT AND ADVANCED SYSTEMS (ICIAS), 6., 2016, Kuala Lumpur. **Proceedings...** Kuala Lumpur: IEEE, 2016. p.1–6.

HESPANHA, J. P.; NAGHSHTABRIZI, P.; XU, Y. A survey of recent results in networked control systems. **Proceedings of the IEEE**, Torino, Italy, v.95, p.138–162, 2007.

JIN, X.; WANG, J.; ZENG, P. End-to-end delay analysis for mixed-criticality wirelesshart networks. **IEEE/CAA Journal of Automatica Sinica**, New Jersey, v.2, p.282–289, 2015.

KARBASCHI, G.; SAILHAN, F.; ROVEDAKIS, S. Towards a fault-tolerant wireless sensor network using fault injection mechanisms: a parking lot monitoring case. In: INTERNATIONAL CONFERENCE ON GREEN COMPUTING AND COMMUNICATIONS, 2012, Besancon. **Proceedings...** Besancon: IEEE, 2012. p.783–787.

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

KUNZEL, G. et al. Passive monitoring software tool for evaluation of deployed wirelesshart networks. In: BRAZILIAN SYMPOSIUM ON COMPUTING SYSTEM ENGINEERING, 2012, Natal. **Proceedings...** Natal: IEEE, 2012. p.7–12.

MACHADO, T. et al. Ferramentas para inspeção e análise de redes wirelesshart: comparação e avaliação dos métodos existentes e proposta de uma nova ferramenta. In: PROCEEDING SERIES OF THE BRAZILIAN SOCIETY OF COMPUTATIONAL AND APPLIED MATHEMATICS, 2013, São Paulo. **Proceedings...** São Paulo: SBMAC, 2013.

MACHADO, T. et al. WirelessHART network analyzer with coexistence detection. In: INTERNATIONAL CONFERENCE ON INDUSTRIAL INFORMATICS (INDIN), 12., 2014, Porto Alegre. **Proceedings...** Porto Alegre: IEEE, 2014. p.696–701.

MULLER, I. **Gerenciamento descentralizado de redes sem fio industriais segundo o padrão wirelesshart**. 2012. 105 p. Tese (Doutorado em Engenharia Elétrica) — Programa de Pós-Graduação em Engenharia Elétrica, Universidade Federal do Rio Grande do Sul, Porto Alegre, RS, Brasil, 2012.

MULLER, I. et al. Development of a WirelessHART compatible field device. In: INSTRUMENTATION MEASUREMENT TECHNOLOGY CONFERENCE PROCEEDINGS, 2010, Austin. **Proceedings...** Austin: IEEE, 2010. p.1430–1434.

NOBRE, M.; SILVA, I.; GUEDES, L. A. Reliability evaluation of wirelesshart under faulty link scenarios. In: INTERNATIONAL CONFERENCE ON INDUSTRIAL INFORMATICS (INDIN), 12., 2014, Porto Alegre. **Proceedings...** Porto Alegre: IEEE, 2014. p.696–701.

PARADIS, L.; HAN, Q. A survey of fault management in wireless sensor networks. **Journal of Network and Systems Management**, [S.l.], v.15, p.171–190, 2007.

RAPOSO, D. et al. An autonomous diagnostic tool for the WirelessHART industrial standard. In: INTERNATIONAL SYMPOSIUM ON A WORLD OF WIRELESS, MOBILE AND MULTIMEDIA NETWORKS (WOWMOM), 17., 2017, Macau. **Proceedings...** Macau: IEEE, 2017. p.1–3.

SAIFULLAH, A. et al. Distributed channel allocation protocols for wireless sensor networks. **IEEE Transactions on Parallel and Distributed Systems**, Los Alamitos, v.25, p.2264–2274, 2014.

SAIFULLAH, A. et al. End-to-end communication delay analysis in industrial wireless networks. **IEEE Transactions on Computers**, Washington, v.64, p.1361–1374, 2015.

SANTOS, A. C. S. d. **Ferramenta para análise de ativos em redes industriais wirelesshart**. 2015. 87 p. Dissertação (Mestrado em Engenharia Elétrica) — Programa de Pós-Graduação em Engenharia Elétrica, Universidade Federal do Rio Grande do Norte, Natal, RN, Brasil, 2015.

SANTOS, A. et al. Assessment of WirelessHART networks in closed-loop control system. In: INTERNATIONAL CONFERENCE ON INDUSTRIAL TECHNOLOGY (ICIT), 2015, Seville. **Proceedings...** Seville: IEEE, 2015. p.2172–2177.

SILVA, I. et al. Preliminary results on the assessment of WirelessHART networks in transient fault scenarios. In: CONFERENCE ON EMERGING TECHNOLOGIES & FACTORY AUTOMATION ETFA, 16., 2011, Toulouse. **Proceedings...** Toulouse: IEEE, 2011. p.1–4.

SILVA, I. et al. Dependability evaluation of WirelessHART best practices. In: INTERNATIONAL CONFERENCE ON EMERGING TECHNOLOGIES FACTORY AUTOMATION ETFA, 17., 2012, Limassol. **Proceedings...** Limassol: IEEE, 2012. p.1–9.

SMAR. **WirelessHART - Características, tecnologia e tendências**. Outubro de 2017. Disponível em: <http://www.smar.com/>. Acesso em: 10 Out 2018.

SOTO, V. S. et al. Control over WirelessHART Network through a Host Application: a wirelesshart network control proposal. In: BRAZILIAN SYMPOSIUM ON COMPUTING SYSTEMS ENGINEERING, 2014, Manaus. **Proceedings...** Manaus: IEEE, 2014. p.91–96.

SOUSA, F. A. A. C. **Testes de robustez em uma rede WirelessHART**. 2013. 61 p. Graduação (Bacharel em Engenharia Elétrica) — Programa de Graduação em Engenharia Elétrica, Universidade Federal do Rio Grande do Sul, Porto Alegre, RS, Brasil, 2013.

VALLE, O. T. et al. A WSN data retransmission mechanism based on network coding and cooperative relayers. In: WORLD CONFERENCE ON FACTORY COMMUNICATION SYSTEMS (WFCS), 2015, Palma de Mallorca. **Proceedings...** Palma de Mallorca: IEEE, 2015. p.1–4.

WANG, Q.; JIANG, J. Comparative examination on architecture and protocol of industrial wireless sensor network standards. **IEEE Communications Surveys Tutorials**, New York, v.18, p.2197–2219, 2016.

WINTER, J. M. **Software de análise de roteamento de dispositivos WirelessHART**. 2010. 117 p. Graduação (Bacharel em Engenharia Elétrica) — Programa de Graduação em Engenharia Elétrica, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2010.

WINTER, J. M. et al. Wirelesshart routing analysis software. In: BRAZILIAN SYMPOSIUM ON COMPUTING SYSTEM ENGINEERING, 2011, Florianopolis. **Proceedings...** Florianopolis: IEEE, 2011. p.96–98.

WINTER, J. M. et al. Analysis of a radio physical layer fault in WirelessHART networks. In: INTERNATIONAL INSTRUMENTATION AND MEASUREMENT TECHNOLOGY CONFERENCE PROCEEDINGS, 2016, Taipei. **Proceedings...** Taipei: IEEE, 2016. p.1–5.